www.rusi.org

RUSI

Occasional Paper

# Pathways Towards Multi-Domain Integration for UK Robotic and Autonomous Systems

Sidharth Kaushal, Justin Bronk and Jack Watling

Occasional Paper

**192 years of independent thinking on defence and security**

The Royal United Services Institute (RUSI) is the world's oldest and the UK's leading defence and security think tank. Its mission is to inform, influence and enhance public debate on a safer and more stable world. RUSI is a research-led institute, producing independent, practical and innovative analysis to address today's complex challenges.

Since its foundation in 1831, RUSI has relied on its members to support its activities. Together with revenue from research, publications and conferences, RUSI has sustained its political independence for 192 years.



Published in 2023 by the Royal United Services Institute for Defence and Security Studies.



RUSI Occasional Paper, October 2023. ISSN 2397-0286 (Online).

Cover Image: Ukrinform / Alamy Stock Photo

**Royal United Services Institute**
for Defence and Security Studies
Whitehall
London SW1A 2ET
United Kingdom
+44 (0)20 7747 2600
www.rusi.org
RUSI is a registered charity (No. 210639)

# Contents

# Acronyms

| | |
|---|---|
| **ABMS** | Advanced Battle Management System |
| **ASW** | anti-submarine warfare |
| **BACN** | Battlefield Airborne Communications Node |
| **DARPA** | Defense Advanced Research Projects Agency |
| **DoD** | Department of Defense |
| **DyNAMO** | Dynamic Network Adaptation for Mission Optimization |
| **EW** | electronic warfare |
| **FLC** | frontline command |
| **FNC3** | fully networked command, control and communication |
| **IBCS** | Integrated Battle Command System |
| **IDA** | Integration Design Authority |
| **JTRS** | Joint Tactical Radio System |
| **MADL** | Multifunction Advanced Data Link |
| **MDI** | multi-domain integration |
| **MDIS** | Multi-Domain Integrated Swarm |
| **MoD** | Ministry of Defence |
| **NIFC-CA** | Naval Integrated Fire Control – Counter Air |
| **OWA** | one-way attack |
| **PRP** | Personnel Reliability Program |
| **RAS** | robotic and autonomous systems |
| **STITCHES** | System-of-Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems |
| **StratCom** | Strategic Command |
| **SAM** | surface-to-air missile |
| **SEAD/DEAD** | suppression and destruction of enemy air defences |
| **UAS** | uncrewed aircraft systems |

| | |
|---|---|
| **UCAV** | unmanned combat aerial vehicle |
| **XLUUV** | extra-large uncrewed underwater vehicle |

# Executive Summary

This paper examines how multi-domain integration for robotic and autonomous systems (RAS) might be approached. Though it focuses specifically on RAS, a function of a focus on the Multi-Domain Integrated Swarm programme, its lessons can be transferred to integration more broadly.

The authors find that:

- The pursuit of integration can lead to counterproductive outcomes if its scope and optimal operational use cases are not properly defined.
- Bodies such as the Integration Design Authority (IDA) will need to consider the operational use cases which frame their work. Historically, problems have often been created when adoption of standards and programme growth have been driven by a need to demonstrate integration for its own sake, rather than being guided by operational use cases.
- Integration ought to be approached on a tiered basis. The degree to which capabilities will need to be integrated will vary by functional use case. Therefore, standards as defined by bodies like the IDA should be defined contextually, rather than aiming for universality across Defence.
- There are some considerable advantages to cross-service integration, but also costs in terms of the ability to specify and enforce standards in areas like data. Approaches which depend on backwards integration can mitigate these challenges, but at the cost of specific operational vulnerabilities to both kinetic attacks on key nodes and cyber attacks. Therefore, cross-domain integration in any given use case should be assessed in terms of the operational utility gained weighed against the challenges that implementation will create.
- The areas of the battlefield where there is greatest utility to cross-service integration are those like the littoral and close areas of the land operating environment where the capabilities of multiple services will converge at scale.
- In areas like deep zones or blue water, by contrast, the capabilities of specific services will still likely predominate, incentivising a single-service-led approach to integration comparable to that which led to the US Navy's Naval Integrated Fire Control – Counter Air architecture.
- Coordination with operators to identify specific use cases through things like operational analysis will be critical. A top-down process led by technical parameters will encounter resistance, non-adoption and slow-rolling behaviours from the operational level.
- In the medium to long term, hardware may come to define integration. Increases in processing power at the tactical edge may enable new approaches

to both network integration and translation across data formats, circumventing today's challenges around waveforms and data standards. However, integration at the edge will require platforms to meet certain hardware standards. This is currently a frontline command-controlled matter under the Levene model (the existing Ministry of Defence approach to procurement, which empowers the services to make key choices), which creates a tension with centrally managed integration change-management programmes.

- In the medium to long term, the software-led approach to digital strategy will need to embrace hardware standardisation and coordinated procurement. This will require central bodies like Strategic Command to act as facilitators in a service-led process resembling the 31 US initiatives which led to AirLand Battle.

# Introduction

Multi-domain integration (MDI) will be essential for Western militaries in the 21st century. In the US, integration both within the force and across alliances has become a cornerstone of the wider concept of integrated deterrence.[1] Similarly, in the UK, concept notes like JCN 1/20 have articulated an ambitious vision for integration across the domain-specific elements of the joint force, between the joint force and the rest of government, and across alliances.[2]

There is much to be said for the argument that integration is a force multiplier. Much of what is known from other fields of study points to the importance of integration as a means of ensuring a system's efficient allocation of resources and the agility to respond to disruption.[3] This applies to military dynamics.

First, the ability to leverage information across a joint force can lead to efficiencies which will be necessary if, as is likely, Western force structures do not grow significantly. Efficiency will also remain at a premium against opponents which, while sometimes unsophisticated, are likely to generate mass at a scale that the West may not be able to match.

Second, integration can offset adversary efforts to exploit vulnerabilities in existing single-domain kill chains. Russian and Chinese concepts of operation place a premium on systems destruction. This does not necessarily entail destroying Western platforms but rather limiting their operational effectiveness.[4] For example, both China and Russia understand that fifth-generation aircraft represent the primary means by which the US and its allies would seek to conduct critical suppression and destruction of enemy air defences (SEAD/DEAD). Rather than trying to engage these highly lethal and survivable aircraft directly, systems destruction approaches seek to force them to operate from greater distances by holding their airbases at risk. This will limit effective sortie rates and impose a greater degree of reliance on assets like tankers. These can be more readily engaged with long-range surface-to-air missile (SAM) systems like the S-400 and adversary fifth-generation aircraft like the Chinese J-20.[5] Aircraft do not need

1. James E Cartwright et al., *Operationalizing Integrated Deterrence: Applying Joint Force Targeting Across the Competition Continuum* (Washington, DC: Atlantic Council, 2023).
2. UK Ministry of Defence (MoD), 'Joint Concept Note 1/20: Multi-Domain Integration', November 2020.
3. Mancur Olson Jr, *The Economics of the Wartime Shortage: A History of British Food Supplies in the Napoleonic War and in World Wars I and II* (Durham, NC: Duke University Press, 1961).
4. Jeffrey Engstrom, *Systems Confrontation and Systems Destruction Warfare: How the Chinese People's Liberation Army Seeks to Wage Modern Warfare* (Santa Monica, CA: RAND, 2018).
5. Kris Osborn, 'How China's J-20 Stealth Fighter Could Help Beat America in a War', *National Interest*, 6 November 2020, <https://nationalinterest.org/blog/buzz/how-chinas-j-20-stealth-fighter-could-help-beat-

to be shot down in large numbers to be prevented from achieving their missions at the needed pace. However, more integrated systems can create redundant solutions. For example, if aircraft can cue ground-based fires from systems like the HIMARS, then the number of targets engaged in any given sortie can be expanded as engagements are no longer limited by each aircraft's internal payload. This, in turn, compensates for potentially reduced sortie sizes by maximising the operational effect of any one sortie.

A third advantage of integration is the ability to impose complex dilemmas on an opponent. The steps that an opponent needs to take to more effectively defend against a given threat will often make it vulnerable to other modes of attack – something that a well-integrated system can capitalise on. To use a hypothetical future example, one might envision attritable unmanned combat aerial vehicles (UCAV) comparable to those that were being investigated under the UK's Lightweight Affordable Novel Combat Aircraft programme acting as a stand-in jammer, thus leaving an opponent with the choice to engage it and expose air defence radar to other integrated crewed assets or accept a degree of communications degradation.[6]

# Robotic and Autonomous Systems on a Multi-Domain Battlefield

The imperative to better integrate forces will intersect with technological and societal drivers which are putting emphasis on robotic and autonomous systems (RAS) across Western militaries.[7] Though incipient, these new capabilities could have a profound impact on Western forces over the next 10 to 15 years. As the processing power aboard comparatively small and cost-effective uncrewed platforms grows, new approaches to tasks like target classification are emerging. For example, peer-to-peer processing at the tactical edge could enable several individually simple platforms to perform a complex task by decomposing it and solving portions in parallel.[8] In Ukraine, the Russian Armed Forces have already demonstrated the potential effectiveness of networked collaboration. They use complexes of three Orlan-10 UAVs equipped respectively with electronic warfare (EW), optical/designator and communications relay payloads to stimulate Ukrainian SAM radars; identify, locate and degrade them; and designate them

america-war-172094>, accessed 29 July 2023.

6. George Allison, 'Britain Launches New Combat Drone Project', *UK Defence Journal*, 2 November 2022, <https://ukdefencejournal.org.uk/britain-launches-new-combat-drone-project/#google_vignette>, accessed 18 August 2023.
7. Paul Scharre, *Army of None: Autonomous Weapons and the Future of War* (New York, NY: W W Norton, 2018).
8. Arslan Munir et al., 'Artificial Intelligence and Data Fusion at the Edge', *IEEE Aerospace and Electronic Systems Magazine* (Vol. 36, No. 7, July 2021), pp. 62–79.

for strikes by networked artillery and missile units.[9] Effectively, the SEAD/DEAD task that the Russian Aerospace Forces have failed to do is being undertaken by large numbers of significantly cheaper uncrewed platforms with different payloads used in a coordinated fashion. The next step is to increase the level of automation in terms of operator control, data sharing and tasking between platforms. This should allow tasks that were previously conducted by single, relatively expensive platforms to be carried out collaboratively by several potentially much cheaper ones interoperating with a smaller number of crewed systems.[10]

# Questions to be Addressed

Several unknowns regarding the specific interactions between the emergence of RAS and broader integration efforts remain. These include: questions surrounding the optimal use cases for RAS; where these use cases would benefit from integration; and what the organisational pathways towards integration might be. RUSI has conducted work for the Multi-Domain Integrated Swarm (MDIS) programme, which sits within Defence Equipment and Support as part of a wider initiative led by Strategic Command (StratCom) to accelerate MDI. MDIS is focused on RAS and their integration across the joint force. The programme's immediate task is to generate a reference architecture for integrating RAS, as well as to support the frontline commands (FLCs) through operational analysis. This paper builds on previous RUSI research on joint all-domain operations,[11] and seeks to answer several questions:

- What should the level of aspiration within the UK regarding MDI for RAS be, and what costs and trade-offs does integration impose?
- What lessons can be learned from both contemporary conflict and historical case studies about the opportunities and challenges of MDI for RAS? Success is understood in both operational (combat effectiveness) and programmatic terms.
- What lessons can be derived regarding the optimal pathways through which the MDIS programme can deliver its desired effects? What opportunities can be leveraged and which challenges should the programme prepare to confront?
- What broader lessons can be gleaned about how UK Defence approaches the challenge of integration?

9. James Byrne et al., 'The Orlan Complex: Tracking the Supply Chains of Russia's Most Successful UAV', RUSI, December 2022, pp. 1–5.
10. Bryan Clark, Dan Patt and Harrison Schramm, 'Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations', Center for Strategic and Budgetary Assessments, 2020.
11. Justin Bronk and Sam Cranny-Evans, 'Building the Capacity to Conduct Joint All-Domain Operations (JADO)', *RUSI Occasional Papers* (November 2022).

# Structure of the Paper

The first chapter of this paper outlines the options available to the MDIS programme in terms of the degree of cross-service integration that it aims to achieve. Because both RAS and integration cover a broad spectrum of capabilities and outcomes, this chapter aims to be specific regarding available options.

The second chapter describes the costs and benefits of different approaches to integration along two parameters. The first is operational – each approach to integration available to the Ministry of Defence (MoD) will create both opportunities and vulnerabilities. The trade-offs between the operational benefits of greater integration and any attendant risks need to be weighed in each case. The second parameter is programmatic risk. Many previous efforts at integration have failed for a variety of organisational reasons, including a lack of service-level cooperation and excessive growth in programme ambitions. This chapter draws out lessons in success and failure from past programmes and signposts risks that MDIS must mitigate.

The final chapter of the paper highlights areas where the authors believe the MDIS programme can generate rapid success, as well as ways in which it might be able to evolve in order to mitigate some of the longer-term risks it faces.

A combination of sources have informed this paper. Among these are historical research, fieldwork by some of the authors in ongoing conflict areas, and interviews with former military personnel and actors within the private sector who have been responsible for overseeing efforts at integrating capabilities across services and domains.[12]

12. Interviews were conducted anonymously, at the interviewees' request.

# I. Use Cases: How Much Integration is Necessary?

Integration is a broad term that can apply to a range of outcomes. In the context of organisational science, it tends to vary on two parameters. The first is the question of whether integration is intra- or inter-organisational. Individual services control assets that span multiple physical domains. This is most obviously true of the Royal Navy, which combines maritime platform air assets and the Royal Marines. However, as the British Army, for example, embraces UAVs to deliver ISR, it is also true more generally. As such, there exists a choice regarding when integration between services is to be prioritised, as opposed to integrating capabilities held by a single FLC. The latter will suffice for some use cases; for these, demanding cross-service integration will only slow programmes and raise their costs.

The degree to which integration must be achieved on an inter-organisational basis as opposed to an intra-organisational one is task-determined. For example, for a mission like anti-submarine warfare (ASW), there is a significant amount of operational-level coordination between the RAF (which operates P-8 maritime patrol aircraft) and the Royal Navy, with inputs from StratCom also being leveraged. However, at the tactical level, ASW activities are largely coordinated between the services, rather than truly integrated with individual platforms performing specific mission sets independently, even if they may at times receive data from others. Depth may be another predictor of the demand signal for integration between organisations. In the context of AirLand Battle, for example, the close-battle area was signposted as one in which maximal integration must be achieved between the Army and Air Force, while cooperation in the deep-battle area would largely take the form of deconfliction between different services.[13]

In the emerging operating environment, boundaries may blur to an extent. For example, the British Army has expressed an interest in the Lockheed Martin Precision Strike Missile; with its 500-km range, it could be capable of striking targets at strategic depth in many circumstances.[14] Moreover, non-kinetic modes of attack like cyber attacks can have effects across the close and deep areas.

13. Richard G Davis, *The 31 Initiatives: A Study in Air Force–Army Cooperation* (Washington, DC: Office of Air Force History, 1987), p. 37.
14. *Aviation Week*, 'British Reaffirm PRSM Order Plans', 1 February 2022, <https://aviationweek.com/defense-space/missile-defense-weapons/british-reaffirm-prsm-order-plans>, accessed 12 August 2023.

However, the physical limitations of platforms including many current and envisaged RAS mean that they will often have to be divided zonally, and many platforms will reinforce one another in a sequential rather than a convergent way.[15] This being said, as with AirLand Battle, there will be certain contexts where multiple capabilities can deliver convergent effects – for example, the close area of the land battlefield or littoral areas. In a peer conflict, single-domain platforms may have to converge effect to overcome the complex adversary defences likely to be found in these zones.

The second question is whether the form of interdependence that emerges from integration is pooled, sequential or reciprocal. Pooled interdependence involves self-sustaining units of an organisation contributing to one another's activity while remaining capable of operating independently. For example, we might think of an F-35 sharing data with a system like the US Army's Integrated Battle Command System (IBCS), but primarily operating independently of it. Sequential interdependence involves a situation in which one part of an organisation depends on another to perform a set of tasks before it can begin to operate.[16] The relationship between AWACS and fighter jets provides an example. Finally, reciprocal interdependence is a situation in which the output of one part of an organisation becomes the input of another and vice versa. The integration of ground and air assets into a single fires complex might meet this latter description, with the sensors of air assets being used to cue ground-based fires, which in turn are used against hostile SAM systems to create windows for less stealthy air assets to operate, and so on.[17]

In principle, RAS can fit within each model of integration based on both the use case and the theory of how they impact the battlefield. There are three dominant views regarding the future of RAS, and they are not mutually exclusive.

The first school envisions RAS as a source of cheap mass with capabilities similar to loitering munitions, representing a means of denying swathes of the battlefield to an opponent.[18] Examples can be seen today: the Ukrainian and Russian militaries rely heavily on large numbers of cheap commercial DJI Mavic 3 quadcopter uncrewed aircraft systems (UAS) for tactical situational awareness and one-way attack effects, and Ukraine has found significant utility in using

15. Justin Bronk, 'Swarming Munitions, UAVs and the Myth of Cheap Mass', in Jack Watling and Justin Bronk (eds), *Necessary Heresies: Challenging the Narratives Distorting Contemporary UK Defence*, RUSI Whitehall Paper 99 (London: Taylor & Francis, 2021).
16. Henri Barki and Alain Pinsonneault, 'A Model of Organizational Integration, Implementation Effort, and Performance', *Organization Science* (Vol. 16, No. 2, 2005), pp. 165–79.
17. Jack Watling and Sean MacFarland, 'The Future of the NATO Corps', *RUSI Occasional Papers* (January 2021), p. 19.
18. T X Hammes, 'Expeditionary Operations in the Fourth Industrial Revolution', *MCU Journal* (Vol. 8, No. 1, 2017), pp. 1–30.

repurposed agricultural UAS to drop grenades and other improvised payloads.[19] Similarly, Russia has had significant success in depleting Ukrainian air defence ammunition using the cheap and readily replaceable Shahed-136 one-way attack (OWA) UAV. However, this model assumes a significant degree of waste. Beyond minimal deconfliction, expendable assets are primarily a means of pressuring an opponent without drawing on more bespoke capabilities.

'Loyal wingman' programmes involve a second, different concept for RAS. These programmes see RAS as relatively affordable platforms – not munitions – that accompany scarce and expensive crewed assets.[20] A similar view could extend to areas like ASW. Here, systems like extra-large uncrewed underwater vehicles (XLUUVs) could perform the final parts of an ASW tracking cycle to reduce the strain on crewed platforms, or carry out high-risk tasks like mining or operating as forward sensors in well-defended bastions. Effectively, this vision would see RAS augment existing forces with platforms sophisticated enough to be sequentially or even reciprocally integrated with their crewed counterparts.

A final view of RAS, represented by the mosaic warfare concept put forward by DARPA (the Defense Advanced Research Projects Agency), is one in which large numbers of heterogeneous single-purpose platforms, coupled with the decision-making aids that allow them to be coordinated, can enable concepts of operations that overwhelm an opponent by facing them with a kaleidoscopic force that can recompose itself and conduct attacks in multiple ways.[21] Per this view, RAS would not necessarily be comparable in sophistication to crewed platforms, but would not represent simple munitions. Rather, this vision of RAS would see tactical complexity achieved through the recombination of comparatively simple robotic systems (and a smaller number of more complex crewed ones) across domains. The form of reciprocal interdependence that this would entail across domains would impose the most stringent requirements in terms of integration. The contexts where this is likely to be most useful are those parts of the battlespace where systems from across the services are likely to converge, such as the littoral or the close space in the land environment.

# Approaches to Cohering Capabilities

Attendant to each concept for using RAS is a distinct set of requirements for integration with specific programmatic considerations and network architectures.

19. Author interviews with and observation of demonstrations by UAV specialists, Ukraine, July 2023.
20. *Airforce Technology*, 'MQ-28A Ghost Bat Unmanned Aircraft, Australia', 22 June 2023, <https://www.airforce-technology.com/projects/loyal-wingman-unmanned-aircraft/>, accessed 8 August 2023; Bryan Clark and Timothy A Walton, 'Fighting into the Bastions: Getting Noisier to Sustain the US Undersea Advantage', Hudson Institute, 2022.
21. Clark, Patt and Schramm, 'Mosaic Warfare'.

For example, a concept of operations that envisioned uncrewed capabilities as eyes forward for platforms like attack submarines (SSNs) and maritime patrol aircraft, or as forward sensors and wingmen for fighter aircraft, would not require a great deal of cross-service integration. However, it would impose very stringent demands in areas like data security and latency. Single-service approaches towards integration, such as the US Navy's Naval Integrated Fire Control – Counter Air (NIFC-CA) programme, meet this requirement for integration within a service. The programme effectively imposed stringent requirements on each of its pillar projects, such as the F/A-18E/F Super Hornet, Aegis Baseline 9 and E-2D Hawkeye, but did so by creating discrete kill chains between specific platforms.[22]

For concepts of operations which envision the use of RAS as munitions or expendable capabilities, even lower levels of integration would be required. Relatively cheap OWA UAVs that can force an opponent to exhaust air defence interceptors ahead of a missile strike require effective sequencing and deconfliction with other assets, but little else. These methods have already been successfully used with existing weapons without needing extensive multi-domain integration, as during the Israeli SEAD campaign in the Bekaa Valley in 1982.[23] Some level of cooperative engagement between these munitions can multiply the effect, as with the deconfliction and target selection between Harrop and Orbiter UAVs during fighting in Nagorno-Karabakh – this is particularly important for engaging dynamic targets, which is why it is used in Brimstone, for example. However, such deconfliction does not require a high level of integration across the wider service or joint force.

Conversely, an approach that leverages a larger number of more cost-effective RAS as part of a more distributed cross-domain network of sensors and shooters would be cross-service. This could be achieved through backwards integration. A system like IBCS can draw data from multiple systems which were not designed to be compatible and which are also capable of operating independently.[24] The architecture facilitating this relies on open-standard data buses and software-defined radios which facilitate the reception of multiple waveforms and the translation of data from one format to another, as well as gateway bearers which connect disparate networks.[25] However, backwards integration imposes certain costs, especially when platforms must communicate across clearance levels.

22. Nicholas A O'Donoughue, Samantha McBirney and Brian Persons, *Distributed Kill Chains: Drawing Insights for Mosaic Warfare from the Immune System and from the Navy* (Santa Monica, CA: RAND, 2021).
23. Haim Yogev and Ronen A Cohen, 'Revolution in Military Affairs – The Operation Mole Cricket 19 as a Case Study for the Technological Race During the Cold War', *International Area Studies Review* (Vol. 25, No. 2, 2022), pp. 138–56.
24. John R Hoehn, 'Joint All-Domain Command and Control: Background and Issues for Congress', Congressional Research Service, R46725, 21 January 2022.
25. *Ibid*.

During IBCS field trials, when transmitting data across classification boundaries, very specific gateways like the Battlefield Airborne Communications Node (BACN) or the 'Einstein Box' carried by U-2 Dragon Lady aircraft were required to receive and then transmit data.[26]

The RAF Rapid Capabilities Office's NEXUS programme has taken a comparable approach. It similarly relies on a 'publish–subscribe' model for managing data, developing a government-owned common data environment into which data from a range of proprietary systems can be fed. This data can then be used by a range of assets through hosted apps designed to pull, process and exploit data for specific purposes.[27]

Alternatively, systems like DARPA's System-of-Systems Technology Integration Tool Chain for Heterogeneous Electronic Systems (STITCHES) and Dynamic Network Adaptation for Mission Optimization (DyNAMO) could be configured to support ad hoc interoperability across standards. The underlying design of both systems enables messages to be translated across formats between heterogeneous locally communicating devices. Their software-driven approach creates message interface standards between each system and an adjacent system in a network, with transmission occurring between individual nodes rather than through a shared message interface that exists across the system.[28] DyNAMO controls the network protocols, creating ad hoc pathways through the system based on software-defined routing.[29]

Approaches that require platforms at the edge to process and translate data across formats (such as DARPA's and, to an extent, the RAF's) will be hardware-centric, with microelectronics defining the ability of platforms both to receive multiple waveforms and to run the middleware needed to translate massages between formats.[30]

26. Author briefings on the Einstein Box and IBCS trials on U-2 Dragon Lady aircraft, Lockheed Martin Skunk Works, Palmdale, CA, November 2021. See also Patrick Tucker, 'The U-2's Latest Feat: Passing Data from F-35s to Army Missiles', *DefenseOne*, 3 August 2020, <https://www.defenseone.com/technology/2020/08/u-2-gets-new-role-linking-f-35s-army-missiles/167411/>, accessed 18 August 2023.
27. Author visit to Rapid Capabilities Office and interview with NEXUS team, Farnborough, 20 June 2022.
28. DARPA, 'Creating Cross-Domain Kill Webs in Real Time', 18 September 2020, <https://www.darpa.mil/news-events/2020-09-18a>, accessed 18 August 2023.
29. Jackson Barnett, 'Air Force Inks Nearly $1B Contract for Futuristic Command and Control', *FedScoop*, 1 June 2020, <https://www.fedscoop.com/air-force-abms-contract-idiq/>, accessed 18 August 2023.
30. Hoehn, 'Joint All-Domain Command and Control'.

# II. The Strengths and Weaknesses of Different Approaches

Once decisions have been made about concepts and use cases – which would require conceptual alignment between services that currently have independent RAS strategies – coherence needs to be achieved across two parameters.

The first parameter is the network architecture which facilitates the movement of data. Key choices here include whether to impose network standards across the different UK armed services or rely on capabilities like software-defined radios, which can be configured to multiple waveforms to generate interoperability.

Second, data standardisation will be necessary to an extent. While a shared language represents an optimal solution, especially if integration with allies is to be sought through fully networked command, control and communication (FNC3), consensus may sometimes be difficult to achieve across organisations. However, achieving syntactical compatibility between the languages used for different applications may be easier. In effect, the requirement would not be for a shared set of languages but for adherence to a broad set of formatting standards. In both military and civilian contexts, languages that are compatible in terms of syntax and how they structure their transport, middleware and application layers have been made interoperable.[31] What matters is that data headers, which capture the next layer of data within a message, can be understood by two or more systems.[32] Choices will need to be made regarding the stringency of requirements.

A system which imposes loosely defined requirements and relies on backwards integration at a processing node allows greater flexibility at a cost in terms of things like the need to centralise processing capacity in key nodes that can hold large processors, such as command posts. Where possible, these nodes should be mobile. For example, a system like NEXUS would depend on the ability to

31. James Dimarogonas et al., *Universal Command and Control Language Early System Engineering Study* (Santa Monica, CA: RAND, 2023), pp. 20–40; National Research Council, *Realizing the Information Future: The Internet and Beyond* (Washington, DC: National Academies Press, 1994), p. 5.
32. National Research Council, *Realizing the Information Future*, pp. 5–10.

use capabilities like tankers as communications nodes. Alternatively, vessels at sea can act as comparatively safe protected nodes. Ground-based control centres can be made more secure by distributing their components, as well as by shielding their heat and electromagnetic emissions. Despite this, however, there is always a risk of processing nodes being destroyed.

Trends towards processing at the edge can obviate the challenge of centralisation, but will introduce programmatic considerations with respect to the need to standardise hardware. By contrast, a stringent set of requirements can help circumvent these challenges, but for programmatic reasons this will be easiest to achieve within specific use cases where the ownership of one of the FLCs is clear.

This chapter discusses the tactical and programmatic trade-offs of different approaches to MDI that the MoD can opt for.

# Operational Considerations

Two dominant operational factors will impact the question of which approach to MDI is optimal:

- The speed at which effects can be delivered.
- Security against network disruption by both adversary soft kill and hard kill.

This section examines the implications of MDI with respect to these imperatives, with a specific focus on the risks that integration introduces and the approaches to mitigation.

The essence of the challenge in tactical and operational terms is that there is a trade-off between the number of interconnections within a network and its scalability, captured by the N-squared problem in systems engineering.[33] The problem in question is a function of throughput (the amount of data moved), latency and processing power. It is compounded when a system must integrate multiple different source codes, even if they are interoperable.

Contemporary open-standards architectures involve a convergence at the bearer layer of a network (which performs the movement of data) but allow a broader range of options for transport, middleware and application layers which route and translate data to an end user.[34] In this context, the integration of multiple systems within a given network creates several bottlenecks. First, it entails including discovery protocols and additional information within data headers

33. A V Aho and D Lee, 'Hierarchical Networks and the LSA N-Squared Problem in OSPF Routing', Globecom '00 – IEEE Global Telecommunications Conference, San Francisco, CA, 2000, *Conference Record* (Vol. 1), p. 397.
34. National Research Council, *Realizing the Information Future*, p. 5.

to enable routing between addresses. This imposes requirements in terms of bandwidth and attendant costs in areas like data latency.[35] The requirement for middleware to translate data between formats also imposes additional requirements in areas like the processing power of individual nodes and their characteristics in terms of size and power generation.[36] This raises questions about whether demonstrations of interoperability, such as the US Marine Corps cueing a HIMARS with an F-35 data feed, could be achieved at scale.[37]

There are several approaches to integrating capabilities, each of which involves trade-offs in terms of latency, vulnerability and the scope of integration.

## Approach 1: Publish–Subscribe Models with Central Message Brokers

One solution to overcoming the bottlenecks is a hub-and-spoke model where data is routed through a single node. This can reduce the burden by simplifying the process of data routing and reducing the requirement for processing at the edge.[38] Essentially, if data is moving to and from a small number of nodes, it can be compressed into simpler formats because there are fewer routes it can follow.[39] For example, the US Department of Defense's (DoD) compressed version of its data distribution service (which is optimised for resource-constrained environments) was able to shrink a data packet from 100 bytes to 16 using this approach.[40] This approach is visible today in programmes like the IBCS, which routes data to and from an engagement operation centre.[41]

The challenge of an architecture that relies on translation at hubs is that central nodes become targets and single points of failure – with potentially large electromagnetic signatures, given the volume of data being handled.

The risks of using centralised nodes to coordinate heterogeneous systems were seen in Iraq's French-designed KARI air defence network, which used sector command posts to consolidate data from a range of Western- and Soviet-made

35. Dimarogonas et al., *Universal Command and Control Language Early System Engineering Study*, p. 97.
36. *Ibid*.
37. Shawn Snow, 'Marines Connect F-35 Jet to HIMARS for First Time', *Marine Corps Times*, 6 October 2018, <https://www.marinecorpstimes.com/news/your-marine-corps/2018/10/05/marines-connect-f-35-jet-to-himars-rocket-shot-for-first-time/>, accessed 20 August 2023.
38. Dimarogonas et al., *Universal Command and Control Language Early System Engineering Study*, pp. 22–25.
39. *Ibid*.
40. Craig Hoyle, 'RAF Chief Reveals Combat Cloud, Swarming Drone Advances', *FlightGlobal*, 15 July 2021, <https://www.flightglobal.com/defence/raf-chief-reveals-combat-cloud-swarming-drone-advances/144604.article>, accessed 20 August 2023.
41. US Army Acquisition Support Center, 'Army Integrated Air and Missile Defense (AIAMD)', 2022, <https://asc.army.mil/web/portfolio-item/ms-aiamd-2/>, accessed 7 September 2023.

SAMs. Unsurprisingly, these fixed command posts were among the first targets for allied air and missile attack in 1991.[42] Today, centralised nodes would be targets for a range of threats, from hypersonic missiles to SAMs, and for long-range electronic countermeasures, which could actively target airborne nodes. There is also a risk of cyber penetration, because data needs to be compressed into smaller formats to be transmitted at scale. However, this removes the option of decomposing data into packets, which is central to many encryption methods.[43] Most fixes, such as padding data, increase bandwidth consumption and thus create latency problems.

Mitigation strategies exist. In Ukraine, for example, Russian command posts use field cables to link themselves to Ukrainian civilian networks, thereby hiding their data flows and limiting their vulnerability to detection.[44] Some candidates for central processing nodes, such as aircraft carriers or other large vessels, are both somewhat mobile and generally well protected. Using multiple avenues to transfer data, including growing commercial satellite networks, can allow greater throughput, and such approaches have proven resilient in the face of considerable efforts at disruption in Ukraine.[45]

To do this, encryption standards would need to be enhanced to reduce the risks emerging from compromise. Here, it is important to note that setting encryption keys centrally risks widespread compromise if the adversary can penetrate the manufacturer. User-generated encryption keys are far more secure if done properly, but their effective generation and distribution requires robust adherence to tactics, techniques and procedures and imposes a high training burden on users. In tactical contexts, the inflexibility of these processes can require that they are modified, often compromising the system.

Mobility and concealment of physical assets acting as nodes can also mitigate the risk of disruption.[46] Similarly, new forms of encryption could mitigate cyber risks.[47] However, the existence of systemic points of failure represents a risk all the same. This is not to say that a hub-and-spoke model may not add value in certain contexts, but its utility must be weighed against the challenges it creates.

42. Elliot A Cohen et al., *Gulf War Air Power Survey Volume IV: Weapons, Tactics, and Training and Space Operations* (Washington, DC: Department of the Air Force, 1993), p. 36.
43. Dimarogonas et al., *Universal Command and Control Language Early System Engineering Study*, p. 3.
44. Jack Watling, 'Putting Russia's Army in the Shadow of the Storm', *RUSI Commentary*, 15 May 2023.
45. Jack Watling, 'Supporting Command and Control for Land Forces on a Data-Rich Battlefield', *RUSI Occasional Papers* (July 2023).
46. Jack Watling, 'Ukraine's Counteroffensive Begins: Shall the Leopards Break Free?', *RUSI Commentary*, 14 June 2023.
47. Caltech, 'How will Quantum Technologies Change Cryptography?', <https://scienceexchange.caltech.edu/topics/quantum-science-explained/quantum-cryptography>, accessed 29 August 2023.

## Approach 2: Single-Service-Driven MDI with Stringent Data Standards

Where the demands of a given use case require the interoperation of specific platforms at distinct times within a service-specific construct, there are considerable advantages to a single-service approach that links specific platforms in specific ways, as illustrated by NIFC-CA. The authority of individual services over programmes under their purview can enable the specific details of data protocols to be harmonised, rather than just being made interoperable.[48] This, in turn, reduces the requirement for data translation across platforms and removes certain challenges in areas like latency and required processing power. Projects such as NIFC-CA were built around three well-defined kill chains.[49] While relatively rigid, this model was nonetheless successful at generating task-specific MDI with low data latency and a demonstrated ability to operate at scale.[50] There will be incentives for UK forces to adopt a comparable pathway in areas like ASW, where RAS like XLUUVs will likely communicate with specific systems (for example, SSNs) in order to perform well-defined tasks, and the bulk of the kill chain will be owned by a single service. A single-service approach could also see the enforcement of data standards like FNC3, which could facilitate interoperability with US assets.

In the UK, the small size of the FLCs as compared with the US and the new authorities invested in the Integration Design Authority (IDA) could, in principle, allow the MoD chief information officer and the IDA to manage the process of creating stringent standards for specific functions across services. While this is possible, the need for clear mission specification (for example, deep strike) and limiting the number of decision-makers involved would still mean that integration would be achieved for specific force packages with well-defined missions. It is also not clear, at the time of writing, whether the IDA is vested with more authority than US analogues during the net-centric transformation era.

## Approach 3: Translation at the Tactical Edge

There is a longer-term route towards a genuinely decentralised multi-domain approach to integrating RAS. Exemplified by programmes like STITCHES and DyNAMO, it relies on localised communication between adjacent nodes to create

48. The only non-Navy programme under NIFC-CA was the Joint Land Attack Cruise Missile Defense Elevated Netted Sensor System, which was eventually defunded.
49. O'Donoughue, McBirney and Persons, *Distributed Kill Chains*, p. 19.
50. *Ibid*.

emergent networks. In essence, each node passes data to the one directly adjacent to it, which does the same in turn. The need to pass and translate data to one specific node within a network limits the size of data packets as well as the number of packets any given node is processing at one time.[51] It also means that short-ranged communications like millimetric wave radios, which are harder to jam, can be relied on to form the backbone of a network.[52] That said, there is still a requirement for discovery protocols, as well as the processing power to run middleware for data translation on power-constrained devices. This would, in principle, impose considerable challenges in terms of platform size and power generation. However, it is likely that long-term trends in processing power and energy usage enabled by newer generations of chips and processor designs could solve these problems within a decade. Debate exists regarding trends in processing power beyond this point.[53]

Trends in areas like processing power, coupled with progress in AI, could allow for dynamic integration at the edge. For example, AI-enabled decision-making aids could identify locally available capabilities with which a system could network to perform a specific task, and could inquire about the availability of these capabilities on a peer-to-peer basis.[54] The network protocols needed to underpin such a decision-making chain could be established dynamically based on the ability of platforms processors to translate signals, as opposed to waveform cards (as is envisioned under DyNAMO). Finally, middleware can be run at the edge, limiting the extent to which data needs be standardised beforehand (even if basic requirements for syntactical compatibility would remain).

## Drivers for RAS Success in MDI: Horses for Courses

Scalability and adaptability are two other pertinent considerations worth exploring. In peacetime, the regulatory frameworks around employing RAS create barriers to entry for candidate platforms. In wartime, ruthless simplification and loss rates of equipment drive a need to scale production. This invariably leads to gaps between supply and demand as industry tools up to meet rapidly expanding requirements.

51. Bryan Clark, Dan Patt and Timothy A Walton, 'Implementing Decision-Centric Warfare: Elevating Command and Control to Gain an Optionality Advantage', Hudson Institute, 2021.
52. Thomas Hamilton and David Ochmanek, *Operating Low-Cost, Reusable Unmanned Aerial Vehicles in Contested Environments* (Santa Monica, CA: RAND, 2019), p. 9.
53. James McKenzie, 'Moore's Law: Further Progress will Push Hard on the Boundaries of Physics and Economics', *Physics World*, 20 June 2023, <https://physicsworld.com/a/moores-law-further-progress-will-push-hard-on-the-boundaries-of-physics-and-economics/>, accessed 29 August 2023.
54. Clark, Patt and Schramm, 'Mosaic Warfare', pp. 20–40.

Beginning with scalability, if the data standards for integrating RAS are difficult to share with industry, costly to integrate into new platforms, or overly complex to train to use properly for the end user, then they will likely be bypassed in conflict. For use cases with well-defined end-to-end kill chains, such as the air defence of a surface task group or strikes at strategic depth, this may be acceptable, as there are a limited number of systems to be networked and they fall within the same component command.

Where a larger number of heterogeneous platforms are needed, such standards mean that the force will then go through a period of self-imposed disintegration. For example, evidence from Ukraine suggests that if the UK were to enter a major conflict today, each platoon would require two UAS to be available at any given time.[55] If this volume of UAS that were compliant with the imposed standards could not be provided, it is reasonable to assume that British units would acquire off-the-shelf systems that were readily available but did not meet the standards. It is therefore important that the standards can be imposed cheaply. Critically, they must not be created with only the peacetime regulatory framework for employment in mind.

The second consideration is adaptability. RAS ultimately receive instructions and sensor data and interpret this data in defined ways to perform a repertoire of actions. As RAS malfunction, are damaged, or run out of battery and are captured, the adversary will test how they respond to a range of EW effects. Evidence suggests that almost all RAS employed today in Ukraine require alterations and updates to be made on a six-week cycle in order to keep ahead of EW tactics.[56] This is not a case of designing a perfect system, but rather an appreciation that software, frequencies and other aspects of a RAS's operation must be continually adapted to keep ahead of the adversary's understanding of how these systems work. Failure to adapt over time results in adversaries developing hard counters to most RAS.

For this reason, any standards imposed on RAS to ensure integration must enable sufficient breadth of frequencies and protocols to continue to integrate new systems that respond to evolutions in threat. This trend suggests that standards intended to support heterogeneous and ad hoc networks are likely preferable. This will be especially true for platforms which are likely to be deployed within adversary engagement zones in multiple political and military contexts. By contrast, for assets that are sufficiently sensitive to be kept out of all but the most extreme scenarios, or which will operate at reach, there will be a greater incentive to impose stringent standards in order to ensure security against other forms of compromise – especially in peacetime and the very early stages of a

55. Author visits to Ukrainian units and interviews with UAS operators, Ukraine, July 2023.
56. *Ibid.*

high-intensity conflict. In essence, a balance must be struck between standard specification and flexibility.

In effect, then, there is no one 'right' approach to integration in operational terms. Some tasks may be best achieved through highly structured integration which can be overseen by either a single service or by one or more services supervised by the IDA. This will be especially true when the RAS involved are highly sensitive platforms, such as loyal wingman UCAVs.

Where a system needs to be flexible enough to incorporate a large number of RAS including commercial systems, there will be a greater requirement for translation across data formats within a broadly defined architecture. This could be achieved through central message brokers, albeit with the assumption that this will introduce requirements in terms of protection and a need to balance the need for encryption and low latency. Where the two ideals need to exist in tandem, this will introduce limits in terms of the number of platforms incorporated into a system. However, for other tasks, especially those involving expendable assets, more flexible standards might be adopted. Finally, in the long term, an entirely different approach to coordination which involves the standardisation of hardware over software might come to underpin concepts like mosaic warfare.

# Programmatic Considerations

There are several barriers to the adoption of network standards which can bedevil enterprise planning:

- Non-adoption or partial implementation by users, especially in the absence of an authority to compel adoption.
- The inability of key stakeholders to agree on the characteristics of a standard.
- Feature and scope creep – the addition of requirements which slow the rate of adoption.
- The emergence of standards so complex that they act as a barrier to entry for new capabilities, technologies and actors.[57]

There is a considerable amount of evidence from the history of joint defence acquisition of each challenge in action. The US DoD's efforts to roll out the Joint Tactical Radio System (JTRS) across the services in the 2000s as part of a wider network-centric transformation effort illustrated many of these challenges. The vision was to create a software-defined radio system which could store multiple waveforms to be used across the services. The Office of the Assistant Secretary for Defense for Network Information Integration had the capacity for oversight

57. Carl F Cargill, 'Why Standardization Efforts Fail', *Journal of Electronic Publishing* (Vol. 14, No. 1, 2011).

but not enforcement over integration initiatives. It created a set of standards like the Net-Ready Key Performance Parameter but had no ability to control service-level acquisition.[58] This meant that there was little recourse when individual services sought to circumvent some of the standards imposed on them because the size and weight requirements that JTRS-compliant equipment would mandate was incompatible with the dimensions of planned platforms.[59]

The episode also highlights a challenge for approaches to change that begin with data architectures: in many instances, compliance with a given data architecture requires physical changes to platforms and thus a degree of oversight over decisions about platforms which services are likely to guard jealously.[60] This illustrates a third, much more universal organisational challenge: the larger the number of actors involved in any collaborative endeavour, the harder collective action becomes.[61]

In the UK context, the MoD chief information officer and the IDA will have to consider the possibility of facing a similar challenge. Like the Office of the Assistant Secretary for Defense for Network Information Integration, they can impose standards and provide oversight, but do not control platform acquisition per se. It is unlikely that standards generated will be openly defied, but notional compliance which circumvents intent, as observed within the context of JTRS, is possible – especially given the relationship between the physical characteristics of platforms and the data they process.

The US experience also highlights the risk of a growth in the scope of efforts to network capabilities. The US Air Force's Advanced Battle Management System (ABMS) evolved from a replacement for the E-8C Joint Surveillance and Target Attack Radar System aircraft into a broader and much more expensive effort to create an Internet of Things for the Air Force. The attendant cost growth placed the programme under considerable congressional scrutiny.[62] Though the programme has recovered, the growth in ambition and thus cost is instructive; in part, it reflects the absence of a clear coordinating authority, which allowed a range of sometimes poorly coordinated efforts driven by programme executive

58. On the Office, see Deputy Secretary of Defense, 'Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer (ASD(NII)/DoD CIO)', DoD Directive, 2 May 2005, <https://nsarchive.gwu.edu/document/18345-national-security-archive-deputy-secretary>, accessed 26 September 2023. On Net-Ready Key Performance Parameters, see Department of the Navy, 'Net-Ready Key Performance Parameter (NR-KPP) Implementation Guidebook', 2011.
59. Hoehn, 'Joint All-Domain Command and Control', p. 25.
60. Michael C Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010), p. 45.
61. Mancur Olson, *The Rise and Decline of Nations: Economic Growth, Stagflation and Social Rigidities* (New Haven, CT: Yale University Press, 1982), p. 31.
62. Nathan Strout, 'Congress Dealt ABMS a Blow, But Experts See Progress that Could Help at Budget Time', *C4ISRNet*, 15 June 2021, <https://www.c4isrnet.com/battlefield-tech/c2-comms/2021/06/15/part-2-congress-dealt-abms-a-blow-but-experts-see-progress/>, accessed 26 September 2023.

offices to occur under ABMS.[63] The programme's structure saw responsibility for integration held by the Chief Architect's Office, albeit with control over individual programmes which sit within ABMS held by individual programme executive offices.[64] The problems attendant on this division of authority led to the Air Force's Rapid Capabilities Office being placed in charge of integration and provided with the authority to make funding trade-offs, partially as a result of the concern that the programme was producing a number of disjointed integration use cases that lacked either wider coherence or demonstrable operational value.[65]

Well-defined mission sets and effects chains can mitigate these challenges, especially if driven by services which can impose internal standards. The more narrowly defined an effect chain is (for example, between the F/A-18E/F and an E-2D in the context of NIFC-CA), the more precise one can be with respect to both the operational requirement and the necessary standards.[66] Programmes which exist within a single service can be useful in this regard, given the ability of the service to impose decisions regarding matters like data standards and hardware requirements. However, the cost of this definition will likely be standard complexity and idiosyncrasy that may hinder future efforts at MDI. That said, this may be a viable option when the scope of what is operationally necessary does not require many assets to be integrated. In other instances, however, early successes driven by service-level activity may limit the potential scope of further integration, even when desirable.

To meet the challenge of defining the scope and function of integration, operational demonstrators can be useful. As illustrated by the history of ABMS' onboarding events (demonstrations), these tend to be most useful when demonstrating the utility of integration to meet a specific challenge, rather than merely giving the officers responsible for two different capabilities the opportunity to demonstrate that they can communicate with each other.[67] More broadly, operational analysis that is conducted on a cross-service basis can be useful for identifying which service-specific RAS programmes have cross-domain utility and – just as importantly – which do not. This can be a basis for down-selecting programmes to receive a greater focus on the standards needed for cross-service integration.

63. US Government Accountability Office, 'Defense Acquisitions: Action is Needed to Provide Clarity and Mitigate Risks of the Air Force's Planned Advanced Battle Management System', April 2020.
64. W Roper, 'Advanced Battle Management System Management Construct', Memorandum for Record, 2020, <https://insidedefense.com/sites/insidedefense.com/files/documents/2020/nov/11242020_abms.pdf>, accessed 26 September 2023.
65. Roper, 'Advanced Battle Management System Management Construct'; Ellen Chou, *Advanced Battle Management System: Needs, Progress, Challenges, and Opportunities Facing the Department of the Air Force* (Washington, DC: National Academies of Science and Medicine, 2022), p. 80.
66. Author conversation with former NIFC-CA programme manager.
67. Chou, *Advanced Battle Management System*, p. 80.

As mentioned, in the long term, more dynamic approaches to integrating RAS can be pursued. This can obviate some of the challenges described, though at the cost of introducing other programmatic challenges. For example, the scope of software-defined approaches to networking can be expanded to allow network integration without recourse to a limited number of waveform carrying cards.[68] This could be analogous to civilian systems like GNU Radio, which rely on processors to translate messages between network formats, rather than using waveform cards.[69] The dynamically configurable networks that this could enable would be further enhanced by increasing processing power at the edge, which can enable multiple language formats to be translated at pace.

On the one hand, there are considerable risks in building concepts and approaches around architectures which depend on technologies that are still maturing. Indeed, this was one of the problems bedevilling failed US programmes including JTRS, the US Army's Future Combat System and the Air Force's Transformational SATCOM.[70] On the other hand, one can point to endeavours like the advent of aircraft carrier warfare, which would likely not have been realised in the absence of efforts to conduct testing and build operational approaches to embrace a technology that was 20 years from maturity.

Perhaps most importantly, this shift would reduce the importance of standardising networks and interfaces, while simultaneously increasing the requirement for platform standardisation as the determinant of effectiveness around factors like processing power. This will pose a major challenge to models of integration which treat digital architecture as something to be approached on a centralised basis, while leaving platform choices to the services. In such cases, some of the risks observed in programmes like JTRS, which also imposed physical requirements on service-level platform acquisition, could become more acute. In the medium term, then, the IDA ought to consider whether its present software-driven approach will need to become more hardware-centric.[71]

68. Andrew Feickert, 'The Joint Tactical Radio System (JTRS) and the Army's Future Combat System (FCS): Issues for Congress', CRS Report for Congress, 17 November 2005.
69. Clark, Patt and Walton, 'Advancing Decision-Centric Warfare', p. 34.
70. Todd Harrison, 'Battle Networks and the Future Force, Part 2: Operational Challenges and Acquisition Opportunities', Center for Strategic and International Studies, November 2021, p. 6.
71. On the IDA approach, see Defence Engage, 'UK MOD Defence Command Paper 2023 – Key Takeaways for Industry', 18 July 2023, <https://www.defence-engage.com/news/uk-mod-defence-command-paper-2023-key-takeaways-industry>, accessed 26 September 2023.

# III. Options to Consider to Achieve Multi-Domain Integration

This chapter articulates how lessons from previous programmatic efforts at integrating capabilities across a joint force, as well as recent combat experience, can translate into priorities for future efforts. The authors suggest that:

- Integration should be treated as a tiered process, with different approaches meeting different use cases.
- In the short term, programmes like MDIS and authorities like the IDA can deliver considerable utility if they tailor integration requirements to specific effects chains. Doing this will require close coordination with the FLCs and operational analysis to identify how approaches to integration create both opportunities and vulnerabilities. A sharp distinction between operators and integration authorities will result in an architecture that is unlikely to secure meaningful buy-in.
- In the medium term, a shift to hardware-driven integration will require an expansion of the remit of integration approaches. This will also be most viable through FLC-led processes mediated by StratCom if compliance with the letter but not the spirit of integration initiatives is to be avoided.
- Many of the preconditions for successful integration, including hardware procurement and personnel training, still sit within the FLCs. While a more centralised UK structure could enable StratCom leadership, the experience of US DoD organisations empowered with comparable authority suggests that integration efforts should involve the FLCs early in decisions, rather than merely imposing requirements on them.
- The MDIS programme's operational analysis function may be one of its most important characteristics.

First, there appears to be considerable evidence from programmes like ABMS and NIFC-CA that the ability to situate integration within well-defined operational constructs is critical to avoiding the pitfall of integration for its own sake. If the MDIS programme were to focus on building its approach around scenario-specific use cases like theatre entry, this might help avoid service-specific efforts

to justify parallel programmes. The approach taken could mirror that outlined in the 1960s by RAND analyst G H Fisher, who advocated that platform procurement should be based not on platform characteristics but on a 'total force analysis' which examines how a given platform fits within a broader paradigm.[72] MDIS might, as an early framework, examine four types of RAS tasks:

- Tasks that involve stringent requirements in terms of latency and security and encompass platforms which need to be networked with specific crewed partners on a single-service basis or, at least, a tightly controlled one – for example, loyal wingmen.
- Tasks that involve heterogeneous platforms owned across services with low latency requirements – for example, UAV use to support distributed logistics in the littorals.
- Tasks that involve cross-service coordination with stringent latency requirements and thus a requirement for message brokers and edge platforms with considerable processing power – for example, networking sensors and platforms in the manner of IBCS or NEXUS.
- Future tasks which will become possible with low-latency communication and processing at the edge – for example, recomposable kill webs of crewed and uncrewed systems.

Understanding what will not be integrated is as important as grasping what will be. Given that every additional node in a network involves requirements in areas like throughput, latency and systemic vulnerability to attack, this is likely to be a crucial function of operational analysis. In certain use cases, such as ASW, operational analysis may illustrate that integration within a single service which can impose a shared set of communication standards across its own programmes may be preferable to MDI defined as a cross-service enterprise. In others, such as theatre entry, MDI for RAS may be useful on a cross-service basis. However, even here it will be crucial to understand precisely which capabilities need to be networked to meet the minimum standards for the mission.

Where requirements in terms of security and latency impose stringent demands on a system of systems, success is often a function of centralised control.[73] Here, the leadership of individual FLCs is an optimal solution even if it does potentially limit future growth. In such cases (for example, manned–unmanned teaming in the air domain), the number of platforms which meet the physical requirements of a use case are likely to be limited and often service-specific. So, sacrificing a programme's ability to rapidly embrace new platforms may be acceptable, as the number of new platforms being introduced will be limited. By contrast,

72. G H Fisher, 'Resource Analysis', in Edward S Quade and W I Boucher (eds), *Systems Analysis and Policy Planning: Applications in Defense* (Santa Monica, CA: RAND, 1968), pp. 124–50.
73. Observation by former senior officer involved with NIFC-CA.

however, the example of the need to adopt commercial off-the-shelf capabilities in a land context illustrates that a looser set of standards might be sought where use cases require the introduction of new platforms at pace. The MDIS team and the IDA might, then, take a tiered approach to standards, allowing one or more FLCs to agree a stringent set of standards for the former type of use case, while defining more flexible reference architectures for the latter type of requirement. Where broad-based integration is deemed desirable, it must be recognised that it will be easier to create a broad reference architecture than one that includes more specific standards for communication – as the failure of JTRS illustrates.[74] However, the scope of a reference architecture so defined would still give individual services some considerable leeway in defining both network and interface standards. Backwards integration will be necessary and will come at a cost in terms of factors like increased throughput and reduced data latency.

For cross-service coordination, especially where it is necessary to move information across classification boundaries, this will create a requirement for specialised message brokers. The possibility of this has been illustrated through the use of the U-2 Dragon Lady to mediate data between Multifunction Advanced Data Link (MADL)-enabled platforms and platforms without MADL terminals. Another way in which this might be resolved is analogous to the personnel reliability programmes which still exist on nuclear-armed vessels. In previous years, when general purpose vessels like destroyers carried tactical nuclear weapons, some personnel on a ship passed a Personnel Reliability Program (PRP) and acted as recipients of information that others could not access.[75] In a similar vein, some systems and individuals close to the edge are being certified as fit to receive and retransmit information while others are not. The requirement for well-protected central nodes acting as message brokers creates, in turn, a requirement for an understanding of which platforms are protected enough to serve these functions; this will require coordination with the FLCs and careful operational analysis.

Some of the areas in which there might be the greatest immediate opportunity for cross-service RAS integration are tasks for which demands in terms of latency and the consequences of compromise are limited, or where the very use of a RAS limits latency requirements. For example, mission sets like EW or integrated air and missile defence have very stringent latency requirements because commanders need to update information in seconds. By contrast, tasking a UAV for battle damage assessment, or to harass and stimulate an opponent's SAM

74. Harrison, 'Battle Networks and the Future Force, Part 2', p. 12.
75. On PRPs, see US DoD, 'Nuclear Weapons Personnel Reliability Program', Department of Defense Manual, No. 5210.42, 13 January 2015, <https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodm/521042m.pdf>, accessed 7 September 2023.

systems in order to build an intelligence picture of the battlefield ahead of initial contact, might impose less stringent demands.

Despite the authors' conservatism about immediate use cases, should MoD policy on greater degrees of autonomy change, the use of RAS with onboard sensors could mitigate latency requirements and thus enable more ambitious efforts at integration. For example, where the onboard sensors of a loitering munition or uncrewed ground vehicle give it some ability to search the area in which a target might be, a degree of latency may be tolerable insofar as even if a target has moved, the platform has the ability to search for it based on its last known location.[76] MDIS may not control policy here, but through operational analysis it can help lay the groundwork for services to adapt if policy does change.

A final consideration worth reiterating is that a digital architecture will be more heavily defined by coordinated hardware procurement than is generally discussed. The process of digital integration is too often treated as a software- and data-led effort, creating a neat division of labour between services which procure hardware and organisations tasked with making sure that this hardware coheres. This approach is not tenable in the medium term. In many cases, it imposes very specific hardware requirements on platforms that individual services are funding.

For example, a proposed architecture might require the procurement of gateways to enable the retransmission of different waveforms either in the form of specific systems (such as the US Air Force's BACN) or subsystems emplaced on platforms like ships.[77] The processing power needed for tasks like data translation at speed will also impose platform requirements in terms of modular payload capacity, power generation and survivability at ranges close enough to enable low latency with RAS deployed forward.

Reciprocal integration demands a degree of functional platform specialisation, which in turn would require the coordination of procurement. For example, a potential future UCAV like one based on Taranis might provide phenomenal capabilities potential as a relay, receiving data from advanced waveforms and translating it into less sensitive formats like Link 16 that can be shared across the force. However, this would impose requirements on UCAV programmes in terms of their stealth and carrying the gateways to receive, process and retransmit multiple waveforms. This would mean sacrificing capacity for weapons, sensors and fuel within any given weight and size specification. However, if the UCAV is armed, its use as a relay node may be incompatible with its primary mission

76. Army Recognition, 'L-3 Unmanned Systems Showcased the CUTLASS Tube Launched Expandable UAS at AUSA 2013', August 2013, <https://www.armyrecognition.com/ausa_2013_show_daily_news_coverage_report/l-3_unmanned_systems_showcased_the_cutlass_tube_launched_expandable_uas_at_ausa_2013.html>, accessed 26 September 2023.
77. US Air Force, 'ABMS Fact Sheet', press release, 6 November 2020.

set and an alternative node would need to be found. In effect, digital architectures will in many cases require the coordination of hardware procurement both now and in the future. This cannot be achieved by an authority other than the FLCs, creating a requirement for service-specific agreements comparable to the 31 initiatives between the US Army and Air Force, which coordinated procurement to realise AirLand Battle.[78]

This may become increasingly important, to the point of displacing data and network standardisation. Improvements in processing power may well overcome some of the hub-and-spoke challenges described above by enabling genuine integration at the edge of networks. Software-defined solutions to both networking and interfacing could mitigate the effects of the potential existence of a wide range of standards within the force. However, all of this will entail relatively stringent requirements in terms of the microelectronics that can be integrated onto platforms at the edge of a network. It will also require other enablers, such as AI-enabled decision-making aids and a changing command and control philosophy, to enable boundaries of responsibility to shift dynamically.

The long-term question for a programme like MDIS, if future integration becomes hardware-led, is how it avoids the pitfalls of US network-centric warfare initiatives which found it relatively easy to create shared reference standards, but exceedingly difficult to impose hardware standards.

One solution might be the initiation of a formal process at the service level, comparable to that which led to the 31 initiatives for AirLand Battle. Unlike that entirely bi-service process, StratCom and the programmes under it could act as referees. Operational analysis by MDIS could be used to either validate or contradict individual service-level claims regarding platform requirements and where trade-offs between the single-domain utility of a platform and its ability to host the hardware needed to act in a multi-domain context are identified. Services could, of course, still opt to avoid strict compliance, but would be doing so in a structured setting where both integrating authorities and their peer FLCs might be able to take note of this. In effect, rather than working against the grain of the services, the programme might then leverage their rivalries to good effect. The comparatively small size of the UK armed forces and the new authorities invested in the IDA in the wake of the Defence Command Paper Refresh could enable a more far-reaching version of such agreements to be sought.[79] However, this would imply that the IDA's remit would shift from one that is purely software-led to the embrace of hardware-led integration.[80]

78. Davis, *The 31 Initiatives*, pp. 30–37.
79. MoD, *Defence Command Paper 2023: Defence's Response to a More Contested and Volatile World* (London: The Stationery Office, 2023), p. 45.
80. MoD, *Defence Command Paper 2023*.

# Conclusion

This paper has articulated the pathways towards the integration of RAS capabilities being developed across the joint force, and examined some of the opportunities and challenges that MDIS may face moving forward. Its main findings are:

- Integration can, in many cases, introduce significant operational vulnerabilities which make it important to be judicious about precisely what is being integrated and what the operational use case is. Many RAS uses may be better suited to standalone programmes.
- Where integration is sought, two major pathways exist for immediate exploitation:
    - Narrowly defined single- or bi-service integration for specific tasks (for example, ASW).
    - More broad-based integration in tasks where requirements for data latency are more limited.
- Single-service integration of multi-domain assets provides opportunities with respect to a service's ability to impose strict standards on its own programmes. This is especially the case where the interoperation of these programmes with allied assets requires strict compliance with architectures like FNC3. The example of subsurface platforms like XLUUVs, which will be largely single-service and will potentially need to interoperate with the SSNs of Five Eyes nations, stands out. By contrast, tasks like building a joint intelligence picture, conducting battle damage assessments or tracking targets in a context where latency requirements are relaxed (because the platform can compensate for target movement) may be areas where cross-service integration can be more easily achieved.
- While it is relatively easy to generate reference architectures for a wider force, the more stringent the hardware requirements of interoperation are, the harder it will be to achieve coordination. This is especially true when the body tasked with oversight has no effective control over platform procurement. This is critical because hardware standardisation may become more important to integration as time progresses.

In the long term, the MDIS programme should expand its scope to better grapple with this task – which will supersede creating reference architectures. Using operational analysis and demonstrator events as part of an effort to generate

agreements between the services, as opposed to between StratCom and individual services, may represent a path forward. This would effectively be a refereed version of agreements like those that preceded AirLand Battle. Given the size of the UK's armed forces and the new authorities invested in bodies like the IDA, an expansion of the remit of what integration efforts encompass to include hardware should be feasible.

# About the Authors

**Sidharth Kaushal** is a Research Fellow for Sea Power at RUSI. His research covers the impact of technology on maritime doctrine in the 21st century and the role of sea power in a state's grand strategy. He holds a doctorate in international relations from the London School of Economics, where his research examined the ways in which strategic culture shapes the contours of a nation's grand strategy.

**Justin Bronk** is the Senior Research Fellow for Airpower and Technology in the Military Sciences team at RUSI, and the Editor of the *RUSI Defence Systems* online journal. He has written extensively for RUSI and a variety of external publications, as well as appearing regularly in the international media. He holds a Professor II position at the Royal Norwegian Air Force Academy, and is a member of the Editorial Board of the scientific and technical journal *Weapons and Equipment* at the Central Scientific Research Institute of Arms and Military Equipment of the Armed Forces of Ukraine. He is also a private light aircraft and glider pilot.

**Jack Watling** is Senior Research Fellow for Land Warfare at RUSI and a Global Fellow at the Wilson Center in Washington, DC. He works closely with the British military on the development of concepts of operation and assessments of the future operating environment, and conducts operational analysis of contemporary conflicts. Originally a journalist, he has contributed to Reuters, *The Atlantic*, *Foreign Policy*, *The Guardian*, *Jane's Intelligence Review*, *Haaretz* and others. He was shortlisted for the European Press Prize Distinguished Writing Award in 2016 and won the Breakaway Award at the International Media Awards in 2017.