www.rusi.org

RUSI

Occasional Paper

Supporting Command and Control for Land Forces on a Data-Rich Battlefield

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, July 2023. ISSN 2397-0286 (Online).

Image credit: Joint terminal attack controllers. *Courtesy US Marine Corps / Dani Zunun*

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

Executive Summary

The maturation of an ecosystem of data bearers and data management tools means battlefield hyperconnectivity is now realisable for militaries. Forces that can leverage these capabilities are likely to secure a competitive advantage over those that cannot. However, adopting these technologies requires a series of changes in how land forces conduct command and control (C2). To that end, this paper seeks to explain what is driving changes to land forces' C2, the enterprise architecture that best supports the emerging requirements, and the implications for how command is practised. The foremost drivers of change are that:

- Armies that achieve greater situational awareness will have a competitive advantage.
- Situational awareness is achieved by moving relevant data between both units at echelon and sensors and effectors to enable forces to converge their efforts.
- Data relevance must either be determined by pre-agreed prioritisation or by analysis conducted at higher echelon.
- Latency in data transfer must be minimised for control of effects.
- Latency may be high for command of the force, but the picture must constitute as complete a data set as can be reasonably assembled.
- Low-latency, high-bandwidth communications impose an unacceptable draw on power for most tactical units, which must support low-latency, low-bandwidth communication to maintain situational awareness.
- The concentration of analytical capacity at higher echelons exposes the formation to an unacceptable degree of risk from long-range fires unless these elements can be dispersed.
- Dispersion demands the automation of a significant proportion of headquarters tasks.
- Automation demands a bearer-agnostic heterogeneous data ecosystem for the force, the remotely accessible nature of which also makes it vulnerable to cyber attack.
- Any future C2 architecture must degrade gracefully and in a predictable manner under constant disruption of the electromagnetic spectrum (EMS).

Envisaging a single architecture that can support all requirements in future military networks is a mistake. Instead, it is better to design future land forces' communications on three network types:

- Tactical networks aimed at enabling lateral situational awareness, demanding high assurance, low bandwidth and medium-latency traffic. These are best delivered through mobile ad hoc networks (MANETs).

- A fire control architecture able to move ISR collection beyond line of sight through a contested EMS. This is best delivered by a bearer-agnostic heterogeneous network governed by a prioritisation stack delivering low-latency, high-bandwidth communications, theorised as a kill web.
- An operational command network through which headquarters can distribute orders and supporting information, and gather situation reports from across the force that require moderate assurance of access, can function with high latency and offers medium bandwidth. This is best delivered through a combat cloud, accessed through satellite bearers.

Although the tactical situation means that these networks should not be fully integrated, it is critical that appropriate data can pass between them. What distinguishes them is their bearers and how data is managed on the system. It is therefore important that common data standards are used to enable information egress between these three network architectures.

The adoption of such an architecture would have some implications for how command is exercised.

First, it would be important for commanders to exercise greater command discipline because the architecture would give them sight of (and the ability to direct) sub-tactical activity. Used properly, this access would be invaluable in helping them to allocate and distribute their resources and reserves. However, it would also be disastrous if operational commanders were drawn into interfering with tactical activity.

The structure would also change how headquarters function because dispersion and disaggregation, while necessary to ensure survivability, would isolate teams and make it difficult for a chief of staff to maintain a headquarters battle rhythm. It would therefore be crucial for different teams to actively strive to collaborate and to contribute where possible, rather than standing up and down in sequence.

The system would also depend heavily on AI to drive prioritisation and assist smaller staffs to plan and fuse information. Trust in these tools would be critical and training would be required to ensure their proper employment. Most of the time, it would not be viable to have a human in the loop or to have personnel understand how AI reached its decisions. For this reason, it would be necessary for AI tools to have clearly defined purposes so that confidence could be maintained by assessing them against their results. Human supervision would remain on the loop to provide assurance.

Assurance of the architecture would also be critical to ensuring that personnel remained confident in it. This would require active cyber defence, as well as a shift in mindset from an expectation of absolute security to an appreciation of

relative security. The expectation should not be that the communications architecture is sufficiently robust to always operate at peak efficiency but should instead be anticipated to be continually disrupted. Troops must therefore use its benefits as a force multiplier rather than relying on its outputs as a crutch.

Finally, such a C2 architecture would render the EMS a plane of manoeuvre and the force's posture would need to shift from minimal emissions to one in which emissions were continuous, but ambiguous. Force protection would depend on active enemy kill chain disruption rather than passive concealment. A bearer-agnostic approach would also mean that assurance of access to communications would need to be fought for and resourced. Units would proactively plan to fight for connectivity levels, rather than simply being forced from primary to alternative, contingent and emergency communications protocols based on adversary activity.

Introduction

Four primary factors drive the evolution of land warfare: arms; logistics; societal capacity; and communications. Arms development drives an evolution in tactics to employ and mitigate their effects. Gunpowder, for instance, progressively inverted survivability from being gained through elevation to being premised on separation and excavation.[1] The development of new logistical capabilities determines the force size that can be sustained, the reach at which it can be projected and the speed at which it can move. Thus, the combustion engine drastically increased the tempo of operations.[2] Societal structure determines the scale at which wars can be fought and thus its character. A society only able to generate warbands is limited in the ground that it can control, creating conflict dynamics that are driven by violence as a tool of influence and raiding being a primary function. By contrast, an industrialised society that can conscript millions of troops pushes conflict towards absolute ends. Meanwhile, communications drive the agility and complexity with which military force can be employed. For instance, it was hard to conceive of the synchronisation of operational theatres until it was possible to communicate between them.[3]

Although it has become popular to propose that advances in technology lead to 'revolutions in military affairs',[4] it is important to note that the actual introduction of emerging technologies into military service often takes 30 years before they mature enough to significantly alter the character of war. The machine gun, for example, had been in service for three decades by the time of the Battle of the Somme. The pace of evolution is sometimes faster, especially when evolutions in two or more of the factors align. Nevertheless, rather than viewing the advancement of military activity as being driven by breakthrough technologies, it is more realistic to argue that militaries adapt as a technology's implications become sufficiently clear and the capability itself matures enough to allow for general adoption. The force that transforms the battlefield tends not to be the

1. Pushkar Sohoni, 'From Defended Settlements to Fortified Strongholds: Responses to Gunpowder in the Early Modern Deccan', *South Asian Studies* (Vol. 31, No. 1, 2015), pp. 111–26.
2. H G W Davie, 'Logistics of the Combined-Arms Army — Motor Transport', *Journal of Slavic Military Studies* (Vol. 31, No. 4, 2018), pp. 474–501.
3. Brian Hall, 'Technological Adaptation in a Global Conflict: The British Army and Communications Beyond the Western Front, 1914–1918', *Journal of Military History* (Vol. 78, No. 1, 2014), pp. 37–71.
4. Steven Metz and James Kievit, *The Revolution in Military Affairs and Conflict Short of War* (Carlisle, PA: US Army War College Press, 1994).

first to employ a capability, but rather the first to work out how to employ it at scale.[5]

When considering the emergence of hyperconnectivity, it is reasonable to argue that we are approaching the 30-year horizon at which the implications of the internet and personal mobile telecommunications are sufficiently mature to drive an evolution in the character of war. As with previous technological developments, it is not that data has not played a significant role on recent battlefields. Nevertheless, its use within land forces to date has largely replicated structures that were originally designed in an analogue age, or else represent niche components attached to legacy orders of battle. The military may have swapped out analogue for software-defined radios, but the layout, staffing and functions of a modern military headquarters is recognisable when compared with its equivalent from the 1980s. It has bloated as more and more novel systems and capabilities have been added, but the fundamental underlying structure and logic remains the same.

The continuity in the military contrasts with the transformative impact of hyperconnectivity in some civilian organisations. While the implications of having ubiquitous access to data have driven a great deal of military theorising about future warfare, the practicalities of power generation in the field, signature management and communications security have all limited the adoption of many civilian methods. Nevertheless, it is becoming clear that the force that is best able to structure and equip itself to most efficiently and securely use available technology will have an advantage over its adversaries. As with previous moments, adopting modern technology at scale can be done more or less effectively. The French, for example, attempted to gain first-mover advantage when they invented smokeless powder and, as a consequence, ended up with the least ergonomic small arms of the major powers. Their early lead was shortlived.[6] It is important to get it right.

Much of the existing literature on data and the modern battlefield fits into two distinct categories. The first comprises highly technical studies of network architectures, often examining specific new technologies like encryption methods and bearer types, and revolving around programmes of record. The second emanates from military concepts like Multi-Domain Integration[7] or Joint

5. Michael C Horowitz, *The Diffusion of Military Power: Causes and Consequences for International Politics* (Princeton, NJ: Princeton University Press, 2010).
6. Yoel Bergman, *Development and Production of Smokeless Military Propellants in France, 1884–1918* (Tel Aviv: Tel Aviv University, 2008).
7. Ministry of Defence, 'Joint Concept Note 1/20: Multi-Domain Integration', November 2020, <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/950789/20201112-JCN_1_20_MDI.PDF>, accessed 20 July 2022.

All-Domain Command and Control,[8] and tends to describe an end state of perfect situational awareness with very limited engagement with the practical limitations or technologies. The former, while grounded in reality, fails to explore how a force may change how it operates as a result of evolutions in communications. Instead, it focuses on refining existing capabilities or accelerating established processes. The latter presupposes that the technology will catch up with the concepts.

In an attempt to straddle the divide between these bodies of literature, this paper takes the developments in the technology and considers how they may drive changes in the structure of how land forces are organised and how they conduct command and control (C2). It sets out a conceptual framework for thinking about the opportunities that modern communications currently present to land forces, how a force might be organised to seize them, and the communications architecture necessary to support that structure. This is not a survey of existing programmes aimed at modernising military communications. While cognisant of the trajectory of Morpheus, Mercury, Zodiac and Theia, among others, a heavy focus on these projects and programmes risks making the articulated requirement deterministic. Nor should this study be considered an attempt at systems architecture. Instead, it should be viewed as an effort to draw the enterprise architecture of C2 in the land domain to best seize the opportunities on a data-rich battlefield and mitigate emerging risks.

The emphasis on land forces requires some explanation, since modern communications architectures aim at linking the joint force and depend heavily on both the space and cyber domains. First, land forces face some distinct challenges when managing large data volumes. These largely arise from the significantly greater number of points that must be connected in a land force, the limited power available to soldier-borne systems compared with more platform-centric domains, and the interference that complex terrain generates.[9] The changes in communications architecture also have domain-specific effects on C2 for land forces. So, this paper should not be seen as excluding the other domains. Some of the networks discussed are implicitly or explicitly joint, but their effects on how a force fights are discussed as they apply to land forces.

It might be contended that this paper is not primarily about C2, but rather command, control, communications and computers (C4). This is correct, but C4 as an acronym is deeply unhelpful. Command and control are related but separate functions. The former concerns the conception and dissemination of purpose

8. Congressional Research Service, 'Joint All-Domain Command and Control (JADC2)', last updated 21 January 2022, <https://sgp.fas.org/crs/natsec/IF11493.pdf>, accessed 20 July 2022.
9. Jack Watling, 'More Sensors Than Sense', in Justin Bronk and Jack Watling (eds), *Necessary Heresies: Challenging the Narratives Distorting Contemporary UK Defence,* RUSI Whitehall Paper 99 (Abingdon: Routledge, 2021), pp. 87–98.

among bodies of troops, while the latter comprises the direction of the implementation of plans in pursuit of the defined purpose. Communications and computers, by contrast, are not functions but tools. Thus, this paper explains how the evolution of communication and computing tools realistically interact with and alter the exercise of C2.

It is also worth clarifying why a distinction is made between communications and computers. Since many communications devices are computers, this acronym is also unsatisfactory. The distinction is clearer if it is understood as that between bearers/networks and services/applications. The former is how data is moved, while the latter is concerned with what is done to it on a device. It is perhaps useful to explain this in relation to an everyday tool: the smartphone. A smartphone may use 3G, 4G, 5G or WiFi networks, which are different bearers. However, the encryption, decryption, presentation and input of the information being transmitted might be managed by a range of different services, including WhatsApp or Signal, which are distinct applications.

The paper is structured in three chapters. Chapter I outlines some of the opportunities and risks that modern communications pose and how these pressure the force to adapt from existing C2 practices if they are to be correspondingly realised or mitigated. Chapter II takes the drivers outlined in Chapter I and breaks down the architectures necessary to field the capabilities described. Chapter III seeks to map the non-structural implications for how the force would need to adapt if it were to effectively employ the systems outlined in Chapter II. The methodologies for this work are diverse, but at its core the paper is based on real-world experimentation with emerging communications systems and observation of exercises and operations on which various communication systems have been tested and employed.

I. Drivers of Change

To grasp how the exercise of C2 over land forces can adapt to best employ emerging capabilities or to mitigate the risks they pose to a traditionally structured force, it is necessary to understand how these capabilities exert pressure on the existing C2 architecture. This chapter outlines several opportunities and risks that are assessed to be drivers of change that the force must acknowledge.

Situational Awareness as a Combat Multiplier

The miniaturisation of computing means that today's battlefield is saturated with high-fidelity sensors and detections that can be retained and transmitted. The proliferation of digital systems means that the modern battlefield is data rich; the question is whether the available data can be accessed and exploited. The combination of radar, electro-optical, acoustic, electromagnetic, thermal and positional sensor payloads on vehicles and personnel is remarkable in terms of the distances at which enemies can be detected.[10] This effect is magnified exponentially when multiple sensors can be fused on a given platform and interrogated algorithmically with edge processing, and is amplified again if the picture from these sensors can be shared. Historically, humans carried out and logged target detection and classification across the battlefield. Voice was the only way to disseminate this in real time, and there was a limit to how much of this information could be shared. Nor could it be rapidly updated. However, the automated classification of objects by sensors – combined with humans logging their own observations as data – allows vastly more detections to be available to be fused if the data can be collated.

If this data can be accessed, the situational awareness of personnel across the force would radically improve. Situational awareness may be defined as the extent to which a soldier understands where they are in relation to friends and adversaries, and what those around them are trying to achieve. Having better situational awareness than the adversary gives a force a competitive edge.[11] To

10. Mikael Weissmann and Niklas Nilsson (eds), *Advanced Land Warfare: Tactics and Operations* (Oxford: Oxford University Press, 2023), pp. 163–68.
11. Patrick Downes and Michael J Kwinn Jr, 'Proving Situational Awareness Impact in the Land Warrior Project', *Military Operations Research* (Vol. 14, No. 4, 2009), pp. 47–59.

use a single example, a force in which each friendly entity can accurately track its own position and communicate this will give each soldier the ability to access blue force tracking. The inability to access blue force tracking imposes a wide range of constraints on operations. First, there is the temporal impact of needing to confirm that detected movements are hostile before delivering or calling for effects to be delivered against them.[12] Second, there are the constraints that the need to deconflict fields of fire and axes of advance impose on manoeuvre. This leads to the imposition of boundaries between units, which often creates seams (and therefore weaknesses) in formations that the enemy can exploit. Third, there is the psychological constraint imposed on soldiers by the uncertainty regarding their exposure and the extent of support once supporting or neighbouring troops are out of sight. Blue force tracking would: enable soldiers to engage enemy forces more rapidly while reducing the risk of blue-on-blue engagements; increase the freedom to manoeuvre by allowing a force to have dynamic unit boundaries; and offer a soldier psychological reassurance that they are supported.

The basis on which situational awareness may be described as a combat multiplier is the transformative effect it has on mission command. As originally conceived, mission command was premised on the ability of a soldier to use their initiative to improve their position in a manner conforming to a broader intent in the absence of centralised instruction.[13] Of course, the risk is that multiple commanders exercising this judgement reach contradictory or conflicting conclusions based on the limited information available to them. The greater the situational awareness of all troops, the more context they have to confidently exercise mission command.[14] This might be termed convergence. If mission command is premised on a soldier's ability to maintain a trajectory without supervision, with situational awareness, soldiers should be able to converge to dynamically cover gaps and exploit opportunities in a manner that deviates significantly from initial plans without dislocating the force. In short, situational awareness allows the trajectory to alter in flight. Setting the conditions for convergence also reduces the interventions necessary from command, allowing commanders to think ahead rather than become fixed in cohering disparate actions across a force.

To bring about this situational awareness, it is necessary for data to move laterally across a force. It is not necessary, for example, for the corps commander to know

12. David J Bryant and David G Smith, 'Impact of Blue Force Tracking on Combat Identification Judgments', *Human Factors* (Vol. 55, No. 1, 2013), pp. 75–89.
13. Uzi Ben-Shalom and Eitan Shamir, 'Mission Command Between Theory and Practice: The Case of the IDF', *Defense & Security Analysis* (Vol. 27, No. 2, 2011), pp. 101–17.
14. Jim Storr, 'A Command Philosophy for the Information Age: The Continuing Relevance of Mission Command', *Defence Studies* (Vol. 3, No. 3, 2003), pp. 119–29.

that an infantry section is moving left around an obstacle rather than right. But if this movement brings the infantry section into the field of view of a friendly unit under a different commander, then this section's identity is highly relevant to these personnel. This is not how most legacy military communications architectures function. Traditionally, military communications are structured to allow data to flow up and down echelons. Where there is communication within a group like the company net, the architecture is usually a hub-and-spoke model in which data is passed upwards and then downwards between sections rather than directly across the organisation. The challenge is that large lateral data movements are not viable on the same network as large vertical ones in systems where one speaker is prioritised at a time.

Lateral data movement and convergence also poses a challenge for commanders because the accumulation of the same data gives a granularity to senior officers that encourages them to take a view and correct their subordinates' activities. In a context where subordinates are exercising mission command, but their movements are visible to senior commanders, the risk is that the commander begins to try and exercise control, slowing down and confusing activity rather than increasing the precision of execution. An organisation that gives a section commander the same picture of the tactical problem as the company commander creates opportunities but also expands the capacity for commanders to misuse the fidelity of the understanding they have access to. Maximising situational awareness will increase combat effectiveness but must drive a different architecture for communications and a new culture of command.

Saturation

Although situational awareness can be enabled through the lateral movement of relevant data, the capacity to process and understand information for units at the tactical edge is finite and the effects available to units in contact to exploit information obtained is similarly limited.[15] Furthermore, as more data is accumulated, it can both improve the judgement and effects deliverable at an echelon while increasing the capacity necessary to process and use the information. Data is not in and of itself a force multiplier; it is only one if it is relevant, and establishing what is relevant to a given user presents several challenges. Moreover, data's relevance has a shelf life. If the process of ingesting, analysing and determining the relevance of information is longer than the period for which it was relevant to a user, then the data has proven a capacity-wasting burden rather than a force multiplier. Historically, echelons have not only been

15. Margaret S MacDonald and Anthony G Oettinger, 'Information Overload', *Harvard International Review* (Vol. 24, No. 3, 2002), p. 44.

divided by the span of their control but also by the temporal span of their interest.[16] Higher headquarters ought to think further ahead and have the capacity to do so. The problem today is that a force that can accumulate information rapidly in the right place can converge effects across or between echelons to achieve a decisive advantage. For example, a missile fired from the brigade echelon may have a greater chance of striking its target if the corps can deliver a cyber payload against an enemy air defence system defending the missile's target, which it may need to deliver using an electronic warfare (EW) effector held at the division, while the detection of the air defence target may have been achieved using national technical means. Conversely, the range of fires means that echelons are often simultaneously engaged throughout their operational depth. If the battlefield is saturated with high-fidelity sensors, the force that can get the right information from the right sensor to the right user has a significant advantage over one that holds but cannot transmit, process and act on the information within it. This is what concepts like Joint All-Domain Command and Control promise,[17] but they often do not address the consequent risk of saturation.

There are two kinds of saturation risk: analytical saturation; and bearer network saturation. Avoiding analytical saturation requires the prioritisation of information based on relevance to the end user. A plans cell, for example, likely requires the greatest possible volume of information to be available to them. Given the volume of data generated on a modern battlefield, there is also a strong argument for such functions to be pulled up echelon or delivered through reach-back, so that there is capacity to store and interrogate large volumes of data with sufficient computing infrastructure and analytical personnel. A tactical commander, by contrast, is going to be unable to analyse the volume of data from most of the battlefield, much of which will be of limited relevance to them. There may be many data points that are relevant to them, but they cannot be the ones finding them. Thus, data must either be brought to higher echelons, processed, analysed and then disseminated, or there must be a sift for data that is known to be relevant to a particular tactical formation at the edge using edge processing so that this can be prioritised for transfer to the end user.[18] The answer is not one or the other but depends on the latency requirements of the given data type.

Bearer network saturation is inevitable if all information is attempted to be assembled all the time.[19] The volume of data on the battlefield is expanding faster than the bearer capacity to move it. Prioritisation reduces the volume of data that needs to be moved from one location to another and prevents this.

16. Donn A Starry, 'Extending the Battlefield', *Military Review* (Vol. 61, No. 3, 1981), pp. 31–50.
17. Congressional Research Service, 'Joint All-Domain Command and Control (JADC2)'.
18. David S Alberts and Richard E Hayes, *Power to the Edge: Command and Control in the Information Age* (Washington, DC: Command and Control Research Program, 2003).
19. Robert Leonhard, *The Principles of War for the Information Age* (New York, NY: Ballantine, 1998), pp. 16–20.

Latency is another means of reducing the requirements on the bearer network. If there is no requirement for low-latency transfer, information can be routed inefficiently to fill up slack capacity or underutilised links, or held back for transfer once higher-priority information has been moved. Conversely, higher-priority information can be moved rapidly via any available means, even if this means suppressing the movement of lower-priority information.[20] A good example here might be to contrast track quality data on an enemy air or missile threat with a routine situation report from a screening unit. Clearly, the former takes precedence. When one maps the prioritisations likely in a modern force, this does not conform to the order of battle. Thus, information may, in certain contexts, need to jump echelons entirely, move rapidly laterally between units, or else a commander's information requirements may in fact justify de-prioritisation. Seniority does not necessarily determine the latency requirements for success.

Another way that saturation can become a critical threat to the system, and thus a driver for its design, is power consumption.[21] Soldiers can only carry so much power. Processing and analysing data consumes a great deal and must be centralised. Transmission of large-bandwidth data over distance also draws on considerable power. For tactical echelons wishing to maintain persistent situational awareness, moreover, power consumption is a constant, whereas the ability to move information at low latency is an intermittent but essential requirement for critical systems. If the intervening elements have run out of power and are unable to transmit this data, the system breaks down. Conversely, if low-latency or higher-echelon critical information requirements route traffic through tactical units on a routine basis, they risk running down the force's available power and leading to blackouts or creating a massive logistical demand for batteries. The need to avoid saturation is thus a critical determinant of how future C2 architectures must be structured.

Precision Fires as a Pervasive Threat

As mentioned earlier, situational awareness may be a force multiplier, but constructing a relevant picture of the battlespace from a huge volume of data requires analytical capacity and power, which drives centralisation into headquarters. This was certainly how these challenges were managed during the War on Terror, when brigade headquarters grew attachments until they

20. David Zats et al., 'DeTail: Reducing the Flow Completion Time Tail in Datacenter Networks', Proceedings of the ACM SIGCOMM 2012 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, Helsinki, 13–17 August 2012.
21. John W Lyons, Richard Chait and James J Valdes, 'Assessing the Army Power and Energy Efforts for the Warfighter', Center for Technology and National Security Policy, National Defense University, March 2011.

were orders of magnitude larger than a viable warfighting formation even in the 1980s.[22] This situation is only possible because of the low threat from enemy fires in these environments. At the same time, the capacity to find such concentrated entities on the modern battlefield has expanded drastically because of the saturation of the battlefield with stand-off sensors, especially in the joint environment. Furthermore, the proliferation of loitering munitions and cruise and ballistic missiles – offering precise, layered and long-range fires – means that such facilities can be held at threat at any relevant operational depth to land forces.[23]

The pervasive threat of detection and long-range precision fires drives several structural requirements for the C2 infrastructure that introduce friction into the characteristics outlined above. First, there is a need to either be highly mobile or make an element's signature minimal or ambiguous. Second, on the assumption that the adversary might be lucky even against the most disciplined of forces, the headquarters should be dispersed to reduce its exposure to fires. This may even mean the dispersion of headquarters functions between states or continents. Here, there is a tension between the concentration driven by the demand for analytical capacity and power to process the available data, and the need to be survivable driving the disaggregation of headquarters elements.

Perhaps the greatest irony is that the direction of long-range precision fires likely creates one of the foremost demands on low-latency, high-bandwidth communication and rapid data fusion and analysis for the purposes of fire control. At the same time, it is precisely these fires that render the establishment of the infrastructure to support such a capability most precarious. Again, therefore, there is a compelling reason to strive to be able to ingest, interrogate and use the data on the modern battlefield. However, the side that is able to do it most efficiently – with a lower signature, greater dispersion and likely more effective prioritisation – will have a competitive advantage that should grow as Lanchester equations make fire exchanges more unequal over time.[24] Lanchester equations highlight how attrition constrains force projection so that as one force suffers greater losses, its relative loss at each exchange expands. They have proven highly unsatisfactory in assessing engagements for much of the 20th century, but the advent of mass precision may make them more relevant to future exchanges.[25]

22. Harry Tunnell, 'Task Force Stryker Network-Centric Operations in Afghanistan', Center for Technology and National Security Policy, National Defense University, October 2011, p. 2.
23. Mykhaylo Zabrodskyi et al., 'Preliminary Lessons in Conventional Warfighting from Russia's Invasion of Ukraine: February–July 2022', RUSI, 30 November 2022, pp. 53–54.
24. James G Taylor, 'Solving Lanchester-Type Equations for "Modern Warfare" with Variable Coefficients', *Operations Research* (Vol. 22, No. 4, 1974), pp. 756–70.
25. CSM XVIII Airborne Corps, LANPAC panel audio, 26 May 2023, <https://otter.ai/u/dr6TdUGHPGmodiWJ7tSlBw-iWKQ?utm_source=copy_url>, accessed 10 June 2023.

Dispersion is a sensible approach to expanding survivability, but it poses major challenges for assuring a capability's delivery. Once key functions are geographically separated, communication not only becomes vital for the exercising of C2 but also in the internal functioning of the headquarters. A dispersed force therefore begins to build in single points of failure. Whereas a headquarters with co-located functions can physically connect parts of its internal infrastructure (and, failing that, physically co-locate staff as a reversionary means of overcoming connectivity issues), a dispersed force becomes entirely dependent on its network. This renders it vulnerable to another kind of precision effect which modern sensors and targeting processes can make effective at long range: EW. The ability to interrogate the electromagnetic spectrum (EMS) combined with the use of software-defined EW systems means that it is becoming easier to assess a target network's characteristics, build a payload to achieve the greatest possible disruption and deliver it at reach in combat-relevant timeframes.

Interrogation by Machine

A critical enabler of dynamic and precise electronic attack is the employment of AI to support the creation of effects. This is also arguably the most effective means of prioritising bandwidth.[26] Use cases for AI are often framed around the analysis of vast data sets.[27] However, since assembling such data sets is often prohibitively burdensome for a deployed network, AI can depend on machine learning (ML) used at the edge to fuse sensor data on the originating platform and package what is sent to higher echelons or laterally to key users. Again, such judgements become the basis for managing latency too. An F35, for example, generates far more data than it can relay, but much of that can be centrally ingested once it lands and is plugged into an autonomic logistics information system (ALIS) terminal.[28] The question concerns what cannot wait and ensuring that what is off-boarded moves with sufficient metadata to be useable by another system with incomplete information.

ML-enabled reconnaissance and AI-enabled bandwidth prioritisation is likely to give a force a decisive situational awareness advantage because of the efficiency gains it offers in sensor performance. At its most basic, humans interrogating a sensor feed tend to distinguish signal from noise through the size of deviation from the background environment. ML-driven data interrogation is different. ML systems define objects by reference to unique characteristics, and deviation

26. N H Saeed et al., 'Intelligent MANET Routing Protocol Selector', IEEE, 2008.
27. N A Wilson, 'Understanding the Battle for AI in Warfare Through the Practices of Assemblage: A Case Study of Project Maven', Master's thesis, Utrecht University, 2020.
28. Justin Bronk, 'Maximum Value from the F-35: Harnessing Transformational Fifth-Generation Capabilities for the UK Military', *Whitehall Report,* 1-16 (February 2016).

from those are therefore counted irrespective of magnitude. This can create problems. An ML algorithm trained to look for humans may, for instance, fail to classify a person walking underneath a cardboard box as such because it deviates from the prescribed definition.[29] A human would, by contrast, note the contrast with the background environment and deduce what was under the cardboard box. However, in terms of sensor data, the implication of this difference is that ML algorithms will make detections based on far smaller – and less distinct – returns than a human. Thus, if appropriately applied, ML will significantly increase the range and accuracy of detections, thereby improving the fidelity of the situational awareness available to be transmitted across the force. The point is that a force that fails to capitalise on such capabilities risks being uncompetitive.

AI also offers a support tool to higher headquarters for data ingestion and analysis, as well as the creation of courses of action in planning. It may also contribute to another form of situational awareness relevant to those exercising command: the ability to anticipate adversary moves. A good example of this has been demonstrated in Ukraine, where 18 Airborne Corps, monitoring Russian activity from space, is able to use AI to anticipate whether Russia is about to conduct offensive action by recognising artillery fire patterns.[30] The use of AI in headquarters is also the most likely means of enabling dispersion as it would reduce the necessary size of a given staff element. The aim would not be to replace the commander or the supporting headquarters functions. Instead, by using AI to rapidly assemble the labour-intensive products that must underpin an assessment of a course of action, it would reduce the headquarters' footprint. A good analogy is the introduction of satellite navigation tools used by drivers in cars. Prior to the availability of applications like Google Maps, ubiquitous cellular connectivity, real-time traffic-density data and algorithms able to compare viable routes, dynamic navigation while driving required a second person to work with a map, or the driver to stop the vehicle to look at one. Today, a single driver can leave the navigation to their phone, reducing the number of people required to dynamically assess viable routes. Drawing up a scheme of manoeuvre based on terrain and an assessment of adversary troop strength is something that AI can do, even if a human wants to select from the options generated and potentially tweak the eventual scheme. It is in these more basic functions that AI is likely to best enable the force, not in complex decision support tools.

There are two requirements for such a system to reduce a headquarters' size and enable dispersion. First, data must be bearer agnostic. That is to say that for a headquarters to assemble the relevant information at the speed of relevance,

29. Katherine Tangalakis-Lippert, 'Marines Fooled a DARPA Robot by Hiding in a Cardboard Box While Giggling and Pretending to be Trees', *Business Insider*, 30 January 2023.
30. CSM XVIII Airborne Corps, LANPAC panel audio.

it will need to accumulate data from a range of units that, transmitting over various distances in the face of differing threats and interference, will be communicating on different bearers. Some will be using civilian comms, others will be using high-frequency radio or satellite communication. Inputs from these feeds have historically been separate and required human integration. If a headquarters' headcount is to be reduced, these feeds will need to be fused with human supervision, but not through manual data transfer between systems. The data's format and language must be compatible so that systems supporting a headquarters can properly ingest the information.

Cyber Attack as a Persistent Threat

The need to ensure that data can be transferred through multiple bearers and ingested by systems from multiple feeds means that the future C2 architecture is significantly more accessible than its predecessors. But such a system is vulnerable to cyber attack and, if it is to be useable, cannot be proofed against this. So long as humans are involved, means of access and interference exist. The protocols and permissions inside the system may limit the impact or scale of possible interference, but it will occur. Furthermore, any system that is accessible beyond line of sight can be targeted not just by an opponent's military but also by their non-military institutions, vastly increasing the resource available to attack it. Again, the battlefield advantages of such a system drive its adoption to retain competitiveness even as it creates vulnerability. Appreciating that such a system will be attacked and that attacks will succeed, its survivability becomes a question of how well its borders in cyberspace are patrolled. Vigilant cyber threat intelligence, systems monitoring and incident response can maintain a system's survivability even against the most persistent and aggressive adversary. The banking sector provides evidence of this: while a highly diverse set of actors continuously attack it, and intrusions and data loss occur, this threat does not fundamentally prevent the system's functioning. The sector does, however, invest heavily in active network defence.

Unlike electronic attack or precision fires, the cyber threat does not diminish in peacetime. Hostile forces are continuously tasked with infiltrating payloads against digital systems outside of an armed conflict.[31] Far from this being the nefarious and irresponsible practice of rogue actors, the time it takes to reconnoitre a hostile network, gain access, design and deliver a payload, and establish a trigger mechanism, means that this is an activity that must be practised continuously. If it is not, then such capabilities will not be available

31. John P Carlin with Garrett M Graff, *Dawn of the Code War: America's Battle Against Russia, China, and the Rising Global Cyber Threat* (New York, NY: Public Affairs, 2018).

when they are required. The result is that headquarters must be on a permanent war footing when it comes to network assurance. Detecting and closing intrusions is an ongoing commitment. This requires expertise that does not traditionally exist within militaries and means that while one part of a headquarters may be exercising, its cyber defenders are very much on operations.

Resilience by Design

Given the advantages of the processes already described in this chapter, it follows that breaking down an adversary's communications architecture and monitoring to inform targeting are key collection priorities for any force. However, there are some misconceptions about the dynamics likely to dominate the future battlefield in relation to the contestation of the EMS. First, the prospect of a denied EMS has been widely hypothesised. While possible over a limited area for a limited period, total denial of the EMS is not viable because the emitters necessary to deliver such an effect are themselves highly vulnerable to strike. Conversely, however, there is often a conflation of resilience and assurance that is deeply problematic. Designing a communications architecture that is highly resistant to jamming and interference is a worthy but impractical aspiration. As software-defined electronic attack systems are twinned with AI and ML, it will become increasingly possible to deliver bespoke payloads that optimally target communications systems. The likelihood is that while total denial will be impossible, continuous disruption to parts of the EMS and the uneven interruption of transmission will be a feature of the future battlefield. It is also important to note that forces will want to minimise their signature under many circumstances and may proactively withdraw from networks to do so. They may also wish to practice deception and mimic the communications patterns of other force elements. For parts of the force, this may be critical to their survival.

The considerations outlined above present some serious challenges for an effective C2 architecture. First, some nodes may voluntarily withdraw themselves from the network, thereby severing pathways for information flow. Second, the adversary may deny certain pathways for periods of time or reduce bandwidth and increase latency of transmission, rendering kill chains unpredictable. Between friendly and adversary actions in the EMS, therefore, the risk is that a force expecting to have strong situational awareness will act in the belief that they have an up-to-date picture of the operating environment while lacking critical information.

Some technical and tactical requirements emerge out of this. Technically, it is necessary for a network to be built with the presumption that parts of it will not work optimally. In other words, rather than trying to build a completely assured

architecture, it is better to have one that accepts that degradation is inevitable and degrades gracefully. Another requirement is that the system's components can verify the latency at which it is operating and adjust prioritisation, routing and assessment accordingly. Third, it is vital that users understand whether they are operating with a current or degraded picture of the operating environment. A part of the force severed from blue force tracking, for example, has lost an advantage and the commander may expend resources to regain access to it. But it is critical that the commander knows that the connection has been disrupted rather than being forced to work this out only when the tactical situation confronting them differs from its representation on their technical systems.

Tactically, resilience demands that control as to exposure and participation lies with the user. This may also mean that a commander decides to instruct part of a force to reduce its connectivity, either in terms of its lateral or vertical integration, to minimise its signature. Units may also make these decisions themselves, but the network structure must function for those that remain connected even as parts of the system withdraw from it. Here, it is necessary to conceptualise the EMS as a plane of manoeuvre and – like all manoeuvre – activity in this space must be proactively planned and reactively adapted to based on the tactical situation. A network structure that presumes a single configuration and linear degradation from it is likely to be overly centralised and too easy for adversaries to map and target. So, resilience should not be defined purely in terms of the difficulty of disrupting the network, but in the tactical options that the network architecture provides to commanders. A resilient system is one that can be configured based on mission requirements, rather than having system requirements constrain mission planning.

II. A Straw-Man Command and Control Architecture

Surveying the drivers outlined in the previous chapter, some basic propositions can be put forward that determine the contours of a future C2 architecture. These may be understood as the system's requirements, but also its constraints. The challenge, in some instances, is to reconcile conflicting imperatives. In such cases, forces may vary in how they choose to reconcile these variables, but will need to mitigate the vulnerabilities they accept through tactics. This chapter considers the architecture supporting C2; the next chapter examines the practice of command.

The propositions emerging from Chapter I may be outlined as follows:

- Armies that achieve greater situational awareness will have a competitive advantage.
- Situational awareness is achieved by moving relevant data between both units at echelon and sensors and effectors to enable forces to converge their efforts.
- Data relevance must either be determined by pre-agreed prioritisation or by analysis conducted at higher echelon.
- Latency in data transfer must be minimised for control of effects.
- Latency may be high for command of the force, but the picture must constitute as complete a data set as can be reasonably assembled.
- Low-latency, high-bandwidth communications impose an unacceptable draw on power for most tactical units, which must support low-latency, low-bandwidth communications to maintain situational awareness.
- The concentration of analytical capacity at higher echelons exposes the formation to an unacceptable degree of risk from long-range fires unless these elements can be dispersed.
- Dispersion demands the automation of a significant proportion of headquarters tasks.
- Automation demands a bearer-agnostic heterogeneous data ecosystem for the force, the remotely accessible nature of which also makes it vulnerable to cyber attack.
- Any future C2 architecture must degrade gracefully and in a predictable manner under constant disruption of the EMS.

These propositions suggest that there are three processes with very different characteristics in play: command; control; and convergence.

Table 1: Network Characteristics Against Functions

	Command	Control	Convergence
Latency	High	Low	Medium
Traffic Regularity	Low	Medium	High
Signature	Low	High	Medium
Bandwidth	High	Medium	Low
Assurance	Low	High	Medium
Distance	High	Medium	Low

Source: Author generated.

Observing the distinct requirements of an appropriate communications architecture supporting each of these functions, it is possible to outline mature and emerging technologies that might be leveraged to deliver appropriate systems for future forces.

Enabling Convergence Through Mobile Ad Hoc Networks

The immense tactical value of a company net in which all soldiers in a formation can listen to a defined frequency, and those with transmitters can speak over it, should not be underestimated. The ability to provide situational awareness through passive monitoring, to coordinate actions where sections are beyond verbal range, and the capacity for commanders to clarify their tactical picture, all allow for a unit to adapt to overcome challenges in contact.[32] There are some serious limitations, however, to traditional company nets. The fact that only one person can speak at a time limits the complexity of what can be managed. The pattern of transmission and receipt on such a system also allows the formation's structure to be tracked in the EMS, allowing for the identification of command posts and support weapons. Furthermore, an attachment joining the company or transiting its battlespace cannot simply tune in to the network but must swap encryption keys with the company and, in doing so, must stop communicating on other frequencies. Thus, attachments like joint terminal attack controllers, tasked with communicating with aircraft, will be on a different net and be readily identifiable in the EMS. While this system worked well for the transmission of verbal instructions, it is not well suited to the ingestion, integration and

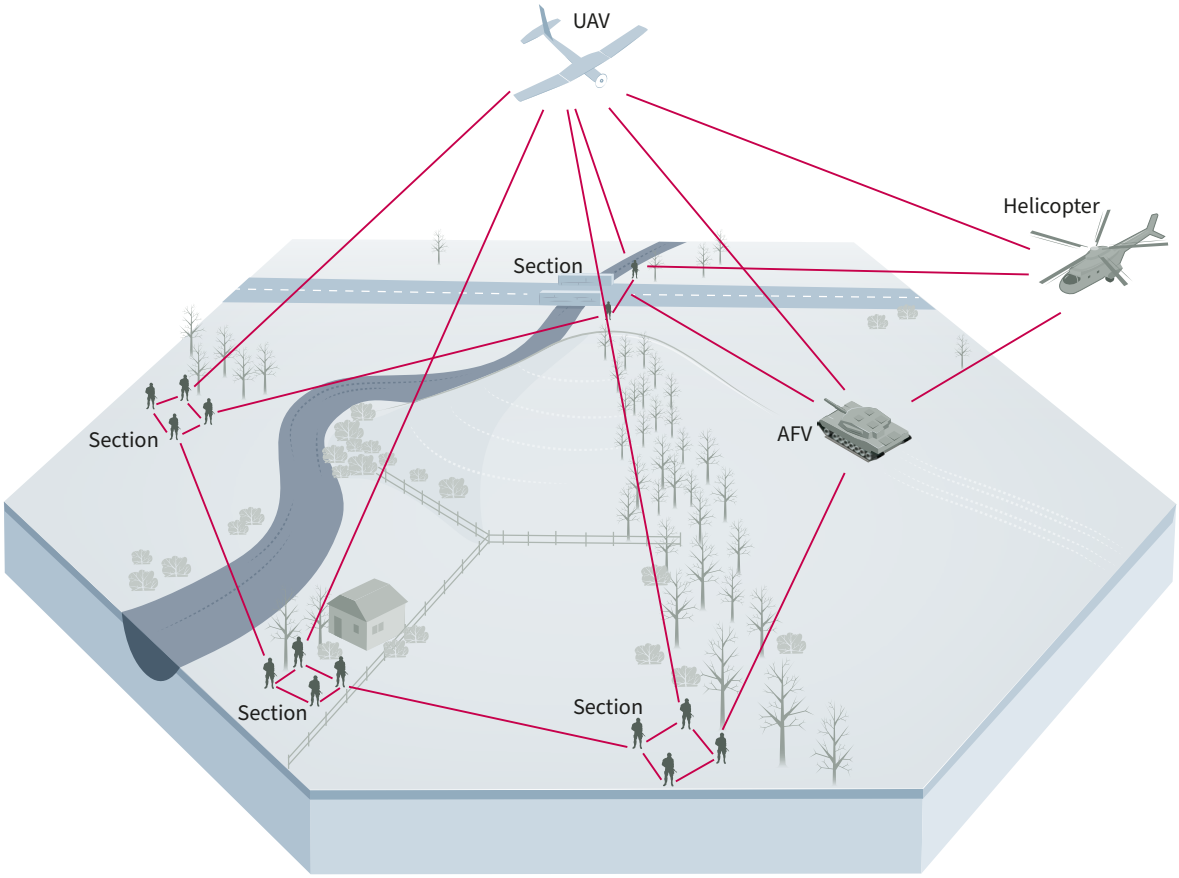
32. Nick Reynolds, 'Getting Tactical Communications for Land Forces Right', *RUSI Journal* (Vol. 166, No. 5, 2021), pp. 64–75.

dissemination of combat-relevant data.[33] Militaries have sought to overcome some of these limitations with hub-and-spoke data management approaches, essentially using key elements of the network as data routers, analogous to a WiFi hub.[34] The challenge with this is that it is limited in its flexibility and has single points of failure, both in terms of survivability and in terms of a bottleneck on routing and bandwidth.

Fortunately, there are technical solutions that are suited to the requirements of modern tactical formations, not least the mobile ad hoc network (MANET).[35] A MANET is a network in which every connected device is also a router. As such, data can be routed dynamically in small packets through any and all available pathways around the network. This has several advantages. When someone authenticates themselves to join the MANET, they become an additional link in the chain, which can wrap around terrain.[36] Because all communications are routed via multiple paths, nothing really stands out in the EMS. The size of each transmission is also reduced, leading to a wide area being covered in an electromagnetic haze, rather than having single points that have a clear behavioural pattern. Moreover, because all nodes are transmitting and receiving, it becomes possible to maintain accurate blue force tracking and to push information rapidly across the network or pull critical data from one point to another. Another critical advantage of a MANET is that it allows for the integration of the battlefield 'Internet of Things', enabling concepts like human–machine teaming.[37] If a force places a sensor in a position, or if a vehicle is autonomously using its sensors to detect and classify objects, these can be shared across a MANET with human operators in real time.

33. Neville A Stanton et al., *Digitising Command and Control: A Human Factors and Ergonomics Analysis of Mission Planning and Battlespace Management* (Farnham: Ashgate, 2009).
34. Note that hub-and-spoke structures are likely more robust at higher echelon. See R Bryce, R Pall and A Ghanmi, 'On Simulating the Resilience of Military Hub and Spoke Networks', IEEE, 2013, pp. 2902–13.
35. Jeroen Hoebeke et al., 'An Overview of Mobile Ad Hoc Networks: Applications and Challenges', *Journal: Communications Network* (Vol. 3, No. 3, 2004), pp. 60–66.
36. Karin Mascher et al., 'NIKE BLUETRACK: Blue Force Tracking in GNSS-Denied Environments Based on the Fusion of UWB, IMus and 3D Models', *Sensors* (Vol. 22, No. 8, 2022), p. 2982.
37. Steven G Spada and Michael T Franco, 'Unmanned Tactical Autonomous Control and Command (UTACC) Command and Control (C2) Framework', Naval Postgraduate School, 2019, <https://upload.wikimedia.org/wikipedia/commons/c/cf/UNMANNED_TACTICAL_AUTONOMOUS_CONTROL_AND_COMMAND_%28UTACC%29_COMMAND_AND_CONTROL_%28C2%29_FRAMEWORK_%28IA_unmannedtactical1094563504%29.pdf>, accessed 10 June 2023.

Figure 1: A MANET Wraps Around Terrain, Integrating People and Crewed and Uncrewed Systems



Source: Author generated.

There are some limitations to MANETs. First, they place the responsibility for configuring and inputting the credentials to join the network on the end user, pushing a training burden to them. Second, MANETs rely on personnel being team players and passing data to others, which means that there is a continuous power draw on all active nodes, limiting endurance. Third, the routing protocols involved are complex and, as the network increases in size, there is a greater risk of it being corrupted or losing functionality.[38] While MANETs may provide a good architecture to replace the company net, therefore, they do not offer a means to connect the whole force. MANETs should enable lateral data fusion within defined geographic boundaries, irrespective of the composition of the force joining the net, but they are a tactical system that is not suited to stitching echelons together.

38. Dimitris Kanellopoulos, 'Congestion Control for MANETs: An Overview', *ICT Express* (Vol. 5, No. 2, June 2019), p. 77.

The ability to rapidly fuse a common operating picture and transfer key information points from one point within a company and its attachments to another offers the kind of situational awareness called for in the previous chapter. If all troops are equipped with software-defined radios, this can be supported by a robust, frequency-hopping mesh against which adversary EW neither has critical identifiable nodes to focus precise effects on nor the agility to carry out blanket denial. Accessing the data available does present challenges. In those forces that have experimented and deployed these kinds of tools, the usual interface is a touch-screen tablet mounted on the chest. This must be robust. It can be difficult to use in high-glare environments, or in cold or CBRN[39] environments where soldiers must keep gloves on. It also poses a risk from a light discipline point of view at night and requires a further draw on power. But these are surmountable problems.

If the MANET allows lateral data transmission to provide the situational awareness necessary for convergence, the question arises as to how detections are to be offboarded to the relevant echelon. Although the two architectures for this method are described later, it is important to identify what should be offboarded. For those platforms with multiple mounted sensors and the ability to have the returns fused for ML interrogation, there should be the ability to disseminate an automatic identification onto the MANET, subject to a human operator's confirmation of the detection. Thus, a symbol can be placed on a coordinate and this data disseminated via the MANET, either with a regularly updated live location if it remains under observation, or indicating a historical detection once contact is lost. Human operators who identify a target could have several options for generating a detection on the system. It would be possible to have a voice-activated command in some circumstances. Alternatively, it would be necessary to create an icon, identify the type of object and drop it on the relevant location, with the object automatically timestamped. This would be viable in a pre-contact situation. Once in contact, operators are likely to avoid focusing on a screen and would either need to use a voice command to the device or verbally announce the detection over the net, to be marked down by members of the company not in contact. The point is that the input at this point constitutes a tiny volume of data comprising the grid reference of the identification, the classification (Red, Green, Blue, White + Pax/IFV/MBT, etc.) and a timestamp for the detection. The same tiny data packet broadcast from each device at fixed intervals could provide live blue force tracking. Thus, offboarding target information does not need to be raw data but rather very small volumes. Some data that is required for key missions, such as radar detection of an air object, cannot function on a periodic basis. For this live track data – relevant only to key nodes such as those associated with air defence or with the ability to offboard

39. Chemical, biological, radiological and nuclear.

data to higher echelons – must therefore be prioritised for transmission across the MANET, and this requires the protocol governing the network to have a built-in bandwidth prioritisation stack. The order of the priorities must reflect the structure of the force and where effectors are held.

The point about time stamping and the half-life of the relevance of detections is worth highlighting as a limitation of such a system. In practice, it would likely be wise to have two layers on the mapping application: one for current (within a defined period) and one for historic detections, with the ability to swipe back through time intervals. This may help to prevent multiple detections of the same unit over time creating the impression of a vast enemy force and other distortions, but there is no complete technological solution to this challenge. It is therefore crucial that operators of such a system are trained to interpret what they can access appropriately. The system may act as an invaluable guide but cannot be wholly trusted. This is especially true in a context where the network may be under EW attack and therefore not function consistently. The overall point is that while technology may enhance capabilities when appropriately exploited, operators must still retain tactical proficiency and use the technology as a force multiplier rather than a crutch.

One of the greatest concerns about a system like the one described above is what happens when a soldier is killed and their body overrun by the enemy or they are captured. First, there is a clear need to be able to rapidly disconnect from the MANET, requiring a re-entry of one's credentials to reconnect. In the case of a dead soldier, it would be necessary for any member of the MANET to be able to eject others from the network. It is also possible that a soldier who is captured may divulge their credentials. We may assume that a soldier must have a radio with the right frequency settings and enter credentials to request to join the network. Thus, there is an immediate two-factor authentication. A third, however, must be used to guard against the case of a soldier captured with their equipment. Here, those already in the network being required to approve joining requests could suffice to secure the network's integrity. This is especially critical because it is important that a user remain credentialled even when they stop receiving or transmitting data, or pause onward data transmission. There are tactical reasons as to why a force may switch to only receiving transmissions or go comms dark. It may be to conserve power, reduce their signature or simply be caused by a break in connection due to terrain. Re-credentialling must be managed on the basis of reconfirmation at intervals, rather than automatically if someone drops off the net, to prevent an unacceptably disruptive process.

Exercising Control Through the Kill Web

The latency between the detection and effect of targets, and the precision and accuracy of strikes, will largely determine lethality on the future battlefield. Moreover, strikes on key targets invariably require exquisite capabilities, whether to find or hit them, and these must be husbanded. So, this part of the force must be under tight, low-latency control. For this to occur, the relevant headquarters must have a detailed understanding of the environment and fuse the returns from stand-off detection directly under its command, wider collection from the force, and the provision of collection from national technical means to prioritise and coordinate effects.

There are two challenges: the structure of the fire control headquarters so that it is survivable within the projected threat environment, and the approach to getting the headquarters the relevant information while disseminating its instructions.

With regard to the process of moving the data, the best framework for understanding how such a network must operate is arguably the kill web.[40] This is an evolution of the kill chain concept: the links by which target information must travel to complete a strike.[41] The kill chain is judged by its efficiency (the fewest possible links) and latency (how quickly it can be completed). The kill web adds agility and therefore resilience to the concept by hypothesising that the information should move via the fastest available route, taking into account that certain routes may be denied at any given time.[42] A further vital feature of the kill web is that although specific jumps within the web may be within line of sight, the end-to-end process is almost always beyond it.

Working from the starting point of the previous section, where companies and their attachments' own battlespace within which lateral communication of detections are transmitted over a MANET, the question becomes how to route the information picked up across the edge and held within these MANETs to the fire control headquarters. First, the fire control headquarters is not interested in all detections. They are interested in key targets, formations and feeds of track-quality actionable information. Defining what constitutes these priority information requirements must be coded into the mission data files that govern how the force's network operates. If a detection marked as a priority in the

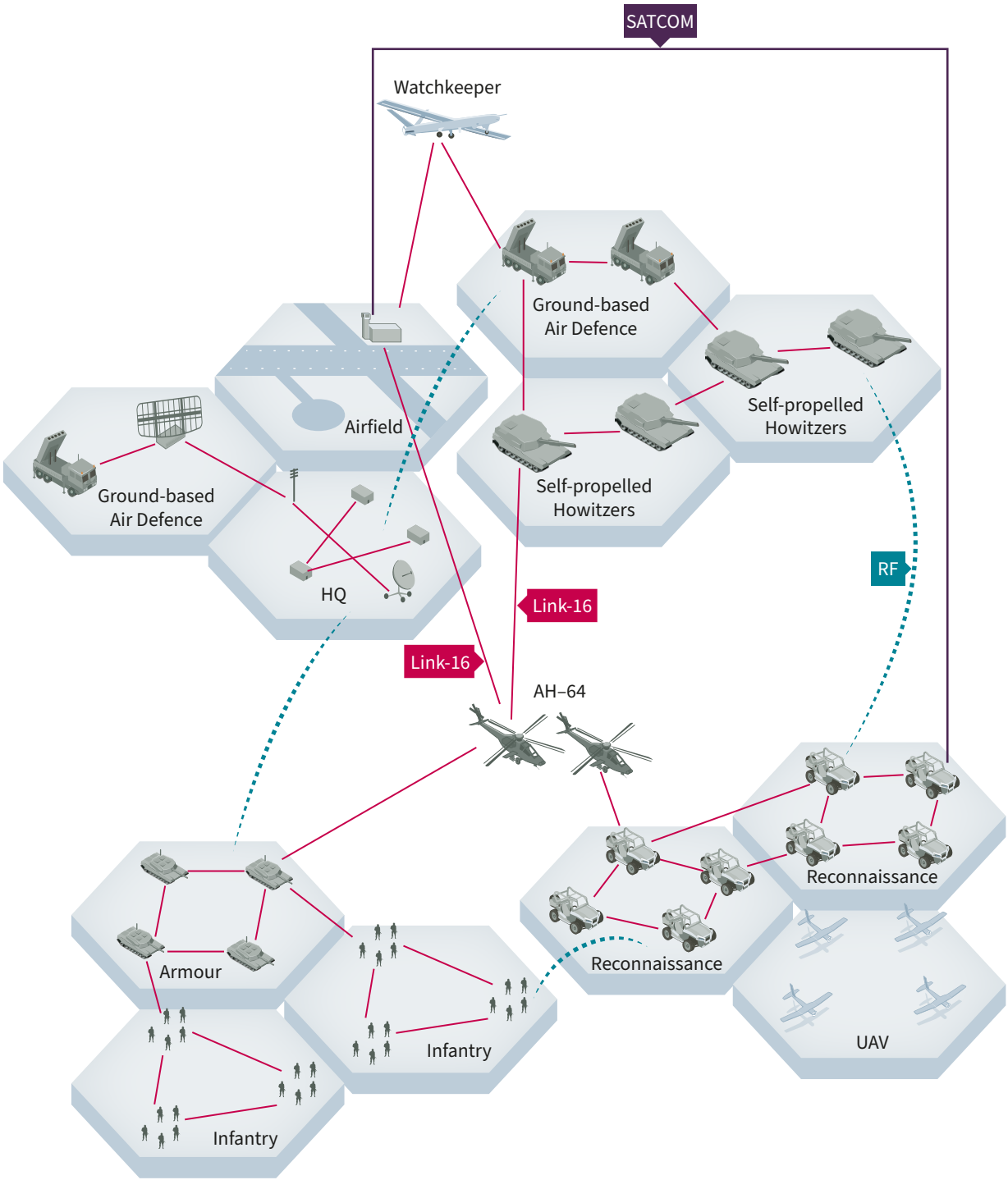
40. Greg Kuperman, 'Adapting Cross-Domain Kill-Webs (ACK)', DARPA, <https://www.darpa.mil/program/adapting-cross-domain-kill-webs>, accessed 20 April 2023.
41. Christian Brose, *Defending America in the Future of High-Tech Warfare* (New York, NY: Hachette, 2020).
42. Bryan Clark, Daniel Patt and Harrison Schramm, 'Mosaic Warfare: Exploiting Artificial Intelligence and Autonomous Systems to Implement Decision-Centric Operations', CSBA, 2020, <https://csbaonline.org/uploads/documents/Mosaic_Warfare.pdf>, accessed 20 April 2023.

mission data files, or data that is flagged as top priority at the edge, enters the system, it must be routed to the point in the MANET where it can be moved onto a different network for further transmission. It must be possible for data to pass between bearers, meaning the data management system should be bearer agnostic. So, the first requirement is that the kill web comprise a heterogeneous network: one that can pass data between operating systems and through different bearers.[43]

The data can jump out of the MANET once it is at a point to be passed upwards. For example, suppose a British Army Wildcat helicopter entered a company's operating area and applied to join the MANET. On doing so, it received a detection shared via the MANET of an enemy manoeuvre element preparing to apply pressure to the company's flank. Here, the Wildcat took this information from the MANET and transferred it to Link-16, allowing the data to be relayed via blue aircraft to the Link-16 terminal in the fire control headquarters. The fire control headquarters could then either direct its own ISR to track the target to set up a fire mission or instruct the Wildcat to do so with its sensors.[44]

43. X Wang, X Li and V C M Leung, 'Artificial Intelligence-Based Techniques for Emerging Heterogeneous Network: State of the Arts, Opportunities, and Challenges', *IEEE Access* (Vol. 3, 2015), pp. 1379–91.
44. Justin Bronk and Samuel Cranny-Evans, 'Building the Capacity to Conduct Joint All-Domain Operations (JADO): Considerations for the UK', *RUSI Occasional Papers*, November 2022.

Figure 2: The Kill Web



Source: Author generated.

This incidental use of additional bearers is one means of strengthening the kill web. However, the company would also need organic means for transmitting data. Suppose that some vehicles in the company had free-space optical (FSO) transmitters and receivers and that the fire control headquarters maintained a

relay UAV above the brigade rear to which FSO comms could be passed.[45] Here, the same process would apply. A detection by the company would be automatically shared with the vehicles able to communicate via FSO as part of the lateral movement of information over the MANET. At this point, it would be transferred automatically to the FSO bearer and transmitter via the relay UAV to the fire control headquarters. Other members of the company might have high-frequency comms or SATCOM to relay back as a reversionary method, albeit with greater latency. Data could be channelled back through many potential pathways. Some detections, like aircraft tracks, need continuous updates and exceedingly low latency to be useful. Thus, there is a need for the prioritisation stack to account for these data requirements in the pathway prioritised when there are higher- and lower-latency paths available.

It is also the case that while distributed sensors may provide non-track quality detections across the front, the fire control headquarters is also likely to have a range of standoff and stand-in sensors under its direct command. These would include capabilities like ground-moving target indicator (GMTI) and air defence radar, as well as longer-range penetrating UAVs. These units would likely have their own low-latency links to the fire control headquarters. Many of these sensors would be tasked to confirm high-priority targets. The fire control headquarters would also draw on data from higher echelons, including national technical means and space-based capabilities. The headquarters must be able to receive data from a wide range of sensor platforms and bearers, accumulating it from:

- Reconnaissance reports.
- Imagery and synthetic aperture radar (SAR).
- EW baselines.
- Radar.
- Signals intelligence (SIGINT).
- Common air picture.
- Open source intelligence (OSINT)/metadata analysis.

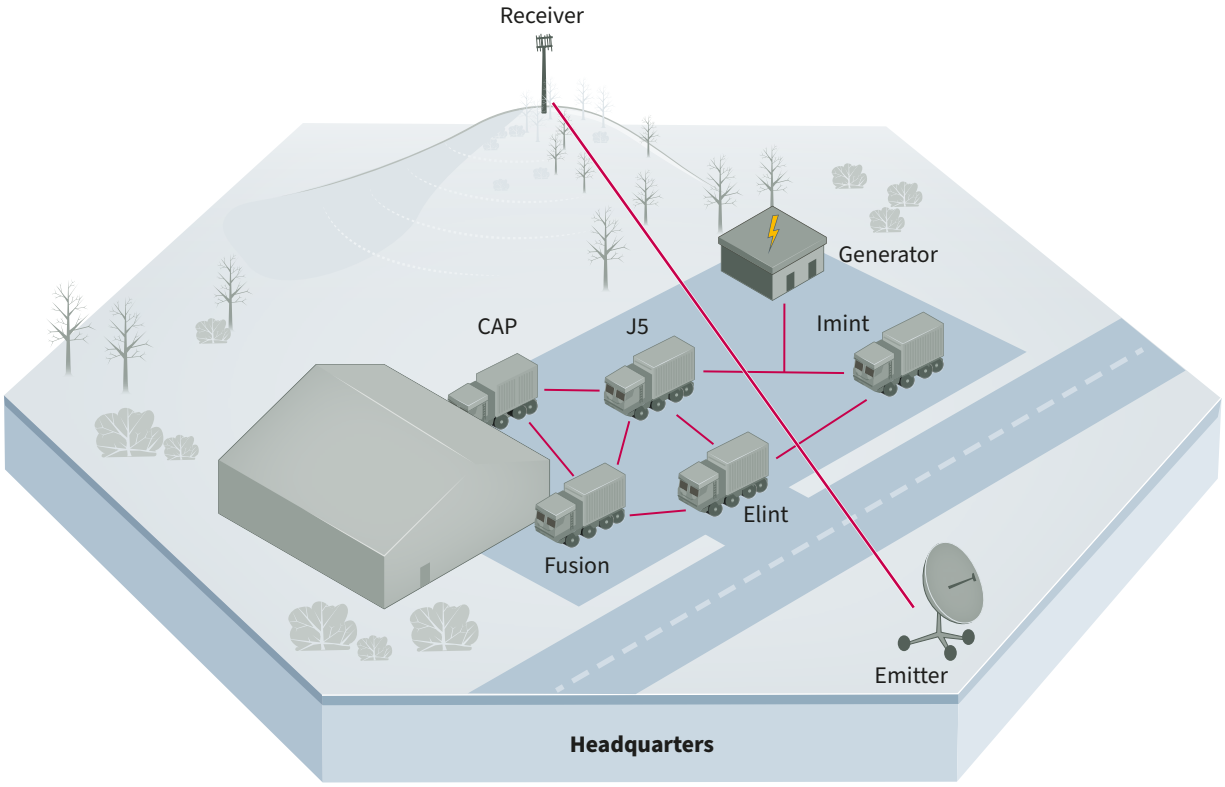
In each case, the force would collect a very large volume of data that – if accumulated – could be plotted and mapped. AI, comparable to Project Maven, could sift each of these data sets separately, providing a classification, location and timestamp. With a team of operators monitoring each feed, these detections could then be fused with AI, cross-referencing the classification, location and timestamp to confirm detections and track them over time. For example, if SAR imagery from space confirmed the location of an air defence radar and a GMTI

45. Kevin Chilton and Lucas Autenried, 'The Backbone of JADC2: Satellite Communications for Information Age Warfare', Mitchell Institute, 2021.

track then started from the location, it could be assessed that the GMTI track was the air defence radar in transit. Upon its going stationary, the system could verify the new position through SAR imagery interrogation.

Once this process is achieved, it should be possible to maintain a map with several layers of detection, including live tracks, confirmed and previous detections, anomalies, and blue and green forces. The headquarters can run two fire control cells from this picture: one for reactive management of time-sensitive effects, including air defence and close-support fire missions, and a second responsible for planning proactive strikes. In total, therefore, assuming that each of the functions described requires processing power, work stations, and a team to liaise with the units supplying the data, assessing and verifying the AI's conclusions, the fire control headquarters could fit into 10 vehicle-mounted ISO containers with seven additional vehicles: one carrying a generator and fuel, one with the headquarters' real-life support, one signals vehicle carrying fibre optic cables to connect the headquarters elements, two transmitters and two receiver masts, able to be set up at a distance from the headquarters. Held at operational depth, the ability to conceal such an arrangement appears eminently feasible. Consider, for example, a group of lorries in a requisitioned supermarket depot or a group of shipping containers. Alternatively, the headquarters could be set up in subterranean working cells.

Figure 3: HQ Laydown



Source: Author generated. Imint = imagery intelligence; Elint = electronic intelligence.

The analytical structure's survivability can be compromised if it emits on a wide range of frequencies. However, the architecture described above envisages the headquarters receiving information on a wide range of bearers but transmitting separately. Transmissions to shooters – completing the kill web – may be divided into lower- and higher-latency sequences. The former demand almost instantaneous direction. This is best achieved with a low probability of detection (LPD) transmission to a relay and down to the battery. Higher-latency activity, like setting up a complex long-range strike, could be distributed via masked satellite uplink. There are a range of options when it comes to the bearer. The point is that it is possible to offset transmissions from the headquarters via fibre optic cable to a transmitter displaced from the headquarters' location, and then to make those transmissions exceedingly hard to detect.

This results in a capacity to draw detections from across the force rapidly via the kill web to a concealable and survivable headquarters, able to obscure its own emissions traffic, and thereby optimally control fires across the force. The use of AI to enable small teams to scrape vast quantities of data, and for these different sets of detections to be fused, should enable the fastest means of coordinating a wide range of both detections and effects. By understanding the range of kinetic and non-kinetic fires being applied, the fire control headquarters

may also issue warnings or orders to units so that they can exploit the impact or take appropriate countermeasures, like bringing down UAVs above their battlespace for the window of time when friendly air is traversing it. In Ukraine, for example, the US XVIII Airborne Corps headquarters could determine whether Russian forces were about to conduct counterbattery or preparatory fires using space-based collection and route these warnings to Ukrainian tactical groups in minutes.[46]

It is these considerations that make proactive and reactive fire control distinct functions, as individuals working out these elements of a strike will be working at a different tempo to an air defence coordination cell.

Although what is described above is highly centralised, some responsibilities could be delegated. For example, if guns were assigned as close-support artillery to a battalion, it would be reasonable for the headquarters to auto-clear approvals for assigned fire missions between the supported and supporting element. Thus, if the battalion loaded a detection onto their MANET and called for fire against it, this request would be routed through the kill web directly to the guns. But this should not be the normal route. First, it denies the headquarters information about the battlefield. Second, tactical echelons are at a higher risk of false positives if they are sensing beyond line of sight, as they have fewer sensor layers to compare. Third, for more capable munitions, of which there are limited stocks, tactical echelons are unlikely to know what is not yet in contact but moving towards them. Nor will tactical echelons fully grasp the severity of their position as compared with others and will therefore expend valuable munitions sub-optimally if given fire control over them. Thus, while appropriate for guns in close support, a centralised fusion process will usually lead to the best results.

Enhancing Command Through the Combat Cloud

The functions of command are very different from the tight and time-bound exercising of control described above, and it does not make sense for command processes to be integrated with control mechanisms. Command is primarily concerned with determining the objectives for units, planning their activity and leading subordinates so that they have the confidence to execute their assigned tasks. If fire control is driven by the need for tempo, command is much more intimately concerned with timing. For example, if a commander decides to send a unit from A to B, their transit will take a fixed amount of time irrespective of

46. CSM XVIII Airborne Corps, LANPAC panel audio.

how quickly the commander can make decisions. The relevant question, therefore, is whether the decision to relocate the unit was made at the appropriate time, not how quickly it was made.[47]

Another important distinction between the processes is that fire control often concerns complicated tasks with lots of precise elements, but the tasks themselves are discrete and readily understandable. Command largely concerns complex tasks, in which a commander must 1) devise a logic to defeat the enemy while the adversary is also in motion and 2) communicate this to subordinates so they can improvise their activities without impeding the overall scheme.[48] This requires more information to be assessed than simply where the enemy is and that information sent to subordinates articulates intent and context rather than just providing a set of instructions. Finally, and in some respects most importantly, the commander holds reserves and supporting capabilities, and they must determine when these resources are expended against what effort. It is important that commanders do not get sucked into the continuous and high-pressure task of exercising control. When they do this, it usually removes them from the place where they can maintain sufficient contextual awareness and analytical detachment to exercise effective judgement. A commander sucked into controlling their force is liable to be led by the nose, or to commit resources against the problem that currently commands their attention, rather than anticipating the problem ahead.[49]

It follows that the communications architecture for command differs from the requirements for exercising control. It is worth considering what must be communicated. First, commanders will wish to distribute orders, summarising what they are asking their subordinates to do – when, where and against what anticipated opposition – and determining the resources available to the subordinate implementing the orders. Second, a commander will wish to provide intelligence support relevant to the operations. This may include schematics of target buildings, assessments of what the enemy is anticipated to be doing rather than just what they are doing now, and contextual information for the subordinate as to their surroundings. Working up these plans takes time. Commanders are not continuously transmitting orders. However, these packages may comprise quite large volumes of data.

The commander also requires key information to conduct their planning. They must have a reasonable picture of the battlefield, including the status and position

47. Nick Reynolds, 'Performing Information Manoeuvre Through Persistent Engagement', *RUSI Occasional Papers*, June 2020, pp. 37–43.
48. Lawrence Freedman, *Command: The Politics of Military Operations from Korea to Ukraine* (London: Allen Lane, 2022).
49. Anthony King, *Command: The Twenty-First Century General* (Cambridge: Cambridge University Press, 2019).

of friendly units and the known and assessed locations of enemy units and what they are trying to do. They need their own orders, require an accurate picture of their supply situation and must be able to feel their troops' morale. This creates an interesting set of architectural challenges. Commanders must circulate the battlefield as leading requires face-to-face engagement.[50] To exercise judgement, they not only need information to be accumulated; it must be presented to them in a comprehensible manner and they should have time to consider the issue. Their decision-making tempo is therefore likely to be inconsistent, and the location from which they may need to exercise judgement is also not fixed. Another interesting aspect is that those receiving the orders require time to understand them, and this interaction is not a constant activity but likely one dependent on their availability based on the tactical situation and conducted at intervals. The fact that a commander must be mobile, but their large, dispersed staff cannot accompany them, creates a requirement for information to be transmitted and received at irregular intervals, and ideally for the recipient to determine when they receive the information and the sender to determine when they send it.[51]

The communications architecture that arguably best supports such a system is the combat cloud, the concept of a remotely accessible data repository.[52] Access to that repository could be achieved through a range of means, but satellite communication would offer a high-bandwidth, medium-latency, dependable, maskable and resilient way of uploading information to a shared environment and downloading it. Access to information within the cloud would need to be compartmentalised according to the authorities and permissions of the individual accessing it, and the individual would need to prove their credentials to access the information within their compartment. Nevertheless, such a system would allow components of a staff to produce their annexes while working in separation, for this to be downloaded and cohered by the principal planning group, uploaded, and distributed to subordinate units. It would also be possible to push supporting data like relevant imagery, mapping or J2 assessments forwards with these orders packs. For the forces required to implement these orders, they could be downloaded when a unit commander has the opportunity to access the repository. Once the data is brought onto the commander's computer, associated layers of mapping, arrows and times could be distributed over the MANET to be available on each soldier's interface. Such a model allows different parts of the headquarters to be situated at any distance, including support functions in the home base.

50. Howard L Ware, *Command Presence: Where Should the Operational Commander be Located on the Modern Battlefield* (Fort Leavenworth, KS: School of Advanced Military Studies, 1989).
51. This is driven by the EW threat. See Bryan Clark, Whitney McNamara and Timothy Walton, 'Winning the Invisible War: Gaining an Enduring U.S. Advantage in the Electromagnetic Spectrum', CSBA, 2019.
52. Jacob Hess et al., 'The Combat Cloud: Enabling Multi-Domain Command and Control Across the Range of Military Operations', Wright Flyer Paper No. 65, Air University Press, 2017.

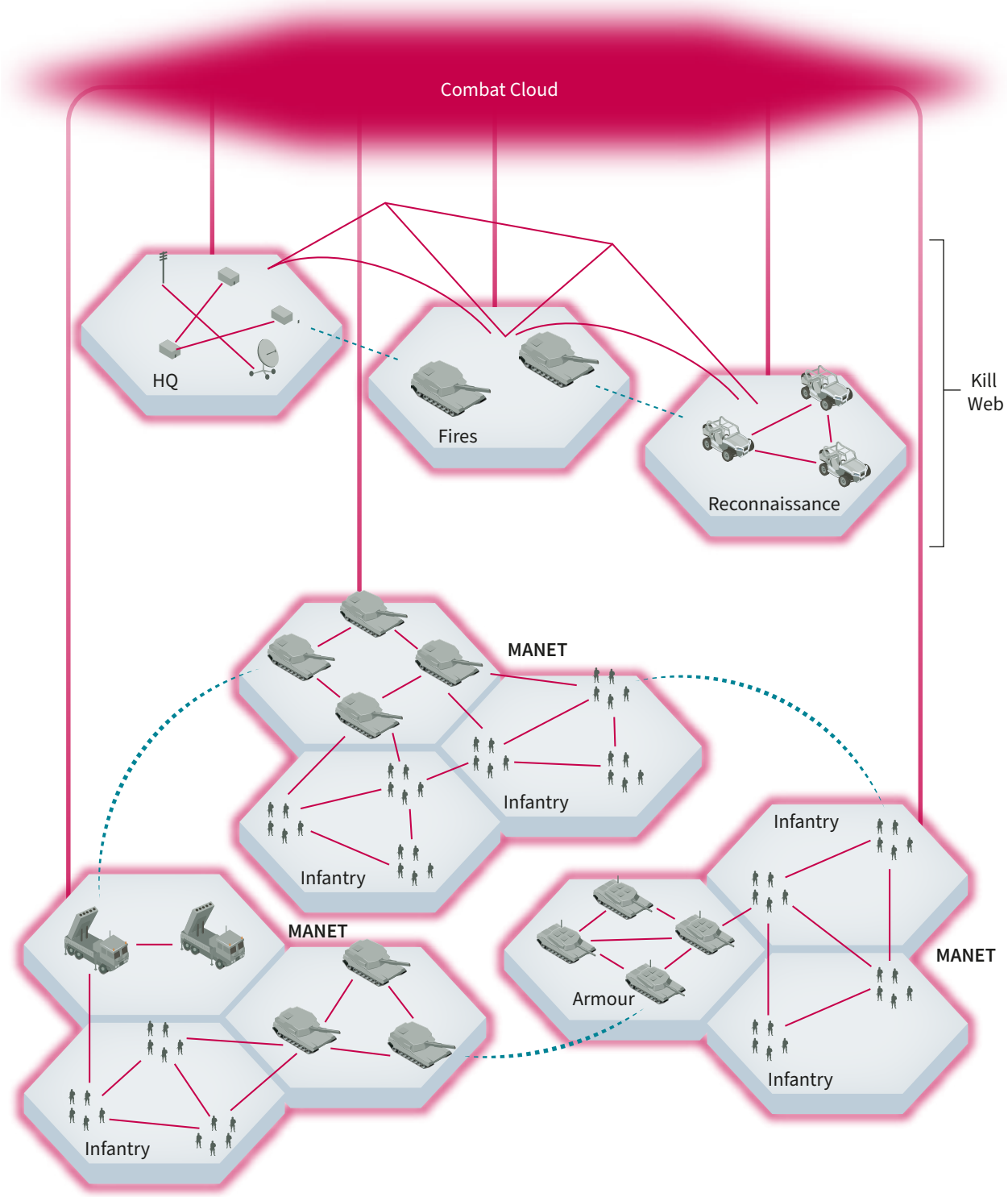
The robustness of this approach has been demonstrated in Ukraine through the use of Starlink terminals.[53]

Historically, the personalisation of briefing annexes to orders would have been impossible for a staff because of the time required as compared to the staff available. However, most of the data for generating these kinds of personalised information packs is generated collaterally during planning. Converting that data into packs is a feasible task for AI, ensuring that a commander's intent is translated into clear visual instructions at each echelon, with the supporting written orders available to understand the 'what' and the 'why'. The mechanisms for this are already visible with ChatGPT when it is used appropriately under supervision.

Flowing in the other direction, the higher latency with which the headquarters needs to accumulate data to inform planning as compared with the short timeframes necessary for effective control can also allow reports and raw material to be uploaded when there is slack capacity in the network to avoid saturating the net. Thus, the headquarters should be able to accumulate a continuous stream of information from the battlefield, albeit with some lag between collection and receipt that would differ depending on the intensity of activity at the tactical edge. It is also reasonable to assume that the headquarters would be passed information from the fire control headquarters' fusion cell as and when there was slack capacity on the kill web.

53. *The Economist*, 'How Elon Musk's Satellites Have Saved Ukraine and Changed Warfare', 5 January 2023.

Figure 4: Integrating the Three Networks



Source: Author generated.

To give a tangible example of how this system could work, consider a logistics unit of four trucks waiting in a hide. They check in to the combat cloud via a satellite link at an agreed interval and receive an order to move to a cache position

and pick up four shipping containers containing combat loads for a forward element and fuel. The most direct route to the caches' location is attached to the orders and automatically populates onto the tactical interface in the vehicles. The logistics packet closes the satellite link and leaves its hide, reaching the cache and scanning a QR code on the shipping containers as they are drawn onto the trucks. The commander then reconnects via satellite to upload the time and place with the shipping container's serial number and begins their route to the handover point with the element they are supporting. A pair of reconnaissance vehicles that had been simultaneously tasked with moving to the front join the packet as it moves forwards, having similarly received instructions. On entering the battlespace owned by the unit they are tasked with resupplying, the logistics group would request to join the MANET, indicating its presence and connecting to coordinate a point to cache the material. Once this was indicated by the receiving unit, the logs group could proceed to the coordinates that the unit commander marked on their tactical interface and cache the pallets from their containers. Following this, the logistics element could scan the QR code on the container, picking up its location, status and timestamp, and attach an indication that the load was now empty, distributing this over the MANET to the unit commander so that they know the supplies are cached and ready to be retrieved. At the same time, the situation report (SITREP) would enter the priority stack in the MANET to be uploaded to the combat cloud when a connection and bandwidth became available, so that the operational headquarters would receive confirmation of mission success and an update on the unit's supply status. This would also indicate that the logistics element was available for tasking again. Because the cache point would be distributed across the MANET, units would know that protecting this point was important. So, attached elements like counter-unmanned aircraft system operators could have the knowledge to converge their activities to keep the area out of enemy observation.

III. The Changing Practice of Command

The architectures in the previous chapter have continuities and differences when compared with the existing communications that land forces use. Because the differences directly connect parts of the force that would have previously been separate, command relationships that would have been manifestly inefficient before are created. The consequences can be positive or negative depending on how the culture of command interacts with these opportunities. This chapter, therefore, seeks to outline some of the changes in behaviour and mindset that are necessary to exploit the system's potential.

Command Discipline

The structure outlined above effectively breaks down the echelon structure as regards C2, as it becomes possible for the operational headquarters to issue direct orders to any part of the force while the force can call for effects from the fire control headquarters. Whereas the current hierarchical communications architecture would require orders at division to be disseminated to commanders, staffs and subordinates in that order, the outlined architecture would enable the division to issue orders to any required level.

This is dangerous. Suppose, for example, that the divisional commander feels uncomfortable with a gap in collection in the battlespace. Under the old architecture, an instruction to prioritise collection against this area would lead the staff to assess what assets remained uncommitted. Then, they would either task them or instruct a subordinate commander responsible for the battlespace containing the gap to adapt their dispositions. It would be for the subordinate to balance their responsibilities, and if they felt that covering the gap would endanger their existing instructions, they could ask the divisional commander for more resource or clarification of intent as regards the balance of risk to be taken and the prioritisation of tasks. Meanwhile, none of these deliberations would be known to the reconnaissance units being discussed who could therefore continue to focus on their assigned tasks. By contrast, it would be entirely possible under the new system for the divisional commander to see the laydown of the reconnaissance troops, select a unit and issue it orders to shift focus. This would solve the commander's problem – apparently improving efficiency – without the

reconnaissance troops' commanding officer being aware of what their subordinates are now doing or why. Moreover, having insight into the tactical fight risks higher headquarters becoming obsessed by and drawn into tactical issues, losing focus on the operational questions that should be their area of responsibility.[54]

This ability to reach around echelons is necessary because a strictly hierarchical C2 architecture is vulnerable and would not facilitate efficient data movement. However, it risks being disruptive without appropriate discipline from commanders. Another aspect of this risk is that it is entirely possible for a senior commander to saturate the force's capacity. The fidelity of modern sensing should mean that an operational commander can get almost any question they ask about the physical disposition of enemy forces answered. However, this will likely draw on a range of assets whose returns must now be prioritised by the network and which are likely unavailable to carry out other tasks. It would therefore be easy for a commander to demand collection against too many targets and, in doing so, saturate the network and exhaust the available assets. Again, the risk is that the higher staff begins to interfere with the planning and execution of these activities to optimise them and becomes drawn into tactical decision-making to answer tactical questions. The question of how good a spectator the commander is arises as a result.

Used properly, the architecture described above offers significant benefits. For example, suppose a commander, through higher echelon collection, observes that the enemy is planning on thrusting a wedge along the unit boundary between two subordinate formations. First, the higher headquarters can pass this information to the subordinates, giving them the situational awareness to account for the threat. Second, the commander now faces a decision point as to whether to deploy reserves to bolster the sector or commit other assets like attack aviation to blunt the threat, thereby directly supporting the subordinate formation. Most importantly, understanding the supply status and disposition of friendly and hostile forces, the commander can plan what to do after the immediate set of fights. Ensuring that the opportunities the command architecture presents are appropriately supported demands training and the development of a culture of command that distinguishes between and separates out command from control, so that officers do not feel the need to exercise control to be in command.

54. Eitan Shamir, *Transforming Command: The Pursuit of Mission Command in the US, British, and Israeli Armies* (Stanford, CA: Stanford University Press, 2011), pp. 67–81.

Disaggregated Collaboration

The architecture described in the previous chapter is intended to make command, not control, agnostic of distance to ensure survivability. Within this, it is eminently feasible for information from the battlefield to be aggregated in the homeland, fused with national collection and made available to the operational headquarters' J2 shop. The latter may be working across two or three concealed locations (like underground car parks) in the corps rear and used to form briefing packs addressing the allocated commander's information requirements. These might then be uploaded from the J2 cell and downloaded by the J3/5 cell in another location before being attached as annexes to the courses of action presented to the commander and their principal planning group, who might be in a mobile command post of two or three vehicles, carrying out battlefield circulation. This is not an optimal way of working and creates several frictions.[55] Getting everyone on the same video teleconference at regular intervals is also likely to be unviable under this architecture. While it may be possible at irregular intervals depending on the situation, it cannot be relied on. The driver for this disaggregation is survivability, not efficiency. Nevertheless, as was demonstrated during the Covid-19 pandemic, such an approach is feasible even if not ideal.

One of the challenges in disaggregated working is that when a system has an uneven and potentially disrupted tempo, it is possible for parts of the structure to be bypassed or forgotten. Suppose, for example, that a commander has an incidental question about something in their briefing pack relating to the enemy's assessed intent. If the headquarters was physically co-located, the J2 cell would likely field this question. However, if contacting the J2 cell requires submitting a question via technological means, and there is a lag in their receiving the request and answering, then in many instances the inclination will be for the command group to use their best judgement and move on without consulting them at all. Here, there is a risk for the J2 cell that the absence of questions suggests an absence of demand: if the team goes quiet under this assumption, they will receive fewer requests over time.

Overcoming the risk of progressive isolation requires an entrepreneurial culture in staffs and across the force. This is very different to mission command, which concerns the ability to continue pursuing a commander's stated intent despite an absence of supervision or control. Entrepreneurialism is a capacity to examine the situation and determine what is to be done in the absence of clear direction.[56]

55. Anita L Blanchard, 'The Effects of COVID-19 on Virtual Working Within Online Groups', *Group Processes & Intergroup Relations* (Vol. 24, No. 2, 2021), pp. 290–96.
56. A description of how difficult this can be and the frictions it creates is contained in Cedric Delves, *Across an Angry Sea: The SAS in the Falklands War* (London: Hurst and Company, 2018), pp. 17–40, 111–54.

The relevance here is that a part of the C2 architecture may have fulfilled its role in the process and delivered against intent. The question then becomes 'what can this component do to further the work of others, to strengthen their situational awareness, bolster their capacity and remain connected?'. The post most likely to be disrupted by this process is the chief of staff, as they can no longer function as an orchestra conductor. Instead, they become more like a jazz band's sound technician, balancing the levels to ensure that all components align.

Trust in the Machine

The prospect of drawing one's commands from the cloud, compiled by a disaggregated staff spread throughout operational depth, risks making it profoundly impersonal. Moreover, although staff at higher echelon may have a high-fidelity picture of the battlefield, they are separated from its texture. The risk is that subordinates come to distrust their superiors' decisions, feeling a lack of connection and the absence of shared risk. Battlefield circulation may help, but ensuring the continuity of trust also requires that subordinates who feel they need clarification or additional engagement regarding instructions can reach for it. Knowing that this is possible in itself likely alleviates the need for its use, but commanders and staffs must be empathetic to the personal connection that underpins trust between those in harm's way and those directing operations.[57]

The trust issue is even more important when it comes to AI.[58] Trust in AI is eminently possible. How often, for instance, do people independently corroborate that Citymapper and other route planning services actually offer the optimal course of action? The AI uses described in this paper – including route planning and the generation of staff work, bandwidth and data prioritisation, and sensor data fusion – all offer a substantial increase in efficiency but only if users trust these systems.

There are barriers to this trust in a military context, including the consequences of failure and the unreliability of connectivity (and thus the available data on which a system is basing judgements). Theorists have also put forward unrealistic expectations, such as the need to be able to understand how an AI is making judgements,[59] or the idea of having a human in the loop.[60] The former is not possible because of the training burden involved. The latter defeats the whole

57. Maria Fors Brandebo et al., 'Trust in a Military Context: What Contributes to Trust in Superior and Subordinate Leaders?', *Journal of Trust Research* (Vol. 3, No. 2, 2013), pp. 125–45.
58. Christina Balis and Paul O'Neill, 'Trust in AI: Rethinking Future Command', *RUSI Occasional Papers* (June 2022).
59. David Beer, 'Why Humans will Never Understand AI', *BBC*, 7 April 2023.
60. Jovana Davidovic, 'What's Wrong with Wanting a "Human in the Loop"?', *War on the Rocks*, 23 June 2022.

purpose of the efficiency gains achievable through AI. There are some processes where a human must exercise judgement, but there are many where they may observe and only interfere if they judge there to be something wrong.[61]

The issue of trust can be managed in two ways. First, there is a need for AI tools to have a very specific purpose and for the outcome to be something that the operator can judge the success of. They need not understand how a result was reached, but if the result is clear then its accuracy will build confidence and the ability to perceive inaccuracy will also reassure. For planning purposes, this does require effective training for users as to what problems a particular AI tool will be effective at and how it is to be used. To take ChatGPT as an example, it can be a very useful tool if used properly for certain tasks. It can also prove highly misleading when used inappropriately for other tasks or if it is assigned to the wrong one. Training staff on employing these tools is important if they are to avoid having their confidence in the system damaged. A second requirement is that AI tools degrade gracefully and transparently. That is to say that when dependencies are not available, the user must be made aware that the tool is now functioning in a degraded state and understand how this may alter its use.

Another trust issue relating to the architecture described in this paper is that of assurance. Cyber attacks are a constant threat and, when combined with EW, are liable to suppress, disrupt and potentially compromise parts of any architecture. If the user comes to believe that their system is compromised or has been interfered with, their confidence in it will collapse, which could have a negative effect on the system's functioning that is entirely disproportionate to the actual direct consequences of a compromise or penetration. An organisation therefore needs to be actively protected by cyber defence specialists. It is also important that staff understand the scale and persistence of attacks on the network so that they do not expect a perfectly secure system, but rather a sufficiently secure and robust one to be depended on even if there are occasional disruptions. This requires a shift in how security is understood from something absolute to something partial. Establishing unrealistic expectations risks a breakdown of trust in the system.

The EMS as a Plane of Manoeuvre

Legacy approaches to C2 tend to view signals as a support function, to have a primary mode of communication and to revert to a series of less efficient but

61. Saeid Nahavandi, 'Trusted Autonomy Between Humans and Robots: Toward Human-on-the-Loop in Robotics and Autonomous Systems', *IEEE Systems, Man, and Cybernetics Magazine* (Vol. 3, No. 1, 2017), pp. 10–17.

more assured methods depending on the level of enemy interference. Furthermore, the instinct has been to minimise transmission to maintain concealment.

This paper has essentially argued that the level of sensor fidelity on the modern battlefield makes concealment a highly temporary state. The extent to which being detected exposes a force to risk depends on whether the enemy can manoeuvre the information to the relevant effector and the confidence of their identification of the detection. This can be combated with EW and constraining the relevance of the information through displacement. However, both of these actions have an associated signature, which perpetuates the enemy having sensor returns on the formation. The force best able to share its information will ultimately have a competitive advantage.

A further proposition in this paper has been that communications must be assured; not through a sequential PACE (Primary, Alternate, Contingency, Emergency) stack, but through bearer-agnostic data transfer to evade interference. Frequency hopping for line-of-sight communications can achieve this at the tactical level. For the kill web, using a range of different bearer pathways can help to achieve this. For the combat cloud, survivability is achieved by removing the requirement for both parties to be connected at the same time, thereby temporally evading disruption. It is nevertheless likely that an adversary can disrupt elements of these networks for limited periods of time, albeit at a significant cost in resource. In this context, the EMS must be understood as a manoeuvre environment – one that is actively contested and through which each side tries to assure its own links while denying the enemy's.

As regards the culture of command, these dynamics require a commander to articulate when and where they wish to prioritise the resources of their signals troops and where they determine the balance in utility between assured communication and signature management. Perhaps most importantly, a commander should not assume that a force will function on EMCON black – without comms – until in contact or on primary communications until this channel is disrupted. The former risks the force being severed from situational awareness and therefore being outmanoeuvred. The latter risks the force being shaped and targeted as its comms plan degrades through a predictable series. Instead, the assumption should be that the force will communicate dynamically, manage active disruption and try to preserve ambiguity rather than concealment as to its dispositions. The concentration of EW effects or shifting to EMCON black may provide a period where the enemy loses understanding of the battlefield and therefore achieves a shaping effect that may offer advantage. Similarly, if the force is dominating the other, then it can likely increasingly shift to a steady state of communications comparable to primary comms. Within this context, it is important that signals troops are involved in developing the scheme of

manoeuvre and can advise on the options available to a commander as to when certain effects can be applied and when risk must be taken.

A final element in understanding the EMS as a plane of manoeuvre is in using the tools described in this paper as a force multiplier rather than a crutch. Situational awareness offers competitive advantage, but access to it will be disrupted. Troops can devote effort to improving access, but if they lack it, it is critical that they do not stop operating in anticipation of its return. Instead, they must revert to appropriate tactics in periods of limited connectivity. It is this skill that offers the force resilience. Resilience is not about having a perfect system that operates optimally all the time; rather, it reflects the capacity for operators to maximise a system's utility when it is operating imperfectly. This increased signals literacy likely creates a force generation challenge. An increased number of signallers at tactical echelons, however, offers troops both situational awareness in the EMS, and the means to fight for connectivity. The move of signallers from a support function to a key part of the combined arms manoeuvre system also requires an adjustment to culture.

Conclusion

For the past 30 years, almost all military concepts have aspired to bring data to the battlefield. Concepts like network-centric operations and systems confrontation warfare have emphasised targeting enemy networks to secure advantage. At the same time, programmes like the US's Joint All-Domain Command and Control,[62] or Russia's striving to build a unified digital fire control architecture through Akatsiya,[63] are all premised on mass data fusion and dissemination around the force. But the lived experience of operations has been rather different. In Afghanistan, in the absence of a contested EMS, it took years to give troops full motion video from their supporting UAVs. Data fusion was achieved through the deployment of hundreds of analysts to combat theatres. Actually deployed in combat, meanwhile, Russia has found its operators unable to employ its modern communications systems proficiently.

There is a significant gap between theory and practice. This is not to say that communications have not improved over this period, but rather that the fielding of new communications equipment has been laborious, uneven and often resulted in a like-for-like replacement of older systems, with the force slowly adapting to exploit its potential. For example, 3 UK Division headquarters has a Link-16 terminal, largely used by its air defenders. However, while data from this terminal could be an invaluable source of situational awareness from a range of air assets, it is rarely integrated into wider targeting and planning cycles.

This paper did not aim to provide a technical evaluation of the range of ongoing attempts to modernise parts of military communications. Instead, it has posited a set of drivers and the architectural responses to seizing the available opportunities that modern technology offers while mitigating emerging risks. One clear conclusion is that there is not one architecture; instead, there are at least three, differentiated by how data enters, is prioritised and moved within the system. Furthermore, the function of command is distinct from the exercising of control and requires a different architecture. A third requirement is to maximise situational awareness laterally between tactical echelons so that subordinates exercising mission command can dynamically converge effects.

62. John R Hoehn, 'Joint All-Domain Command and Control: Background and Issues for Congress', Congressional Research Service, 18 March 2021, <https://crsreports.congress.gov/product/pdf/R/R46725/2>, accessed 19 April 2023.
63. Lester W Grau and Charles K Bartles, 'The Russian Reconnaissance Fire Complex Comes of Age', Changing Character of War Centre, University of Oxford, May 2018, <https://static1.squarespace.com/static/55faab67e4b0914105347194/t/5b17fd67562fa70b3ae0dd24/1528298869210/The+Russian+Reconnaissance+Fire+Complex+Comes+of+Age.pdf>, accessed 19 April 2023.

Separating out the functions simplifies network requirements in a way that makes it possible to fulfil them using technologies that are already mature. The three architectures identified in this paper (MANETs supporting tactical formations, a heterogeneous kill web for control of the fires system, and a combat cloud for the command of the force) are all realisable. However, establishing such a system requires adjustment to training and culture in how command is exercised. Commanders must be more disciplined and avoid interfering where the system gives them access to tactical activity. Headquarters must become better at disaggregated collaboration and being entrepreneurial, not work to a rigid tempo. Trust must be established between the AI support tools required to make this system work and the personnel employing them. This means staff officers need to be trained in how to leverage these tools and understand how they can be misused. It also requires AI tools to be closely tied to achieving specified outputs that can be understood, even if the AI's workings cannot. The force must also be able to trust the resilience and assurance of the network even as it is contested, through graceful degradation and appropriate training to operate without strong connectivity. This requires active cyber defence. It also demands a more manoeuvrist approach to understanding the EMS, appreciating that interference is likely continuous and an issue to be actively combated, rather than an imposition triggering predictable procedures.

A significantly reduced C2 footprint and increased survivability are possible if the architectures described in this paper are realised. Situational awareness would likely also significantly increase the ability of the force's components to act as force multipliers to one another, even while operating in a dispersed posture. Finally, a force using such an architecture would be able to maximise the effectiveness of its fires and maintain a high-fidelity sensor picture of the battlefield, leveraging sensor density across modern militaries. What is described is eminently possible; the question is whether forces have the agility in their procurement processes to seize the opportunity.

About the Author

Jack Watling is Senior Research Fellow for Land Warfare at RUSI. Jack 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.

Jack's PhD examined the evolution of Britain's policy responses to civil war in the early 20th century. Jack has worked extensively on Ukraine, Iraq, Yemen, Mali, Rwanda, and further afield. Jack is a Global Fellow at the Wilson Center in Washington, DC.

Originally a journalist, he has contributed to *Reuters*, *The Atlantic*, *Foreign Policy*, *The Guardian*, *Jane's Intelligence Review*, *Haaretz* and others. Jack was shortlisted for the European Press Prize Distinguished Writing Award in 2016 and won the Breakaway Award at the International Media Awards in 2017.