

WHITE PAPER

LESSONS FROM UKRAINE AND BEYOND

Rethinking MOD CIS Procurement for
Resilience, Integration and Adaptability



Meeting Your Mission. With Passion.



EXECUTIVE SUMMARY

The war in Ukraine has fundamentally challenged many of the assumptions that have underpinned Western military communications for the past two decades. Command-and-control systems are no longer operating in environments characterised by assured connectivity, uncontested spectrum access and reliable infrastructure. Instead, communications networks are continuously targeted through electronic warfare, cyber intrusion, kinetic strike, signal intelligence collection and deliberate interference. Recent operations in the Middle East further reinforce this trend, demonstrating how modern military forces increasingly integrate cyber effects, long-range fires, unmanned systems and information operations into a coherent, multi-domain campaign.

For the Ministry of Defence (MOD), the critical lesson is not simply that communications systems require modernisation. The deeper lesson is that traditional approaches to Communications

and Information Systems (CIS) procurement are increasingly misaligned with the realities of contemporary warfare. Future operational effectiveness will not be determined by the performance of individual communications systems operating in isolation. Rather, it will be determined by the resilience, adaptability and integration of the overall communications architecture.

Current MOD CIS capability remains highly capable in many areas. However, challenges persist around interoperability, rapid integration of commercial technology, operation within contested electromagnetic environments, resilience under electronic attack and the provision of a common operating picture across multiple echelons and coalition partners. The pace of technological change is also significantly faster than traditional acquisition cycles, creating a growing risk that military communications architectures struggle to adapt as rapidly as operational requirements evolve.



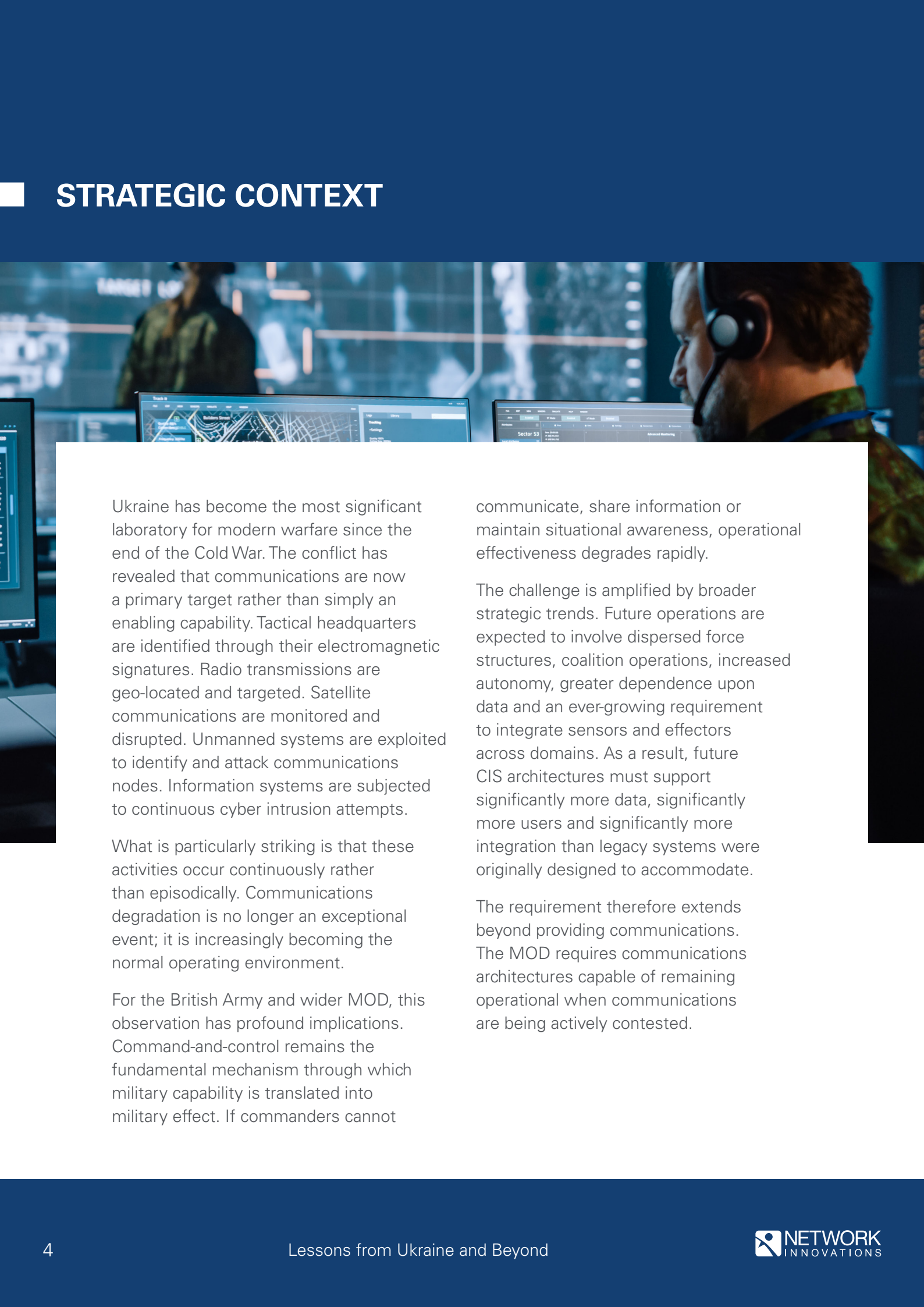
This white paper assesses five technologies that collectively offer potential solutions to many of these challenges:

- **Intellian OW7, OW10 and OW11** deliver resilient beyond-line-of-sight (BLOS) satellite communications for distributed command nodes and mobile headquarters.
- **Peplink** enables network orchestration and bearer aggregation, maintaining connectivity when individual networks are degraded or lost.
- **Team Awareness Kit (TAK)** provides a shared operational picture, integrating locations, sensors, intelligence, mission overlays and operational data into a single environment.

- **Somewear Labs Trackers** extend situational awareness with tracking and messaging capabilities for personnel operating beyond traditional network coverage.
- **EW Scan, Replicate and Deny** capabilities (0-6 GHz) enable forces to detect, map, influence and disrupt the electromagnetic environment on which modern operations depend.

Individually, each capability addresses a specific operational challenge. Collectively, they represent the foundations of a more resilient, integrated and adaptable communications architecture aligned with emerging MOD concepts such as Multi-Domain Integration, Digital Backbone and Federated Mission Networking.

STRATEGIC CONTEXT



Ukraine has become the most significant laboratory for modern warfare since the end of the Cold War. The conflict has revealed that communications are now a primary target rather than simply an enabling capability. Tactical headquarters are identified through their electromagnetic signatures. Radio transmissions are geo-located and targeted. Satellite communications are monitored and disrupted. Unmanned systems are exploited to identify and attack communications nodes. Information systems are subjected to continuous cyber intrusion attempts.

What is particularly striking is that these activities occur continuously rather than episodically. Communications degradation is no longer an exceptional event; it is increasingly becoming the normal operating environment.

For the British Army and wider MOD, this observation has profound implications. Command-and-control remains the fundamental mechanism through which military capability is translated into military effect. If commanders cannot

communicate, share information or maintain situational awareness, operational effectiveness degrades rapidly.

The challenge is amplified by broader strategic trends. Future operations are expected to involve dispersed force structures, coalition operations, increased autonomy, greater dependence upon data and an ever-growing requirement to integrate sensors and effectors across domains. As a result, future CIS architectures must support significantly more data, significantly more users and significantly more integration than legacy systems were originally designed to accommodate.

The requirement therefore extends beyond providing communications. The MOD requires communications architectures capable of remaining operational when communications are being actively contested.

EXPANDING BEYOND UKRAINE: GLOBAL LESSONS FROM CONTESTED WARFARE

While Ukraine provides the most visible and data-rich example of contested communications, similar lessons are emerging across other regions. Recent operations involving Iran and Israel have highlighted how cyber operations, long-range precision strike, electronic warfare, space-enabled communications and information operations are increasingly integrated into a single campaign. Communications systems are targeted not only through electronic attack but also through kinetic action against command nodes, data centres, critical infrastructure and communications relay points.

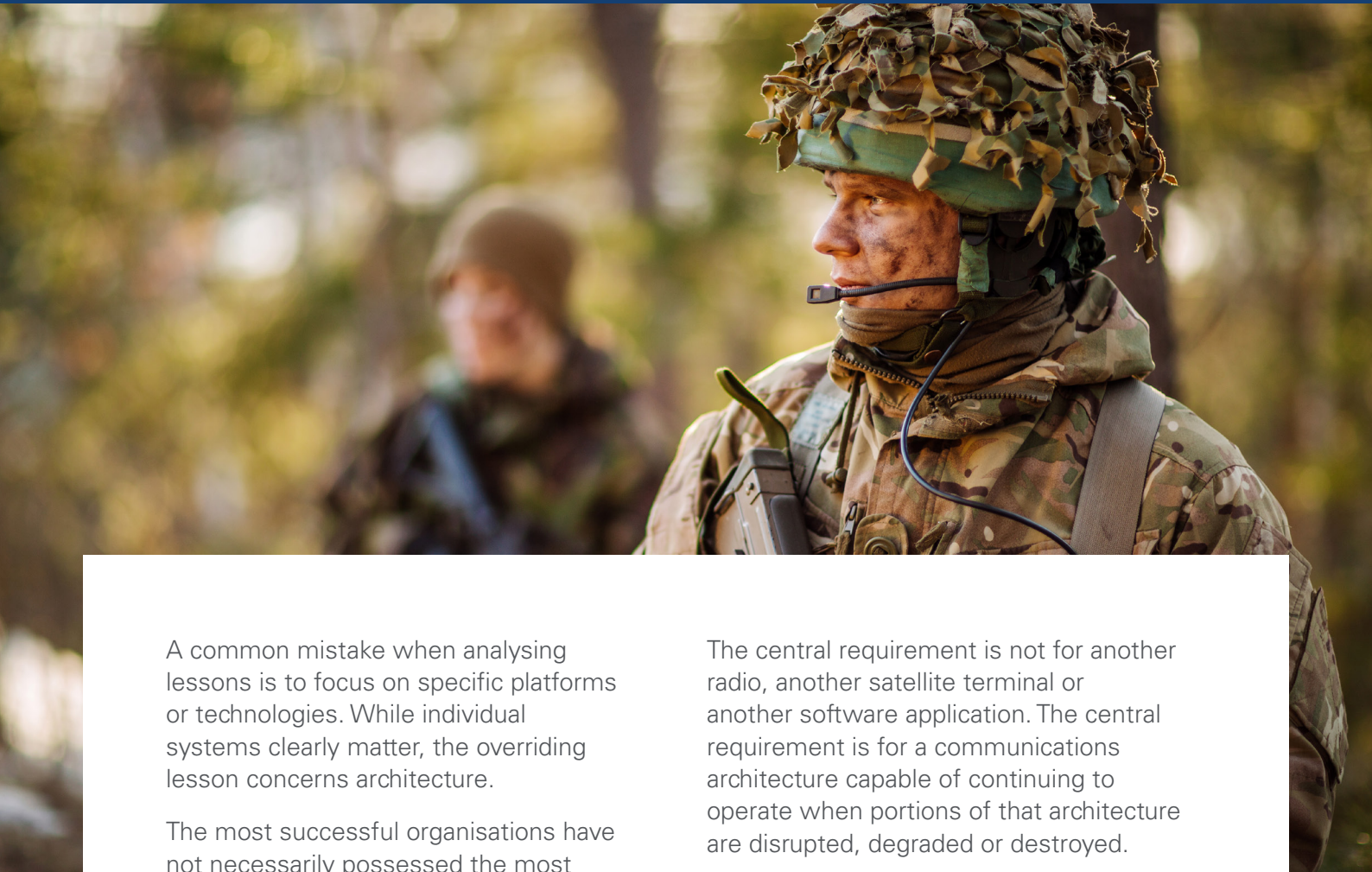
Across the Indo-Pacific, military planning is increasingly focused on highly contested operating environments characterised by vast distances, degraded infrastructure and sophisticated electronic warfare threats. Future operations may require forces to maintain command-and-control across dispersed formations operating hundreds or thousands of kilometres apart while facing cyber-attack, spectrum denial and disruption of terrestrial communications.

In the South China Sea and around Taiwan, military activity increasingly emphasises long-range sensing, distributed operations, resilient communications and electromagnetic superiority. Any future crisis in the region is likely to involve extensive electronic warfare, cyber operations, anti-satellite effects, long-range precision strike and attacks against communications infrastructure from the opening stages of conflict.

For coalition nations such as the UK, Australia, New Zealand and the United States, the Indo-Pacific highlights the importance of communications architectures capable of operating independently of any single bearer, network or infrastructure dependency. The objective is not simply connectivity, but assured command-and-control despite disruption, jamming, cyber intrusion and kinetic attack.

Similarly, many African operating environments present challenges associated with sparse infrastructure, extended logistics chains and expeditionary force deployment. The same lessons apply in the High North, across NATO's northern flank. In such circumstances, resilience is often determined less by technical performance and more by the ability to combine multiple communications pathways into a flexible and adaptable architecture.

THE CORE MOD CHALLENGE: ARCHITECTURE RATHER THAN EQUIPMENT



A common mistake when analysing lessons is to focus on specific platforms or technologies. While individual systems clearly matter, the overriding lesson concerns architecture.

The most successful organisations have not necessarily possessed the most advanced communications equipment. Instead, they have demonstrated an ability to combine multiple communications pathways, multiple information sources and multiple technologies into coherent and resilient networks.

This distinction is important.

The central requirement is not for another radio, another satellite terminal or another software application. The central requirement is for a communications architecture capable of continuing to operate when portions of that architecture are disrupted, degraded or destroyed.

Communications advantage is achieved through integration, adaptability and resilience rather than any individual technology. As a technology integrator, Network Innovations supports defence organisations in developing communications architectures that integrate multiple networks, systems and information sources into an interoperable operational capability.

ALIGNING CIS WITH THE ARMY'S EMERGING 20:40:40 CONSTRUCT

Recent British Army thinking has increasingly focused on the emerging 20:40:40 force construct, developed from lessons observed in Ukraine and discussed extensively across defence and industry forums, including recent RUSI Land Warfare Conference discussions. Under this model, approximately 20% of combat power is delivered through traditional crewed platforms, 40% through reusable autonomous and uncrewed systems and 40% through expendable autonomous capabilities such as loitering munitions and one-way attack systems.

While much attention naturally focuses on the platforms themselves, the success of the 20:40:40 construct ultimately depends upon command-and-control, information sharing and network resilience. Autonomous systems cannot contribute meaningful combat mass if they cannot communicate, share sensor data, distribute targeting information or maintain situational awareness.

Intellian, Peplink, TAK, Somewear Labs and Electromagnetic Warfare capabilities sit squarely within the communications and information layer that enables the 40% of reusable autonomous capability to operate effectively. Together they provide the foundation for resilient and adaptable communications in contested and distributed environments.

Without resilient CIS, autonomous systems become isolated platforms. *With* resilient CIS, they become part of a coherent operational system capable of delivering decision advantage and operational tempo.

RESILIENCE THROUGH DISTRIBUTION AND LAYERING

Recent defence thinking increasingly recognises that survivability in modern conflict depends upon distributing capability across multiple layers rather than concentrating it within a limited number of high-value systems. Discussions at recent defence and industry forums, including those focused on the Defence Industrial Partnership and lessons emerging from contemporary conflict, have reinforced the view that command-and-control systems are now vulnerable to simultaneous cyber, electromagnetic and kinetic attack.

A growing body of operational evidence suggests that communications degradation is often caused as much by physical destruction of infrastructure and command nodes as by electronic attack. Long-range precision fires, loitering munitions and UAS-enabled targeting have demonstrated a persistent ability to locate and destroy headquarters, relay nodes and communications infrastructure. The communications challenge is therefore broader than spectrum protection alone.

The 20:40:40 approach reflects the need to balance exquisite capabilities with scalable and rapidly replaceable systems. Within such a construct, resilient networking, transport diversity and communications survivability become critical enablers, ensuring command-and-control continues even when individual nodes are degraded or destroyed.

Capabilities such as Intellian, Peplink, TAK and Somewear align well with this philosophy because they contribute to the distributed and resilient communications layer that enables forces to maintain operational effectiveness under pressure.

Through partnerships with leading technology providers, Network Innovations helps defence organisations integrate best-of-breed capabilities into resilient, mission-focused architectures aligned to operational needs.

INTELLIAN OW7, OW10 AND OW11 – ENABLING RESILIENT REACH-BACK

Satellite communications remain a vital component of military command-and-control, particularly when operating beyond the reach of terrestrial networks or in areas where communications infrastructure has been degraded.

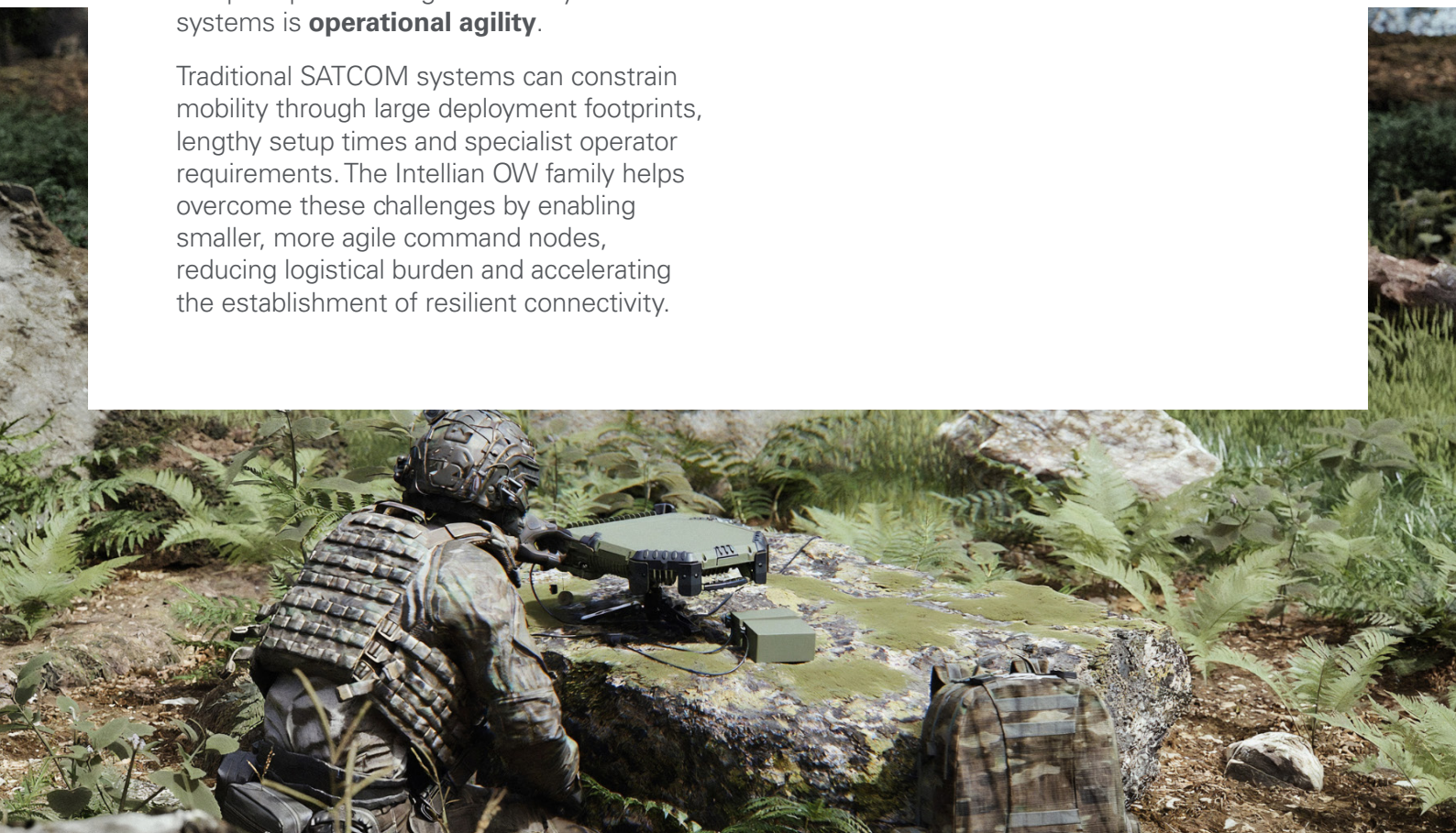
The Intellian OW family provides electronically steered flat-panel satellite terminals designed to support modern commercial and military satellite constellations. While these capabilities are often described in terms of bandwidth and connectivity, their true operational value lies elsewhere.

The principal advantage offered by Intellian systems is **operational agility**.

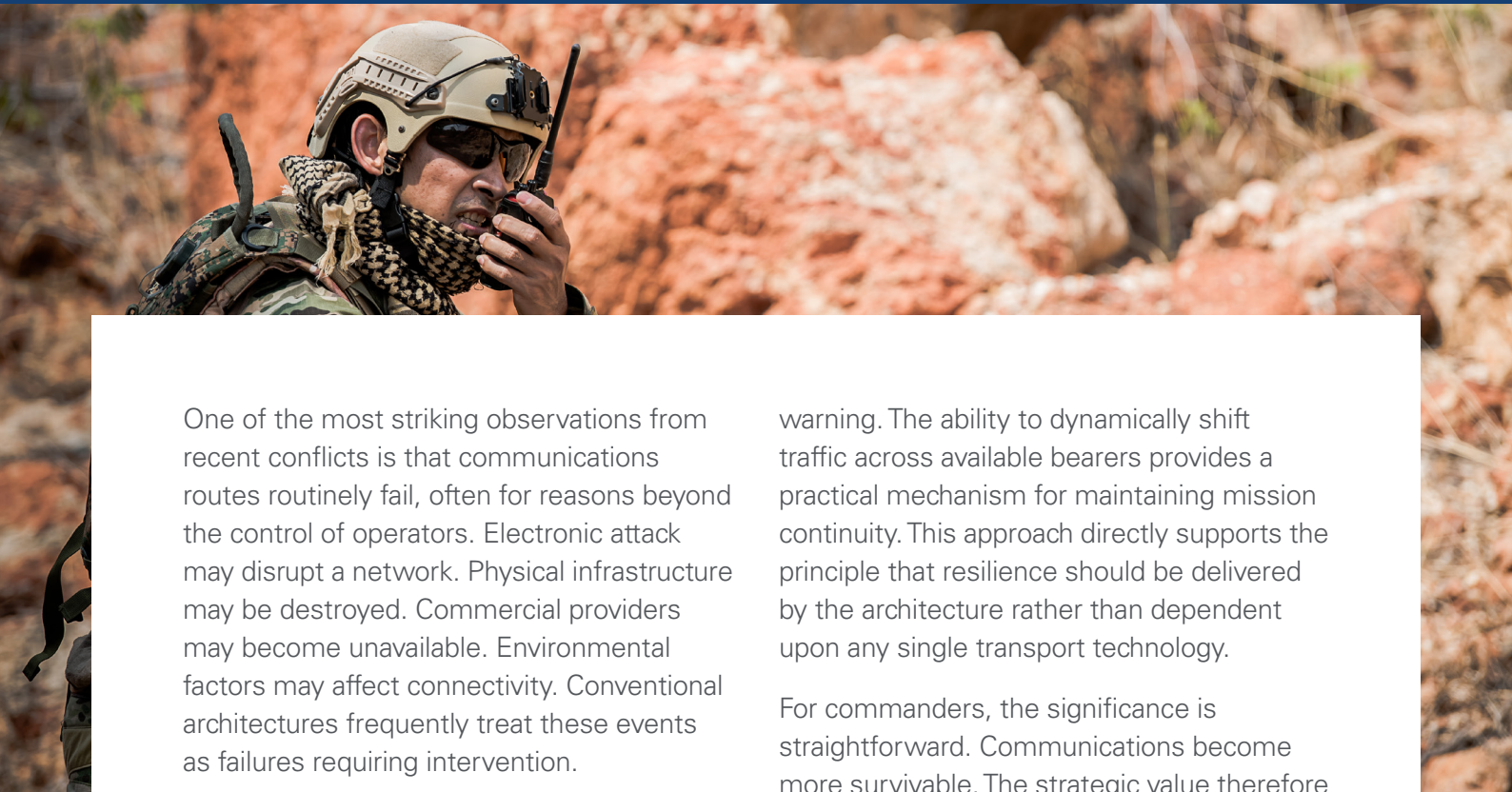
Traditional SATCOM systems can constrain mobility through large deployment footprints, lengthy setup times and specialist operator requirements. The Intellian OW family helps overcome these challenges by enabling smaller, more agile command nodes, reducing logistical burden and accelerating the establishment of resilient connectivity.

Most importantly, Intellian contributes to resilience by providing a transport layer that is independent of local infrastructure. In environments where terrestrial communications are unavailable, degraded or destroyed, satellite connectivity remains available.

However, the lesson from Ukraine suggests that SATCOM should not be viewed as a standalone solution. Its greatest value is realised when integrated with complementary capabilities that provide redundancy and alternative communications pathways.



PEPLINK – CREATING COMMUNICATIONS SURVIVABILITY



One of the most striking observations from recent conflicts is that communications routes routinely fail, often for reasons beyond the control of operators. Electronic attack may disrupt a network. Physical infrastructure may be destroyed. Commercial providers may become unavailable. Environmental factors may affect connectivity. Conventional architectures frequently treat these events as failures requiring intervention.

Peplink approaches the problem differently. Rather than relying upon a single communications path, Peplink orchestrates multiple bearers simultaneously. SATCOM, LTE, 5G, Wi-Fi and terrestrial networks can all be aggregated into a unified service. Traffic is dynamically routed according to network performance and availability.

Beyond simple bearer aggregation, Peplink supports a broader operational objective: ensuring that command-and-control functions persist despite disruption. In future conflicts, commanders may lose access to individual satellite networks, commercial services or terrestrial infrastructure without

warning. The ability to dynamically shift traffic across available bearers provides a practical mechanism for maintaining mission continuity. This approach directly supports the principle that resilience should be delivered by the architecture rather than dependent upon any single transport technology.

For commanders, the significance is straightforward. Communications become more survivable. The strategic value therefore extends beyond networking efficiency. Peplink enhances command continuity, reduces operational risk and increases confidence that communications services will remain available despite disruption.

In many respects, Peplink provides the resiliency layer that modern military architectures increasingly require.

TEAM AWARENESS KIT – DELIVERING A COMMON OPERATING PICTURE

Modern operations generate extraordinary quantities of information. Sensors, intelligence systems, UAVs, headquarters, reconnaissance elements and individual soldiers all contribute data into complex information environments.

The challenge is rarely the absence of information. The challenge is transforming information into shared understanding.

Team Awareness Kit (TAK) directly addresses this problem.

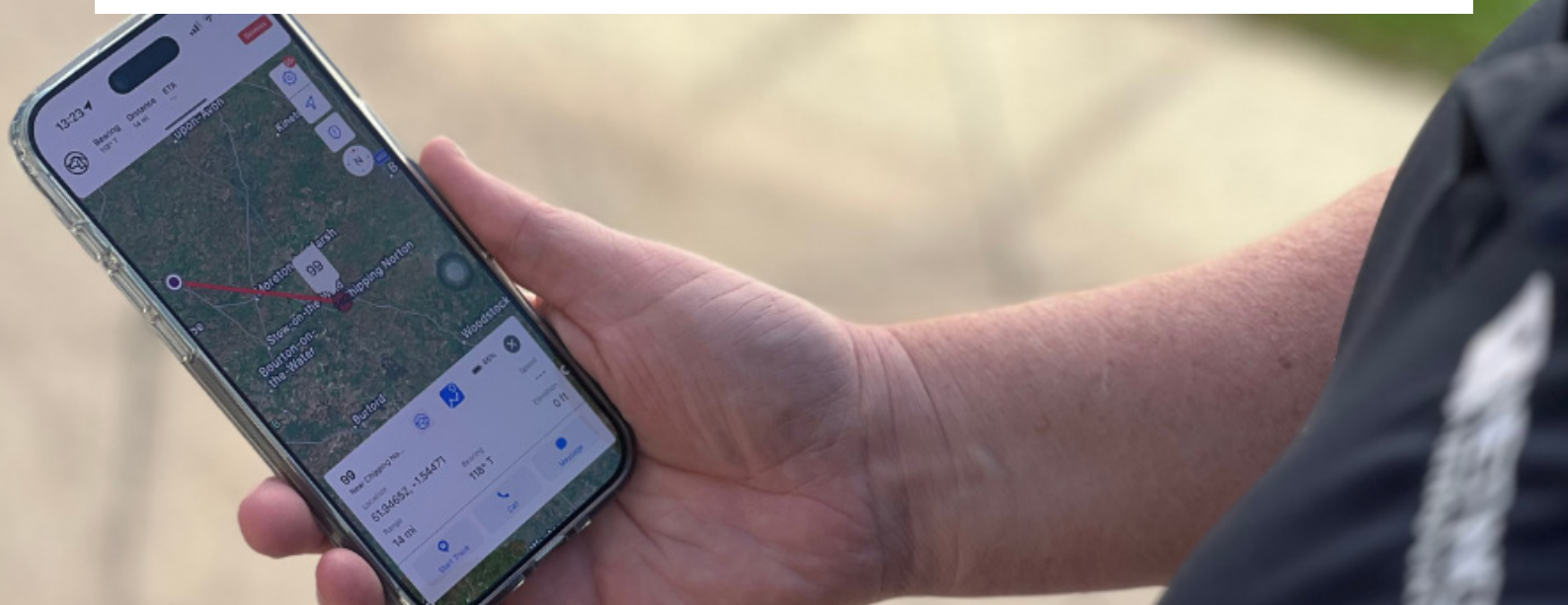
TAK has emerged internationally as one of the most successful approaches to providing situational awareness across military organisations. The reason is not technological novelty but operational utility. TAK enables information from multiple sources to be displayed through a common

operational picture. Personnel locations, intelligence reports, mission graphics, UAV feeds and operational planning data can all be visualised within a shared environment.

For senior leaders, the value proposition is compelling. Better information sharing results in faster decision-making. Faster decision-making improves operational tempo. Improved operational tempo creates military advantage.

TAK's greatest strength lies in its ability to act as an integration layer. Rather than replacing existing systems, it enables disparate systems to contribute to a common operational picture.

This aligns directly with the broader objectives of Multi-Domain Integration and Digital Backbone.



SOMEWEAR LABS – EXTENDING SITUATIONAL AWARENESS TO THE TACTICAL EDGE

The requirement for persistent situational awareness extends far beyond headquarters. Ukraine has demonstrated the importance of small, distributed teams operating independently over large geographic areas. Reconnaissance patrols, liaison officers, logistics elements and specialist operators often work beyond the range of conventional communications systems. Maintaining awareness of these personnel can prove challenging.

Somewear Labs addresses this problem through lightweight satellite-enabled tracking and messaging devices designed for austere

environments. While technically simple compared with many CIS systems, their operational value should not be underestimated. Commanders gain improved visibility of force disposition. Personnel recovery becomes easier. Isolated operators retain access to emergency communications. Importantly, these capabilities provide resilience without significantly increasing burden on users.

Within a layered architecture, Somewear extends connectivity and situational awareness into areas where more sophisticated communications solutions may be impractical.



ELECTROMAGNETIC AWARENESS AND DOMINANCE

A critical lesson emerging from both Ukraine and recent Middle Eastern operations is that command-and-control is now threatened simultaneously across multiple domains. Communications networks may be disrupted through cyber-attack, electronic warfare, physical destruction of infrastructure or precision strike against headquarters and relay nodes.

Kinetic attack against C2 infrastructure has become increasingly common. Adversaries routinely combine intelligence collection, UAV reconnaissance and spectrum monitoring to identify command posts before prosecuting them with long-range fires or loitering munitions. Communications survivability therefore depends not only on protecting data and spectrum access, but also on distributing command-and-control functions across multiple locations and multiple communications pathways.

The solution is architectural resilience. If one headquarters, bearer or communications route is lost, alternative pathways must already exist.

If Ukraine has demonstrated one transformational lesson, it is that the electromagnetic spectrum has become a manoeuvre space in its own right. The ability to communicate remains important. The ability to understand who else is communicating may be even more important.

An EW capability capable of scanning, replicating and denying signals across the 0–6 GHz spectrum provides a critical enhancement to operational awareness. Such systems enable forces not only to detect and identify emitters but also to understand activity within the spectrum and, where required, influence or disrupt adversary use of that spectrum.

This changes the role of communications architectures. The objective is no longer simply communications protection, but battlespace advantage through superior understanding of the electromagnetic environment.

Recent conflicts have demonstrated that electromagnetic activities rarely occur in isolation. Electronic warfare effects are increasingly coordinated with cyber operations, intelligence collection and kinetic strike. Adversaries routinely seek to identify command posts through their electromagnetic signatures before employing long-range fires or unmanned systems against them. Consequently, understanding the spectrum is no longer solely a technical activity. It has become a critical component of force protection, manoeuvre and targeting.

The integration of EW outputs into systems such as TAK offers promise, enabling spectrum information to become part of the commander's common operating picture.

RECOMMENDATIONS

1. Prioritise Resilience-Focused Experimentation

MOD should prioritise experimentation that evaluates CIS resilience against simultaneous cyber, electronic warfare and kinetic threats. Trials should assess how distributed command-and-control architectures support the Army's emerging 20:40:40 force construct and continue to function when communications nodes, headquarters or transport bearers are degraded.

2. Establish an Integrated Brigade-Level Trial Programme

A phased experimentation programme should be conducted at Brigade level, integrating communications, networking, situational awareness and electromagnetic warfare capabilities within a single operational environment. The objective should be to assess command-and-control resilience under realistic communications degradation scenarios.

3. Prioritise Open and Interoperable Architectures

Future procurement should prioritise open architectures, rapid integration and interoperability over platform-specific optimisation. The ability to integrate emerging technologies rapidly is likely to become a key determinant of operational effectiveness.

4. Align Future Procurement with Enterprise Initiatives

MOD should explore how these capabilities align with Digital Backbone, Federated Mission Networking and Multi-Domain Integration initiatives, ensuring future acquisitions contribute to a coherent enterprise architecture rather than creating additional stovepipes.

5. Treat Electromagnetic Warfare as a Core CIS Requirement

Electromagnetic warfare capabilities should be considered a core component of future CIS architectures rather than a specialist adjunct. Communications systems should be designed from the outset to operate effectively within contested electromagnetic environments.

CONCLUSION

The central lesson from Ukraine, the Middle East and wider observations from the Indo-Pacific operating environment is not that militaries require more communications equipment. Rather, they require communications architectures designed to survive the simultaneous effects of cyber-attack, electronic warfare, information operations and kinetic strike. Future advantage will increasingly belong to organisations capable of rapidly integrating diverse technologies into resilient, distributed and adaptive command-and-control networks.

The capabilities discussed within this report are not developmental concepts. They represent mature, operationally proven technologies already employed by military, government and security organisations across NATO, Five Eyes and partner nations. Their relevance extends beyond a single theatre, having demonstrated utility in environments ranging from the High North and Northern Europe to the Middle East, Indo-Pacific and expeditionary operations worldwide. This operational pedigree significantly reduces integration risk whilst accelerating delivery of capability aligned to the MOD's Digital Backbone and Multi-Domain Integration ambitions.

None of these capabilities represents a complete solution in isolation. Together, however, they provide the foundations of a modern communications architecture aligned with the realities of contemporary warfare and the future direction of UK defence.

The key question for MOD is therefore not whether these individual technologies work. The evidence suggests they do. The more important question is whether MOD can rapidly integrate commercially mature capabilities such as these into a coherent operational architecture before future conflicts demand it.

Success will depend not only on technology selection, but on the ability to integrate capabilities into resilient architectures aligned to operational requirements, an area in which technology integrators such as Network Innovations can play an important role.



About the Author

Rob Gains

Business Development Manager – Land & Coalition

An accomplished Business Development and Project Manager, Rob brings 24 years of leadership in the British Army's Royal Corps of Signals, delivering complex IT, communications and transformation programmes across Defence in both sovereign and international coalition environments. He has deep expertise in programme governance, IT service delivery, cyber and information security and stakeholder engagement across multi-national environments. Throughout his career, Rob has led cross-functional teams and implemented robust risk, change and business continuity frameworks to ensure resilience and operational assurance in mission-critical settings.



Your Advanced Connectivity Provider

As technology solution integrators, we enable our customers to conduct some of the most important work on the planet across a multitude of industries – from the front office to the remote mission or field operation. Our customers depend on us for honest advice, a wide array of innovative offerings, and superior service to ensure their worlds are connected securely and seamlessly.

Meeting Your Mission. With Passion.

