Decision Making in the Battlespace of the Future

Digital Intelligence

BAE SYSTEMS

Contents

Foreword

Dave Armstrong MBE, Managing Director, BAE Systems Digital Intelligence

Tackling ongoing global conflicts, whilst navigating the rapid advancement of technology, has continued to raise the demand for connected information to defend our nations.

We're now operating in a challenging defence landscape, where the battlespace has been digitalised, and the boundary between the traditional military domains of land, sea, air, cyber and space are blurred.

Military commanders must work closely together, deal with multiple sources of complex information, and make the right decisions in seconds. But the task is more challenging than ever as the landscape does not stay still. The right tools and doctrine are needed to succeed, and the answer lies in Multi-Domain Integration.

> "By weaving digital threads, we are enabling the whole defence ecosystem – from national security, through to government systems and military organisations – to be connected."

The need to create digital threads, access the right information at the right time, and gain a total intelligence awareness, is clearer today than ever before. This is why BAE Systems Digital Intelligence was founded. By weaving digital threads, through our data driven systems and multi-domain connectivity tools, people are coupled to one true source, driving quicker, data-driven decision making.

Combining expert BAE Systems and third party commentary with data from senior defence and aerospace decision makers in the UK, Canada, Australia, the Nordics, the United Arab Emirates and The Kingdom of Saudi Arabia, we unveil:

- **The challenges** currently being faced by nations around the globe
- **Current levels** of Multi-Domain Integration
- **Key focus areas** for Multi-Domain Integration success

I hope you find this report valuable. Please reach out if you would like to discuss your Multi-Domain Integration goals, and how BAE Systems Digital Intelligence can help you navigate the challenging waters that today's defence landscape brings.

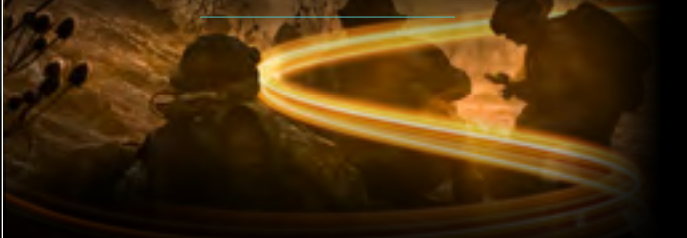
Dave Armstrong MBE
Managing Director,
BAE Systems Digital Intelligence

Methodology

400

Senior IT decision makers and senior business decision makers working in aerospace or defence

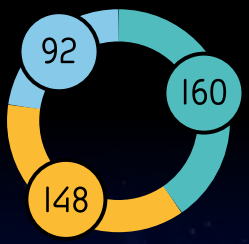
88%



In military roles

From organisations with over 1,000+ employees

- 5,000 or more employees
- 3,000-4,999 employees



- 1,000-2,999 employees

An international survey

Respondents were interviewed by telephone and online surveys in June - August 2023 by market research specialist Vanson Bourne on behalf of BAE Systems Digital Intelligence. There were 150 respondents in the UK, 100 in Canada, 50 in The Nordics, 50 in Australia and 50 in the Middle East (including The Kingdom of Saudi Arabia and the UAE).

Story in numbers

We surveyed 400 senior business and IT decision makers in defence and aerospace from the UK, Canada, Nordics, Australia, UAE and The Kingdom of Saudi Arabia to talk to us about the evolving battlespace and their perspectives on **Multi-Domain Integration.**

The Modern Battlespace is Digital

95% of respondents agree that ongoing digitalisation has led to a more dynamic and complex battlespace

86% say the future battlespace will be an information battlespace

98% agree an evolution of processes will be essential for navigating the complexities of modern defence

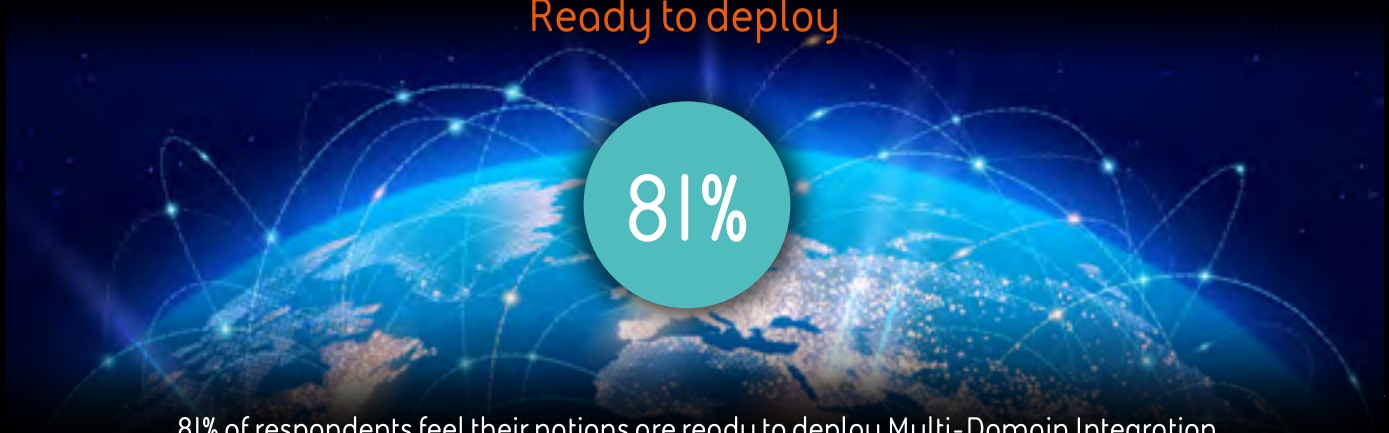
Multi-Domain Integration is Mission Critical

98% of respondents say that Multi-Domain Integration is important in shaping military operations today

99% agree it will still be important in 10 years' time

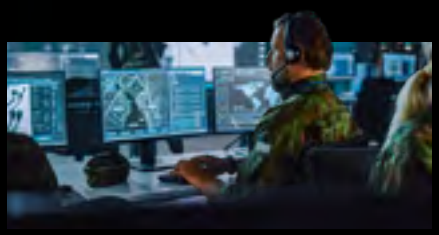
Respondents also agree Multi-Domain Integration is key for navigating the growing threats of cyber warfare (55%) and national security breaches (53%)

Ready to deploy



81% of respondents feel their nations are ready to deploy Multi-Domain Integration

Three key areas of focus



People

Collaboration across military departments

Process

Regulatory standards for Multi-Domain Integration programmes

Technology

Technology solutions designed for collaboration

How to achieve Successful Multi-Domain Integration in defence

94% agree

System interoperability to strengthen the integration of defence technology

92% agree

Diverse defence technology ecosystems to offer an opportunity to promote resilience

54% agree

The ability to use data to improve operational readiness and availability

50% agree

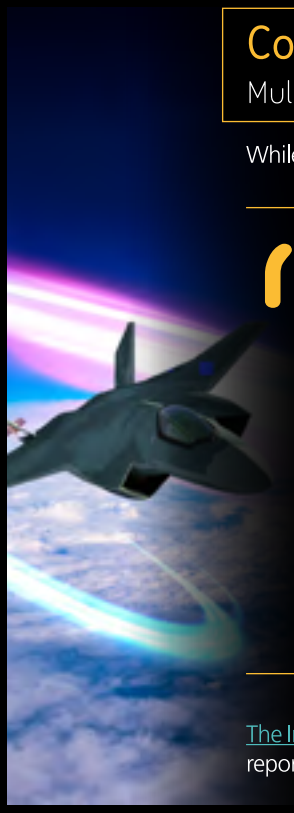
AI and Machine Learning for enhanced situational awareness and decision making

The outcome will power more effective defence

91% agree implementing Multi-Domain Integration is difficult but essential

93% agree integration across domains will be required for defence in the future battlespace

Three key concepts discussed in this report



Concept #1.
Multi-Domain Integration:

While terminology varies across the globe, Multi-Domain Integration is defined by the UK government as

> "Effective integration of space, cyber and electromagnetic, maritime, air, and land achieves a multi-domain effect that adds up to far more than simply the sum of the parts – **recognising that the overall effect is only as powerful as the strength of the weakest domain.**"

The Integrated Operating Concept 2025, UK Ministry of Defence. The five domains in defence that we refer to in this report are defined as: land, air, sea, space and cyber.

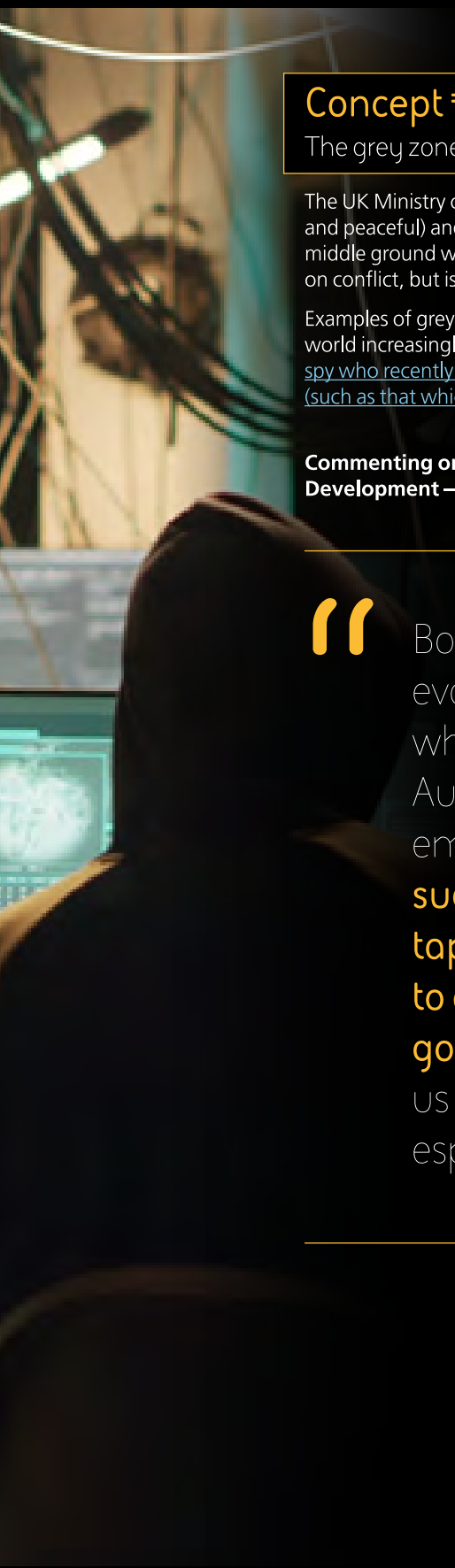
Concept #2.
The information battlespace:

The information battlespace, where information warfare takes place, refers to the battlespace use and management of communications, digital technology and data to gain a competitive advantage over the adversary.

As the volume of global data increases, the information battlespace becomes more important to prioritise. It is domain agnostic, highlighting the need to be more connected between domains, more incisive, more predictive, and more informed in order to create an information and decision advantage.

> "**The pervasiveness of information and the pace of technological change are transforming the character of warfare.** Old distinctions between 'peace' and 'war', between 'public' and 'private', between 'foreign' and 'domestic' and between 'state' and 'non-state' are increasingly out of date."

The Integrated Operating Concept 2025, UK Ministry of Defence.



Concept #3.

The grey zone:

The UK Ministry of Defence contextualises the grey zone as the space between 'white' (where actions are benign and peaceful) and 'black' (where actions are clearly hostile and can be seen as an act of war). The grey zone is the middle ground which, the Ministry of Defence says, "... is a murky area, consisting of everything which isn't full-on conflict, but isn't exactly an innocent act either."

Examples of grey zone activity range from cyberattacks (the most common form of grey zone attack as the digital world increasingly becomes an important part of the battlespace), to espionage (such as the alleged international spy who recently used LinkedIn to lure British officials into handing over state secrets), to mis- and dis-information (such as that which attempted to undermine the UK's COVID-19 response).

Commenting on grey zone activity in Australia specifically, Ron Dempster, Head of Business Development – Defence & Space Australia, BAE Systems Digital Intelligence, said:

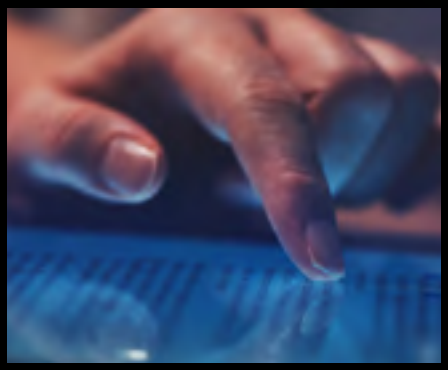
> "Bolstering security measures to address and mitigate evolving threats is a constant challenge across the whole defence spectrum. And it's no easy task. In Australia, ideological extremism is one of the areas emerging as a concern, with **some news reports, suggesting that foreign agents have been able to tap into apps such as WhatsApp and even Tinder to approach Australians with the knowledge of government secrets.** In this context, it's important for us to put security at the heart of our defence systems, especially in a world of increased integration."

Introduction:

Decision making in the evolving battlespace

Rapid technological change is reshaping the battlespace, impacting how decisions are made

The speed of technological change is putting significant pressure on defence technology strategies. Respondents highlight AI and quantum computing (96%), the use of space for national defence (89%), and cyber and hybrid warfare (89%) as major challenges.

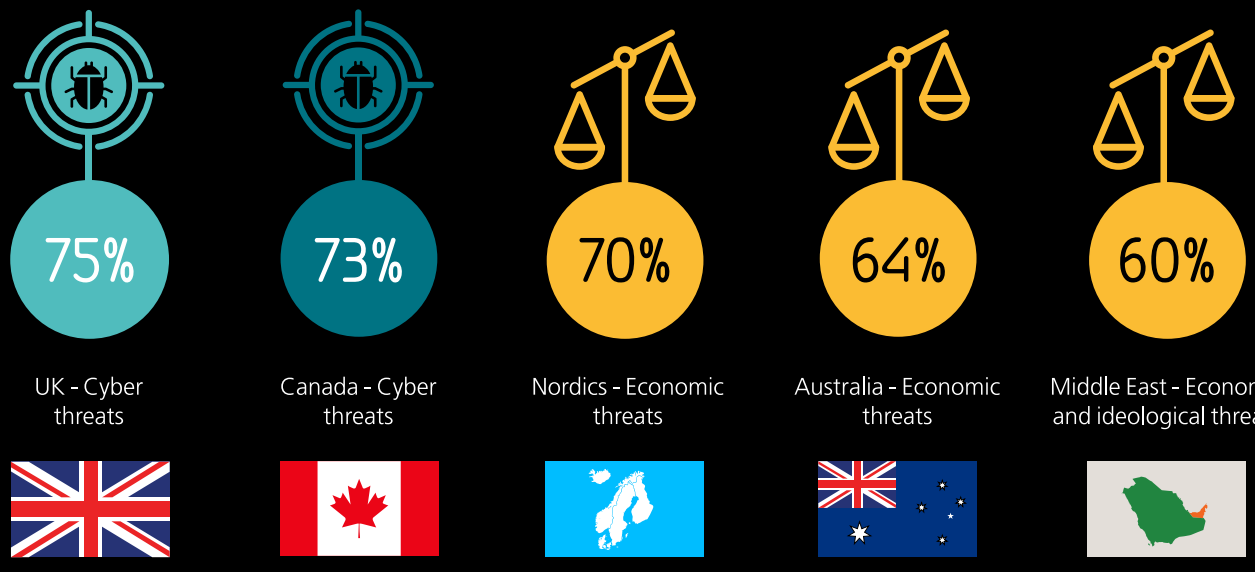


The 'grey zone' is also a key concern to national defence and militaries, with respondents being worried about the spread of misinformation (61%) and challenges in the attribution of cyber activity (61%).

As such, 90% of respondents agree there is an urgent need for more seamless information sharing across domains. System interoperability (94%) is also recognised as essential to driving more effective decision-making in the modern battlespace.

The modern battlespace

Top threat concerns – as cited by military and industry respondents



The evolving information battlespace

What is adding pressure on the development and implementation of defence technology?

Technological change is almost unanimously seen as the biggest pressure on defence today. It is significantly impacting warfare with the introduction of sophisticated technology including uncrewed drones, autonomous weapons that can react more quickly than humans, and intelligence powered by low earth orbit satellite clusters. AI and Quantum Computing enabled technology, the total potential of which we can't yet imagine, was recognised by 96% of respondents as transformative for the future battlespace.

Digital innovation is increasing the information battlespace's size and with it the volume of grey zone attacks. This combination of factors could bring significant challenges:

More cyberattacks, potentially causing more damage: 46% of respondents said the weaponisation of cyber is adding pressure to the development of defence technology strategies in their nation. Yet, cyber tactics remain in the grey zone with the Ministry of Defence saying nation states can inflict real-world damage via cyberspace, while potentially remaining safe from attribution or retaliation. 61% of defence professionals agreed that difficulties in attributing cyber activity is the most concerning factor about the grey zone.

A data glut blocking intelligence: 54% of respondents said data to improve operational readiness and decision making is the most important factor to enable the effective use of defence technology.

Yet, the amount of data being produced means while key intelligence produced by one domain may be of utmost importance to another, there may be no way of identifying that or sharing the data.

'A digital Berlin Wall': 94% of respondents agree collaboration and information-sharing among industry, partners and allies is critical to success in the future battlespace, but the information battlespace is marked by a lack of cohesion. The UN-Secretary General has warned of a 'divide' or 'digital Berlin Wall' between countries creating their own unique internet and AI strategies, guided by separate financial, geopolitical and military views.

> "94% of respondents agree collaboration and information-sharing among industry, partners and allies is critical to success in the future battlespace"

Pavandeep Bhogal, Head of Product Engineering, BAE Systems Digital Intelligence

"A significant portion of strategic initiatives operate below the threshold of overt engagement. The focus has shifted towards subtly engaging adversaries without instigating a response in the grey zone. This nuanced approach requires a pronounced information advantage, something we're already seeing in the transition to a digital battlespace, and underscores the potential existence of tension before conflict, where there is a significant amount of data to be leveraged.

"We must effectively channel and interpret this data influx in a way that empowers us to refine decision-making processes. Success entails getting inside the adversary's OODA (Observe, Orient, Decide, Act) loop quicker than they can infiltrate ours to ensure that we can retain information superiority."

Andy Linton, Head of Future Maritime Aviation Force, BAE Systems - Air

"Multi Domain Integration is essentially about connectivity and the ability to effectively make timely decisions in directing employment of assets from across all five domains to achieve the greatest co-ordinated net military effect, faster than the adversary - know sooner, decide quicker, act faster. The key currency is information, derived from data. Without access to the full spectrum of desired information, it is difficult to make effective decisions and thus quantify the operational risk. This challenge is compounded by the fact that there's so much data available in both the civilian (open source) and military (secure) context, it's difficult to know exactly what information is available and more importantly, relevant. It's often a case of trying to find the proverbial needle in a multispectral and multifaceted haystack. This is driving the need to leverage Artificial Intelligence and Machine Learning to reduce analysis and processing times from days down to milliseconds.

"The aim is to connect all actors in modern battlespace via multi-domain networks and enable access to key information hosted in shared environments. It's also critical to intelligently distil the terabytes of data being collected down to a relevant manageable volume so that it can be shared securely and at the speed of relevance across operational environments, so the right people have access to the right information at the right time."

Mark Fitton, Senior Engineering Sales Manager, BAE Systems Digital Intelligence

"As we step into the latest evolution of modern conflict, a significant shift in threat dynamics demands our attention. The focus is pivoting from the relentless struggle against terrorism to a new paradigm centred on state-on-state confrontations. This creates a need for a comprehensive re-evaluation of our strategies, tools and approaches.

"Merely sharing information is insufficient. The complexities of the modern battlespace demand a higher standard of integration, cohesion and seamless interoperability to bridge the gaps that have historically impeded swift action. We need to look at information as a dynamic force rather than just a static resource. Information must be timely, actionable, intelligent and available. It doesn't solely inform but also empowers decision-makers to respond with agility and insight."

Martyn Orme, Head of Business Development, Techmodal

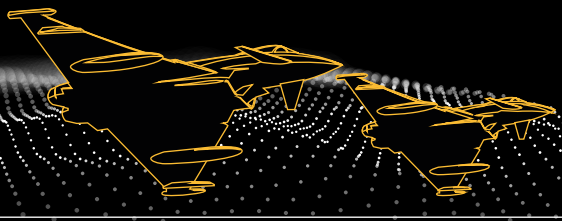
"Multi-Domain Integration is being enabled by the speed of change in the technology landscape, but it's also essential because of it. In the information rich battlespace, we need to keep up, driving value across the entire ecosystem. We need the right tools to safely and securely access information across domains - not just cyber and space, but also across government departments."

How Multi-Domain Integration powers better decision making

Processes are evolving quickly to deal with the complexities of modern defence

98%

of military and industry personnel surveyed agree we must continue to evolve processes to deal with the complexities of modern defence.



Processes need to evolve quickly to deal with the modern battlespace, and adopting the latest and greatest technology isn't the entire solution. Without a Multi-Domain Integration strategy in place, adopting new technology can create further challenges. Driving integration across the domains - alongside other instruments of national power, NATO and other like-minded allies and partners - is essential to managing the evolving defence challenges of today and the future, and to supporting better decision making.

Mivy James, Digital Transformation Director, BAE Systems Digital Intelligence

"One of the main benefits of Multi-Domain Integration is operational effectiveness and the ability to access a holistic view of a situation, across domains. Ultimately, we live in an ever increasing fast moving world where things could be happening across all five domains at once.

"Part of this means we need to re-emphasise the grey zone and differentiate less between the physical and digital, recognising that much of modern warfare is operating across both and we need the digital threads between domains to manage this evolving threat."

Mark Todd MBE, Head of Product Development, BAE Systems Digital Intelligence

"Multi-Domain Integration in theory has been around for a while. If we wind the clock back 10-15 years, we would still be talking about it, but in a slightly different language - we'd be talking about network-centric warfare or joint operations. Part of the Multi-Domain Integration challenge is more than just connecting your own forces together, or the forces of your allies, but also working with political levers. NATO concepts and doctrines pull this out quite well, because they talk about enhancing situational awareness, not just from a military context, but also from a political context."

This is recognised by some nations. The U.S. Joint All-Domain Command and Control Strategy 2022 (JADC2) and the UK's Integrated Operating Concept 2025 are two examples of building Multi-Domain Integration into overarching defence strategies.

As the JADC2 says, "[there is an] urgent need for a focused Departmental push on actions to empower our Joint Force Commanders with the capabilities needed to command the Joint Force across all warfighting domains and throughout the electromagnetic spectrum to deter, and, if necessary, defeat any adversary at any time and in any place around the globe."

> "The U.S. Joint All-Domain Command and Control Strategy 2022 (JADC2) and the UK's Integrated Operating Concept 2025 are **two examples of building Multi-Domain Integration** into overarching defence strategies."

Chapter I:
The case for Multi-Domain Integration

Multi-Domain Integration provides an advantage in present and future military operations, supporting defence against cyber warfare, national security breaches and long-term threats to economies.

Key Insights

The ability of Multi-Domain Integration to support preparedness is recognised among defence and aerospace respondents, with 79% saying it is key to shaping today's military operations.

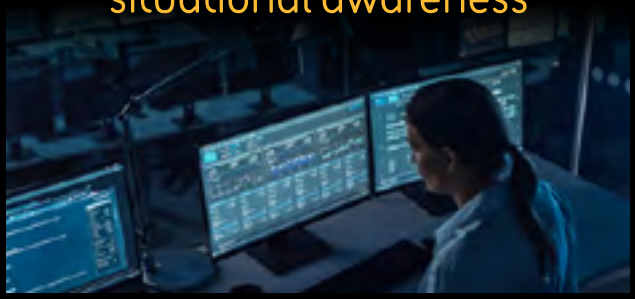
As defence organisations adopt cutting edge technologies such as data and intelligence analytics solutions (91%), AI and Machine Learning tools (86%) and technology that promotes better connectivity (74%), it's important to recognise that these technologies need to be integrated effectively to achieve their full potential.

The top two benefits of Multi-Domain Integration

Which benefits has/would your nation reap from implementing Multi-Domain Integration?

01

Improved situational awareness



02

Improved quality of decision making

Most respondents recognised the many benefits of Multi-Domain Integration. The top two benefits, improved situational awareness and better quality decision making, point to Multi-Domain Integration's powerful value in supporting better data use in a fast-paced battlespace. These are also key outcomes of the adoption of advanced technology, which itself relies on the collection and analysis of vast amounts of data across domains to give nations the advantage against the adversary.

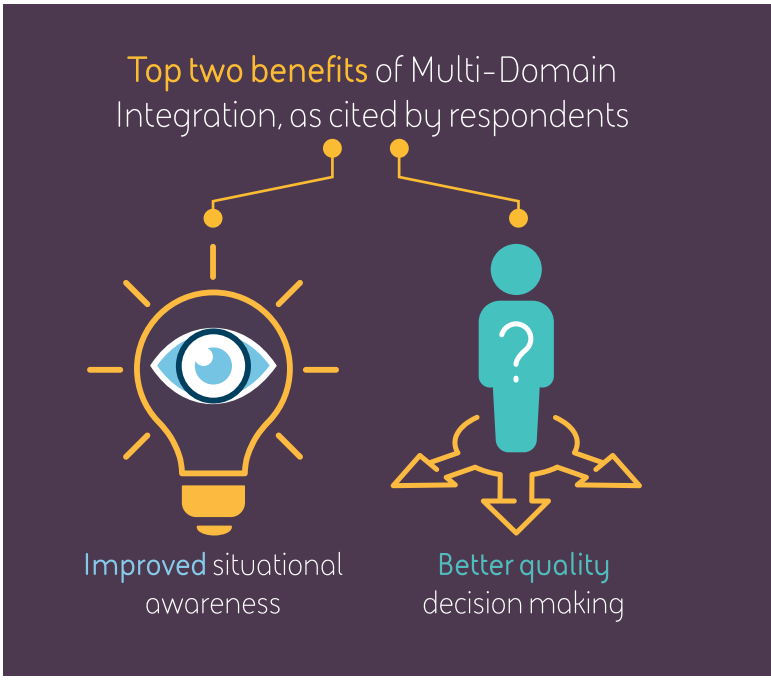
Yet there are significant challenges to overcome before nations can adopt Multi-Domain Integration fully, which we'll discuss in Chapter Two.

Mark Todd MBE, Head of Product Development, BAE Systems Digital Intelligence

"When executed properly, Multi-Domain Integration will provide forces with a clear decision advantage. At BAE Systems Digital Intelligence, we epitomise this approach, by establishing secure digital threads for our customers from Law Enforcement, Central Government to National Security Agencies and beyond. This leads to building a wider intelligence picture, facilitating swift, accurate decision-making in high-pressure defence situations.

"Those of us who have been in operating roles have a real understanding of the need for increased situational awareness.

"It requires a change in mindset to think about defence from a broader perspective than the kinetic effects of the traditional battlefield. You need to think about how you want to break down barriers not just across your military services, but also across aspects of central government, national security and beyond."



Mivy James, Digital Transformation Director, BAE Systems Digital Intelligence

"Nations are at an early stage of implementing Multi-Domain Integration that's characterised by manual integration. To truly reach the next level, it's essential that we shift towards a more automated integration approach, fostering better domain connectivity and allowing humans to prioritise what they do best.

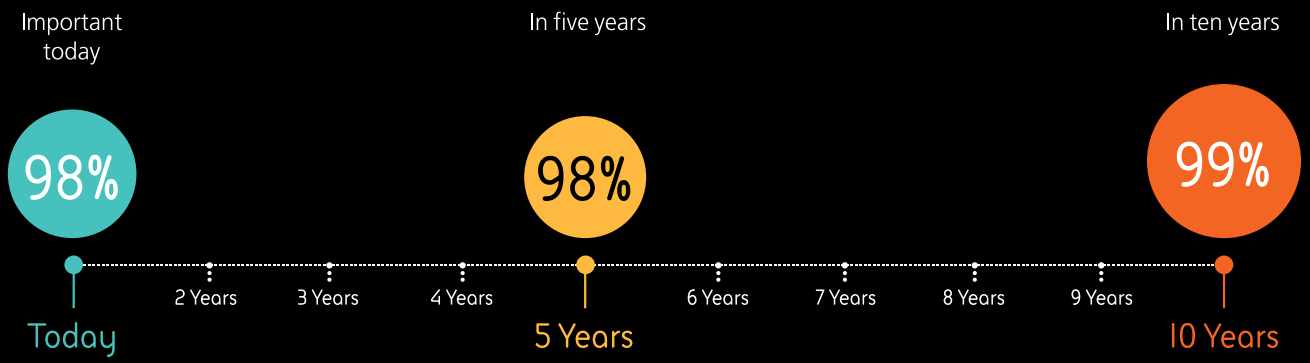
"From a technology standpoint, automating integration will also allow us to adopt state-of-the-art technology at scale, rather than just sprinkling it around domains without thinking about the bigger picture."

Antony Mrozicki, Product Owner FCAS, BAE Systems – Air

"What I'm seeing is that the UK has a Multi-Domain Integration strategy that is putting us in a good position nationally, but other nations will have their own versions. We're now approaching the moment where we need to start taking international collaboration mechanisms into our own strategy so true Multi-Domain Integration can continue to happen, nationally and internationally, without interruption."

Why Multi-Domain Integration adoption is a matter of urgency

The percentage of respondents who believe Multi-Domain Integration is crucial or very important in shaping military operations today and into the future



The importance of Multi-Domain Integration in shaping military options today versus in ten years doesn't shift massively in the eyes of our respondents. This perhaps reflects that the challenges they will face in a decade will be similar to those they are experiencing today, albeit at a potentially larger scale.

Respondents believe Multi-Domain Integration is key for navigating the following growing threats (top five)...

01 Increased cyber warfare attacks

02 Increased breaches in national security

03 Long-term threats to economic interests of the state

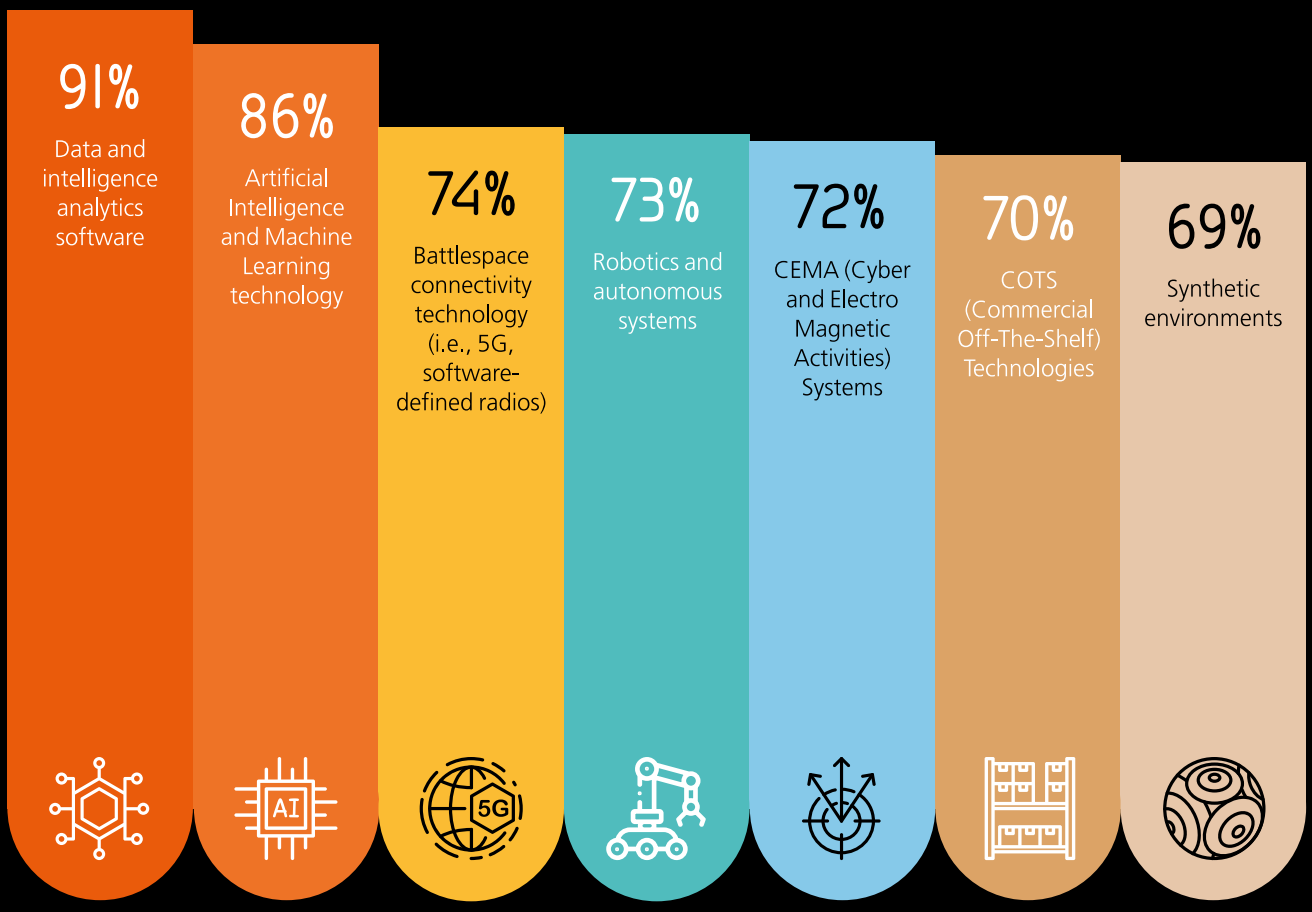
04 Challenges in the grey zone

05 Challenges in keeping up with the latest forms of warfare

Multi-Domain Integration and the adoption of new defence technology

Respondents recognise the importance of new technology to achieve an advantage and many have already started adopting them.

To what extent has your military or nation adopted the following technologies across its defence operations?



Multi-Domain Integration is critical to making the most of this rapid influx of increasingly sophisticated defence technology, as it enables opportunities to maximise technology implementation efficiencies between and even within domains.

Pavandeep Bhogal, Head of Product Engineering, BAE Systems Digital Intelligence

"The most prominent tech trends we're currently seeing in defence are related to autonomy, Artificial Intelligence, Machine Learning, and hypersonics."

> "Data can be a boon or a curse, but if we want to gain the benefits we need the tools to help us make better decisions quickly."

Martyn Orme, Head of Business Development, Techmodal

"More advanced technology means people can ask more complex questions about the battlespace, which is also more dynamic and fast moving. While we can do more with data, the complexity of this data means at times it can be unstructured and therefore less trustworthy. Data can be a boon or a curse, but if we want to gain the benefits we need the tools to help us make better decisions quickly.

"In the last five years, the UK has made great strides in this space. The challenge now is to get more data into existing tools, as well as ensuring the right questions are being asked."

Chapter 2:

Maximising Multi-Domain Integration: areas of focus for defence

Military and industry respondents told us more about the key areas we must focus on to maximise Multi-Domain Integration opportunities.

98% While there is still work to be done, the vast majority of defence professionals also acknowledged that Multi-Domain Integration is 'essential'. The end goal is worth it.

Respondents highlighted the following **top-five** factors as important for the successful implementation of Multi-Domain Integration.

Focus on: people

01 Willingness to collaborate across military departments

02 Trust between office-based personnel and those on active operations

03 Attracting and retaining skills relevant to the industry

04 Non-conflicting priorities between military/defence departments

05 Training associated with the adoption of new technology

Focus on: process

01 Regulatory standards across Multi-Domain Integration programmes

02 Acquisition processes for Multi-Domain Integration technology

03 Collaborative working between different entities and domains

04 Collaboration between defence industry and military

05 Understanding and strategy around business change

Focus on: technology

01 Integrated technology development

02 New technology assurance (ensuring it is robust and up to the task)

03 Cyber security measures around systems integration

04 Compatibility and interoperability between different defence systems and platforms

05 Research and development for Multi-Domain systems

Mindset and culture

Mivy James, Digital Transformation Director, BAE Systems Digital Intelligence

"Historically, defence organisations have been built on hierarchies and this remains a key part of military culture today. However, to achieve Multi-Domain Integration, there needs to be a shift from exclusively looking up to also looking, and moving, across domains."

"The domain-focused, hierarchical defence culture has infiltrated technology as well which means systems and data don't flow freely. A cross-domain information flow needs a collaborative culture to exist, and vice versa."

Industry conversations have argued that contrasting attitudes, behaviours and cultures are some of the biggest barriers to achieving a unified mind-set between domains.

The Ministry of Defence has implemented a 'One Defence Mindset. As summarised by Andy Start, CEO of the UK Ministry of Defence's Defence Equipment and Support team: "One of the things that has become really clear to me is that Defence needs to act as one entity and a 'One Team' mind-set will be vital to our success. This is about everyone working together to achieve Defence's goals and better protect the United Kingdom, its territories and our allies… We therefore need to integrate defence-wide and step away from operating in separate stove-piped workstreams, collaborating across boundaries and disciplines to work towards a common goal."

Cross-industry standards, legislation and policy

Nick Peach, CTO, 2iC Limited

"It is essential to proactively create standards that foster an environment where Multi-Domain Integration becomes ubiquitous. Clear standards will allow defence to implement sophisticated technology and share its value across teams and domains safely and efficiently."

NATO has argued that recent conflict has brought the importance of global standards into the limelight, revealing how important they are to achieving interoperability.

There are currently multiple standards used across the likes of information storage and sharing, across platforms, domains and allies. As well, within national militaries, there is no clear authority to mandate standards for different domains to follow. Each military is creating its own data sharing and command solutions, often in isolation to other services across land, sea and air. Suppliers have been brought in to provide individual bespoke solutions and until recently, there hasn't been a drive for industry to coordinate efforts and create common standards.

At BAE Systems Digital Intelligence, we are bringing together industry and military subject matter experts to collectively discuss the type of standards that might support successful Multi-Domain Integration.

Sidharth Kaushal, Research Fellow, Sea Power - Military Sciences, RUSI

"Regulatory standards are undeniably a central concern when addressing the successful implementation of Multi-Domain Integration.

"While many nod in agreement to the conceptual need for standards and interoperability, the on-ground reality poses a unique set of challenges. It's imperative we strike a balance - leveraging the robustness of a diverse technological landscape, while ensuring the system remains cohesive and does not collapse under its own complexity.

"We can draw inspiration from the shared communication standards of the internet and Open Banking. Their multi-layered approaches merge stringent standards with flexibility, presenting promising frameworks for defence integration."

Technology for collaboration

The research shows varying levels of adoption of new technology across the different nations surveyed. For example, looking at AI and machine learning, 77% of respondents in Canada agreed that their military has implemented AI and machine learning in defence operations to some extent. This rises to 86% of respondents from UAE and The Kingdom of Saudi Arabia, and 88% of respondents in the UK and Australia, with the Nordics leading the way at 94%.

As recognised by the UK Ministry of Defence's Science and Technology Strategy 2020, which has as its Strategic Framework's first objective to sustain advantage through science and technology, technological collaboration is one of the enduring challenges that will prevent the nation from achieving that. Namely:

- Full spectrum, multi domain intelligence, surveillance and reconnaissance (ISR): having this allows nations to respond to the threats and opportunities of emerging technologies affecting our ability to conduct ISR in all domains and environments through affordable resilient solutions.
- Multi-domain command and control, communications and computers (C4): enabling the capability for Multi-Domain Integration and the ability to coordinate effects globally enabling us to execute joint operations against adversaries with well integrated and resilient capabilities.

Mark Thistlethwaite, Head of International Campaigns and Business Development, BAE Systems Digital Intelligence

"As acknowledged by NATO in recent conversations, the Nordic countries are amongst those who are paving the way when it comes to bringing in and applying some of the latest technologies, demonstrating the importance of agility and collaboration in defence procurement. Other nations may take inspiration from this approach."

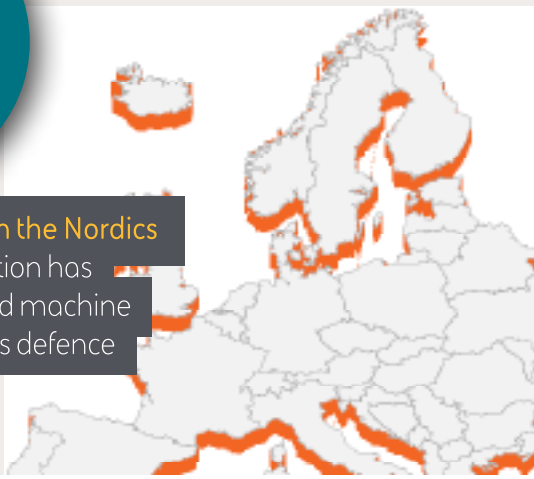
The cybersecurity risk

Interestingly, despite cyber being recognised as one of the greatest vulnerabilities affecting the modern battlespace, only the UAE and The Kingdom of Saudi Arabia recognised it as the top technological barrier preventing Multi-Domain Integration. With the speed of technological innovation meaning that cybercriminals sometimes identify vulnerabilities before developers, it is important that the cybersecurity risk remains a top concern.

Tied to the lack of industry standards, adopting new technology into existing networks can also result in vulnerabilities being unidentified as technologists implement solutions without clear direction on best practice.

93%

respondents in the Nordics agree their nation has adopted AI and machine learning across defence operations



Sidharth Kaushal, Research Fellow, Sea Power – Military Sciences, RUSI

"System integration, spanning domains, nations and industries, inevitably raises cybersecurity concerns. While there's unanimous agreement on the need for greater integration, particularly in our collaboration with allies, we must be prepared for the inherent challenges this brings.

"Integration at this scale isn't just about technology; it's a transformative journey prompting us to revisit and potentially disrupt long-standing procedures. It's essential that we approach this evolution with caution, ensuring we balance the promise of unified systems with the potential risks they might introduce."

There is no doubt that the severity of the cybersecurity risk is acknowledged by all nations. The Australian Cyber Security Centre (ASCS), U.S. Cybersecurity and Infrastructure Security Agency (CISA), U.S. Federal Bureau of Investigation (FBI), U.S. National Security Agency (NSA), and the UK's National Cyber Security Centre (NCSC) launched a joint advisory at the start of 2022 to tackle the cyber threat (specifically from ransomware) on all sectors, especially critical national infrastructure.

Chapter 3:
Looking ahead: Making Multi-Domain Integration a reality

By working together across industry, allies and partners, we can build collaborative cultures, establish resilient standards and implement technology to bring Multi-Domain Integration to life

Key Insights

As the key focus areas for adoption can be grouped into people, process and technology, so too can the solutions enabling defence organisations to adopt Multi-Domain Integration.

Supporting employees to handle information-rich environments, system interoperability to strengthen integration of defence technology, and systems that can manage a constantly evolving landscape are all needed to prepare nations for the future battlespace.

Respondents acknowledged both government (58%) and industry (57%) should play a role in providing resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition.

> "With the right information, forces get a real increased sense of situational awareness which enables **better decision making.**"

The solutions

The people, process and technology areas recognised in the previous section are all factors that require long-term commitment. To achieve Multi-Domain Integration requires a degree of continued transformation across all areas of defence. The good news is that many nations recognise the need to enable change, and have started implementing strategies to do so (such as the UK Ministry of Defence's Integrated Operating Concept).

Reflecting the key areas outlined in the last section: cultural changes within defence teams need to become more open to encourage more cross-domain collaboration; nations need to adopt internationally-recognised open standards that allow better secure integration between domains and allies; and technology needs to be developed with an openness that means it can be used to achieve an advantage across teams.

People-focused solutions

A more open culture to promote collaboration

The research has told us that collaboration is key, with 89% of respondents agreeing better coordination is important for national resilience.

Closely connected to cultural change requirements are diversity and inclusivity goals such as those laid out in the UK Army's Operation Teamwork plan.

Furthermore, the UK Army's Future Soldier strategy, which incorporates teamwork, also outlines a restructured army which encourages more integration within the land domain and beyond as part of Defence's Integrated Force. This strategy, and others like it across domains, recognise that a more open culture is key to managing modern challenges affecting the battlespace, including, "...the proliferation of technology… [and] the information age…" as well as, "... the impacts of globalisation… and climate change."

Process-focused solutions

Establishing an open standards framework

As the last section outlined, respondents cited regulatory standards as important for the implementation of Multi-Domain Integration.

The concept of open standards when it comes to defence technology and Multi-Domain Integration is currently being debated and discussed by subject matter experts in a number of forums. Standards have the potential to prevent vendor lock-in, create incentives that encourage and enhance collaboration, and ultimately result in future-proofed intelligence and deterrence strategies.

Andy Linton, Head of Future Maritime Aviation Force, BAE Systems - Air

"The gradient of technology advancement is ever steepening. A chipset that today enables the latest level of processing power could be obsolete by the time the capability it's powering enters operational service.

"To overcome this challenge, we need to develop and embed open architectures which properly separate software and hardware as well as develop the standards and protocols employed in the digitisation process for longevity. If they remain consistent, organisations can upgrade capability through software updates or refresh hardware more easily without having to unpick everything they've already achieved and potentially degrading connectivity across domains.

"We need to reach a stage where capabilities run on open, robust yet flexible architectures designed around a standardised set of protocols that allow organisations to adopt the latest technology and applications at pace, giving the frontline the advantage they need."

> "Standards have the potential to prevent vendor lock-in, **create incentives that encourage and enhance collaboration,** and ultimately result in future-proofed intelligence and deterrence strategies."

The defence ecosystem working together

What role, if any, does the defence industry and private sector play in shaping future military operations?

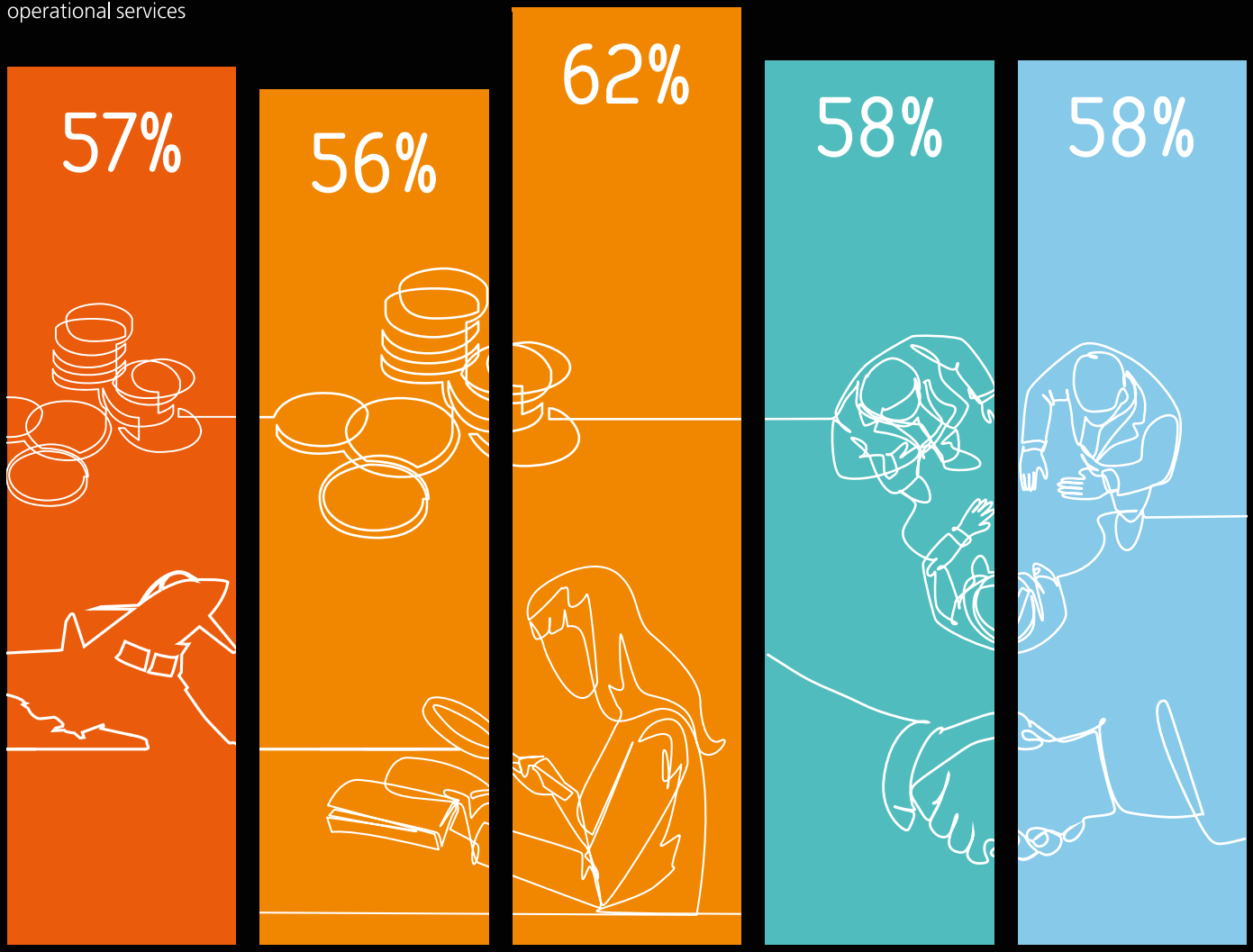
UK - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition and become more involved in the provision of military operational services

Canada - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition

Nordics - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition

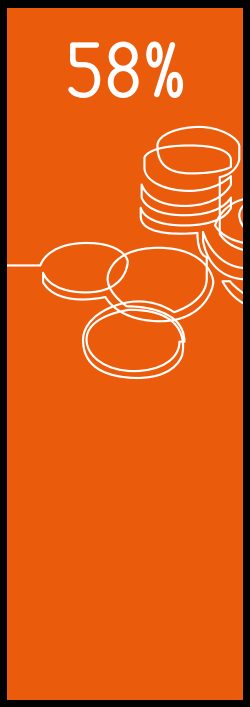
Australia - Define and develop standards and best practices for Multi-Domain Integration to ensure interoperability and effective collaboration

Middle East - Build partnerships that promote Multi-Domain Integration and enable effective collaboration in the future battlespace

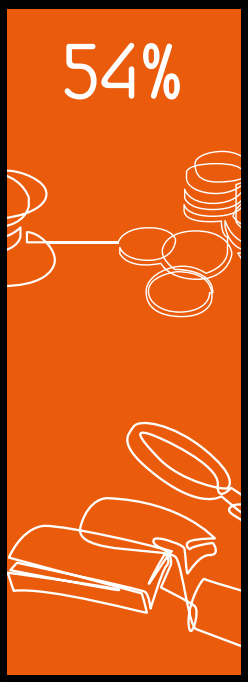


What role, if any, does the government, public and military play in shaping future military operations?

UK - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition

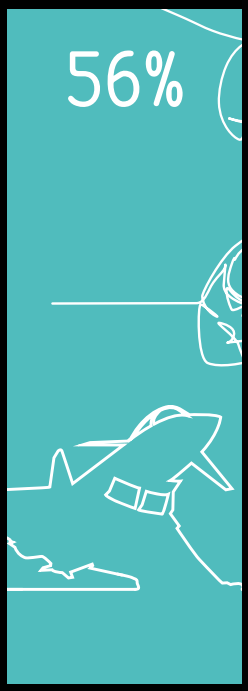


Canada - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition



Nordics - Provide resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition

Australia - Build partnerships that promote Multi-Domain Integration and enable effective collaboration in the future battlespace and share their expertise on Multi-Domain Integration to develop more effective strategies



Middle East - Build partnerships that promote Multi-Domain Integration and enable effective collaboration in the future battlespace

Andy Linton, Head of Future Maritime Aviation Force, BAE Systems - Air

"The key to successfully implementing Multi-Domain Integration is achieving a much more collaborative approach between industry and defence. Defence is developing detail around the operational need but there is a requirement to engage with industry holistically as the thought leaders on the art of possible. Individually, industry players are experimenting with elements of Multi-Domain Integration but we need to bring everyone together to see the big picture. That's why at BAE Systems we are seeking to establish working groups that allow industry stakeholders to play an active role in supporting the development of defence strategies."

Technology-focused solutions

Using data to improve operational readiness and availability

95% of respondents agree that technology advancements are blurring the lines between physical and digital domains, requiring militaries to adapt how they operate. BAE Systems Digital Intelligence's provision of future-ready battlespace hardware and services support customers globally to break down silos with technology built for collaboration, giving them decision advantage when and where they need it most.

Our technology supports the digitally connected deployed battlespace across the operational domains. For example:

- **Our Digital Asset Management capability** builds digital threads between customers' most complex platforms and their support networks, for improved planning and data-driven decisions. This optimises the operational time of a military's mission-critical physical assets, ensuring they're available at the right place at the right time to support successful delivery across domains.
- **Our Platform Mission Planning Solutions** can rapidly plan complex operations while presenting information in a simple manner that is easy to manipulate, providing clarity in an increasingly data rich world. These tools continuously evolve to manage complicated, autonomous tasking problems across assets, whether they are humans, crewed or uncrewed platforms, and for use cases from logistics and resupply to joint operations.

> "**95% of respondents agree** that technology advancements are blurring lines between physical and digital domains, requiring militaries to adapt how they operate."

Driving enhanced situational awareness and decision making with AI and Machine Learning

Using AI and Machine Learning technologies to achieve a decision advantage was the second most important focus (50%) for defence technology exploitation. Reflecting this, 86% have already either fully or partially adopted AI and Machine Learning technologies across their defence operations. We support this objective by providing defence organisations with a decision advantage through AI and Machine Learning enabled enhanced situational awareness. For example:

Our Analytics and Machine Learning solutions appropriately and ethically turn ideas into impact, allowing defence organisations to process and analyse data to reveal insights that improve efficiency, reduce costs, increase competitiveness and fulfil missions.

Our Digital Transformation capabilities merge technology, intelligent doctrine (not rote process), critical thinking, training, collaboration, and people. Drawing on experience across multiple domains, our 360° digital transformation expertise is unrivalled in the defence industry.

Our Command, Control (C2) & Intelligence solutions help customers make sense of the future battlespace. They use open source tools to collaborate with MOD modules, taking sensor information, raw data and intelligence to enable C2 and situational awareness as a mission evolves.

Our UAS expertise allows autonomous systems, like small Uncrewed Air Systems, to play a key role in a connected, information-rich landscape. We elevate and mature emerging technology across platforms and sensors, integrating payloads to deliver solutions that meet commanders' needs.

Paul Spedding, Head Strategy Innovation and Marketing Defence Data Services, BAE Systems Digital Intelligence

"AI has a powerful future role to play from strategic through to tactical operations, helping us make sense of large data sets and complex interactions to support faster and better decision making and action. We must embrace AI, but we must also ensure that we understand how it reaches its recommendations and the implications of bias and limitations on data sets, if we are to ensure users can trust the tools we provide to help them."

Jason Smithurst, Strategic Campaign Lead, KSA, BAE Systems Digital Intelligence

"Digital Transformation enables (and is enabled by) business improvements (in people, process and technology) which, together, deliver game-changing efficiencies (including cost, workforce and pace). While the UK may have paved the way for embracing Multi-Domain Integration with the creation of Strategic Command, we're seeing other nations follow suit and catch up quickly.

"The Kingdom of Saudi Arabia is a good example. As evidenced by the newly formed Saudi Joint Forces Command here, there's a recognition that adopting a new Target Operating Model (TOM) will ultimately help to improve collaboration, reduce stress in tough environments and enable a comprehensive transformation of defence."

Connecting the deployed battlespace across land, maritime, air, space and cyber domains

We have delivered UK secure operational C4I (Command, Control, Communications, Computer and Intelligence) systems for decades and are recognised as a key strategic supplier to the UK Ministry of Defence.

Examples of our solutions:

Our Space-enabled solutions deliver a step-change in space capabilities, empowering governments, armed forces, civilian agencies and commercial enterprises to realise their space ambitions and data needs. In 2025, we plan to launch the first cluster of our Azalea programme satellites to deliver multi-sensor coherent data in real time to military customers across all domains and get intelligence to wherever it's needed.

Our Cyber Security Services understand customers' threats and vulnerabilities, securing their platforms, and responding to active intrusions. We are one of the few organisations that can combine a deep understanding of hostile state threats, expertise in a wide range of military platforms, communications and information systems, with the capacity to deliver specialist cyber consultancy, tools and agile teams across the globe.

We bring automation and network bandwidth and availability optimisation to the point of need so commanders can rapidly access information. Our high integrity software for Battlefield Information System Applications supports Ground Based Air Defence, and we design and develop Command and Control solutions to meet the demands of the Dismounted Soldier.

Our Cross Domain Solutions enable the formation of digital threads by providing high speed packet processing and Cross Domain information exchange capabilities for the most secure and mission-critical organisations on earth.

Dr Kathryn O'Donnell, Chief Operating Officer, In-Space Missions Limited

"Space-based infrastructure is an essential part of Multi-Domain Integration's operational capability. Not only does it provide unique, real-time data sets to the end user, but this data is accessible globally, making it an essential part of any military ecosystem. Constellations and clusters of Low Earth Orbit satellites can provide a wealth of imagery and other data across a wide range of the electromagnetic spectrum, and the combination of this with powerful on-board data processing capability and communications links to other satellite - and road, air and naval vehicles - provides a powerful, integrated network and knowledge base."

Use of synthetic environments to inform product/system development

92% of respondents agree that diverse defence technology ecosystems offer an opportunity for better resilience. Synthetic environments, are a key part of this with 69% already having adopted this technology. We support the creation of digital enabled platforms through digital asset management and synthetic environments to improve operational readiness and advantage. For example:

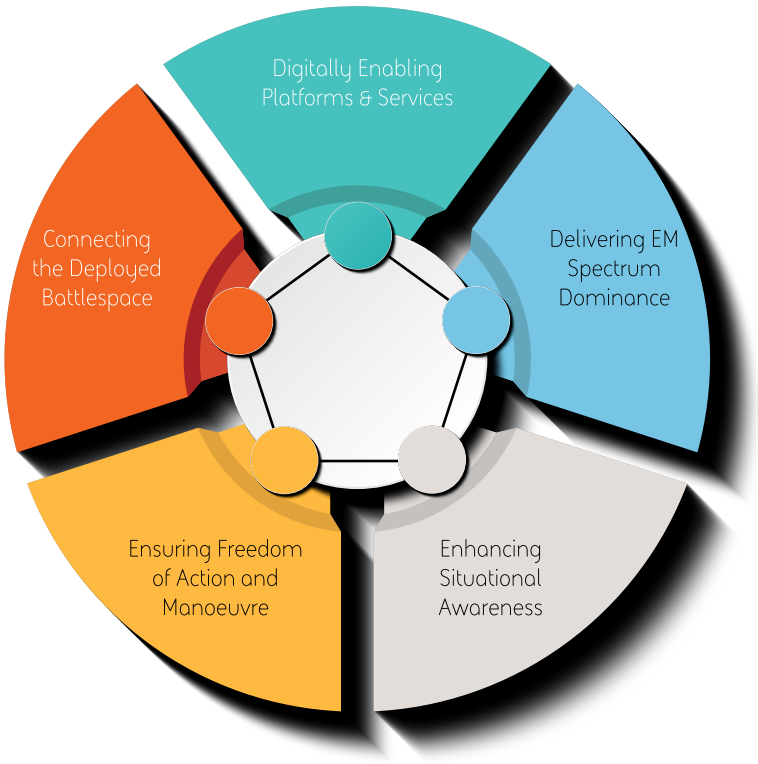
- Using our domain and customer experience, we have developed Synthetic Environment Platforms, aligned to the Ministry Of Defence's Digital Backbone, that are evolving along our products to test and improve them at pace. This supports high release frequency and simultaneously builds an environment supporting mission rehearsal and wargaming of the future.

Gaining electromagnetic (EM) spectrum dominance

Respondents acknowledge CEMA's (Cyber and Electro Magnetic Activities Systems) role in achieving a decision advantage, with 72% already adopting this technology. Our sense and effect CEMA domain capabilities provide our customers with EM spectrum dominance. For example:

- Our CEMA solutions help customers understand the electromagnetic environment they are operating in. They then give customers the ability to manage, synchronise and control their activities to protect equipment and personnel, while delivering operational advantages that simultaneously deny and degrade adversaries' use of the physical and digital battlefield.
- We have many years of CEMA expertise across National Security, specialist domain knowledge and are at the forefront of Research and Capability development producing outputs supporting customers' missions. We also provide CEMA systems and supporting components in the RF (Radio Frequency) domain including antennas, software defined radios and associated packaging and electronics.

> "Space-based infrastructure is an essential part of Multi-Domain Integration's operational capability. Not only does it provide unique, real-time data sets to the end user, but this data is accessible globally, making it an essential part of any military ecosystem."



Digitally enabled platforms through digital asset management and synthetic environments to improve operational readiness and advantage

Sense and effect CEMA domain capabilities providing our customers with EM spectrum dominance

Decision advantage for our customers with AI/ML enabled enhanced situational awareness

Enabling high tempo precision strike, integrated Ground Based Air Defence & pervasive full spectrum intelligence, surveillance & reconnaissance

Digitally connected deployed battlespace across the operational domains

Mark Todd MBE, Head of Product Development, BAE Systems Digital Intelligence

"If systems are built in stove-piped ways (in isolation hindering cooperation) this impacts their ability to interoperate. To ensure the success of Multi-Domain Integration from a technology standpoint, you need to think across three key elements: data, network layer and communications.

"Data must be interoperable, either through the common implementation of standards or through the use of middleware. The network layer must connect data sources and sinks. Different data, depending on whether it's for command, control or convergence will have different characteristics, therefore a single system can't manage everything. Lastly, communications need to connect each of those network nodes, this requires the ability to use all of the electro-magnetic spectrum and have a common approach to the use of waveforms.

"The success of this integration relies on the characteristics of the data, an understanding of the electromagnetic spectrum, and systems' ability to remain resilient when contested and disrupted."

Conclusion

Multi-Domain Integration is crucial to achieve a decision advantage and shape the information battlespace of tomorrow

Key takeaways from this report

1#

Rapid technological change is reshaping warfare, including by increasing the size of the information battlespace and the scale of activity in the grey zone. These changes are blurring the lines between traditional domains, requiring collaboration to achieve an advantage against the adversary.

2#

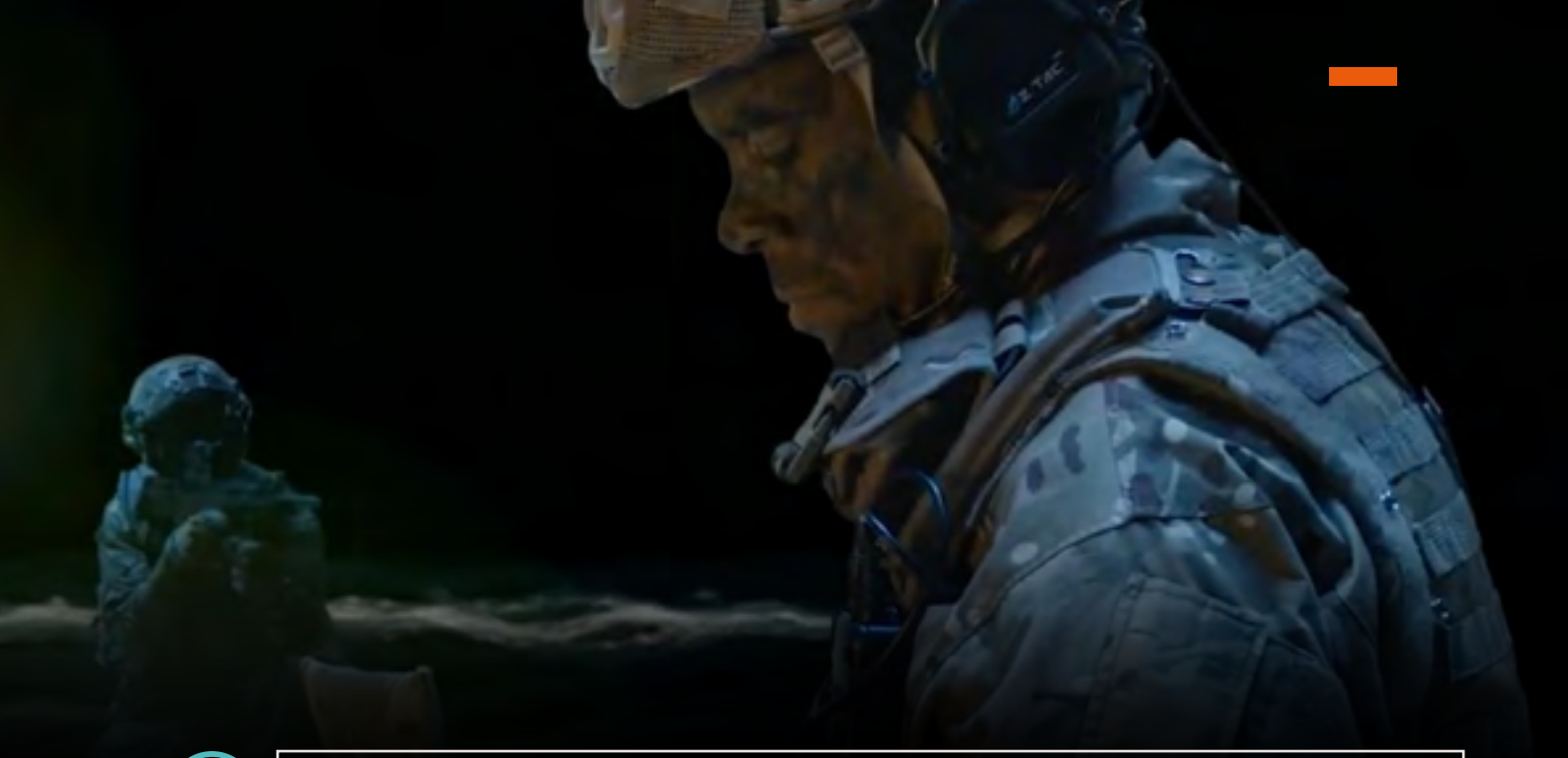
Multi-Domain Integration, which encourages data sharing and weaves digital threads between domains, gives nations a decision advantage against the adversary. Yet while its benefits are recognised by aerospace and defence respondents, even the most advanced nations are still at the beginning of their Multi-Domain Integration journey.

3#

There are significant areas of focus for nations adopting Multi-Domain Integration. These include enabling cross domain collaboration, building regulatory standards for Multi-Domain Integration programmes; and supporting the integration of technology.

4#

People, process and technology solutions require a secure openness that breeds collaboration. Defence's culture must securely open up to encourage collaboration between domains; it must work with industry to create open standards; and the sector must build technology that fosters Multi-Domain Integration.



- If Multi-Domain Integration is absent, increased complexity, uncertainty and volatility will be experienced by respondents' nations (83%)
- It allows for a proactive response to cybersecurity attacks and AI developments (93%)
- It enables a coordinated responses to emerging grey zone threats (90%)
- Multi-Domain Integration programmes counter misinformation in the grey zone (89%)
- It protects unmanned systems in the grey zone (83%)
- It improves situational awareness (54%), particularly supporting better understanding of complex operational environments

>> **Want to find out more** about how BAE Systems Digital Intelligence can help you achieve a decision advantage against the adversary?

With thanks to our contributors

Andy Linton
Head of Future Maritime Aviation Force, BAE Systems – Air

Antony Mrozicki
Product Owner FCAS, BAE Systems – Air

Dave Armstrong MBE
Group Managing Director, BAE Systems Digital Intelligence

Jason Smithurst
Strategic Campaign Lead, KSA, BAE Systems Digital Intelligence

Dr Kathryn O'Donnell
Chief Operating Officer, In-Space Missions Limited

Mark Fitton
Senior Engineering Sales Manager, BAE Systems Digital Intelligence

Mark Thistlethwaite
Head of International Campaigns and Business Development BAE Systems Digital Intelligence

Mark Todd MBE
Head of Product Development, BAE Systems Digital Intelligence

Martyn Orme
Head of Business Development, Techmodal

Mivy James
Digital Transformation Director, BAE Systems Digital Intelligence

Nick Peach
CTO, 2iC Limited

Paul Spedding
Head of Strategy Innovation and Marketing for Defence Data Services, BAE Systems Digital Intelligence

Pavandeep Bhogal
Head of Product Engineering, BAE Systems Digital Intelligence

Ron Dempster
Head of Business Development – Defence and Space Australia, BAE Systems Digital Intelligence

Sidharth Kaushal
Research Fellow, Sea Power - Military Sciences, RUSI (the Royal United Services Institute)

> Multi Domain Integration is **essentially about connectivity and the ability to effectively make timely decisions** in directing the employment of assets from across all five domains to achieve the greatest co-ordinated net military effect, faster than the adversary - **know sooner, decide quicker, act faster.**

References

Multi-Domain Integration
Strategic Command and Ministry of Defence (17 January 2022 - last updated 26 June 2023)

The Integrated Operating Concept 2025
Ministry of Defence (August 2021)

Getting to grips with grey zone conflict
Conrad Beckett, Ministry of Defence (26 April 2021)

'Chinese spy' targeted thousands over LinkedIn
Gordon Corera, BBC (24 August 2023)

COVID-19 vaccine misinformation
UK Parliament (26 April 2021)

Ideological extremism is the "primary form of radicalisation in Australia": security expert
ABC News (10 February 2022)

Australia: economic profile
OEC (accessed August 2023)

Saudi Arabia: economic profile
OEC (accessed August 2023)

Big data - statistics and facts
Statista (2 May 2023)

Data in defence: Weaving digital threads across multiple domains
BAE Systems Digital Intelligence (January 2023)

The Ukraine War: Shaping the Information Battlespace
Harsh V. Pant, The Observer Research Foundation (10 May 2023)

Drones in Ukraine and beyond: Everything you need to know
Ulrike Franke, European Council on Foreign Relations (11 August 2023)

Defend. Resist. Repeat: Ukraine's lessons for European defence
Hanna Shelest, European Council on Foreign Relations (9 November 2022)

Who is winning the war in Ukraine? Experts break down the territorial, psychological, and military gains made by Putin and Zelenskyy
Sophia Ankel, Business Insider (24 July 2023)

Russo-Swedish Wars
Michael Roberts, Encyclopedia Britannica (accessed August 2023)

Low Earth orbit satellite cluster to provide secure digital military intelligence from 2024
BAE Systems (7 September 2022)

The Impact of Digital Technologies
United Nations (accessed August 2023)

Joint All-Domain Command and Control (JACD2)
Congressional Research Service (21 January 2022)

Defense Global Market Report
The Business Research Company (January 2023)

Silicon Valley VCs rush into defence technology
Tabby Kinder, Financial Times (20 June 2023)

Digital Transformation
NHS: Digital Transformation (accessed August 2023)

Digitizing the City: How the UK's financial system is scrapping paper
Michael Carty, World Economic Forum (23 February 2023)

Policy paper: The UK's International Technology Strategy
UK Government Department for Science, Innovation & Technology, and UK Government Foreign, Commonwealth & Development Office (March 2023)

Desider: Start Talking
Andy Start, Ministry of Defence (November 2022)

The Digital Strategy for Defence: A review of early implementation
UK National Audit Office (19 October 2022)

Skill, re-skill and re-skill again. How to keep up with the future of work
Stephane Kasriel, World Economic Forum (31 July 2017)

It is broke - and it's time to fix it: The UK's defence procurement system
House of Commons Defence Committee (11 July 2023)

Global Britain in a competitive age: The Integrated Review of Security, Defence, Development and Foreign Policy
HM Government (March 2021)

Policy paper: Ministry of Defence's Science and Technology portfolio
UK Government Defence Science and Technology Laboratory and the Ministry of Defence (23 January 2023)

Spotlight on Cyber and Technology Risks 2023
Beazley (accessed August 2023)

Australia US and UK stand together to confront global ransomware threat
Australian Government: Defence (10 February 2022)

Time out to Team Up
UK Army (11 February 2022)

Future Soldier Guide
UK Army (30 November 2021)

Defence outlines 2030 vision for the armed forces
Ministry of Defence (22 March 2021)

Unlocking digital advantage in high trust sectors
BAE Systems Digital Intelligence (XX)

STEM student shortage risks a national security crisis, education experts warn
Shashi Baltutis, The Advertiser (21 May 2023)

The Aerospace Talent Shortage Is Complex. Solutions Can Be Simple.
Kristy Kiernan, Forbes (6 March 2023)

Government urged to tackle 'shocking' skills shortage by adding engineering to curriculum
Institution of Mechanical Engineering (8 December 2022)

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,700 digital, cyber and intelligence experts. We work collaboratively across 16 countries to collect, connect and understand complex data, so that governments, nation states, armed forces and commercial businesses can unlock digital advantage in the most demanding environments. Launched in 2022, Digital Intelligence is part of BAE Systems, and has a rich heritage in helping to defend nations and businesses around the world from advanced threats.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Malta Office Park
ul. Abpa A. Baraniaka 88
Poznan
61-131
Poland
T: +44 (0) 330 158 3627

BAE Systems Digital Intelligence
Level 2
14 Childers St
Canberra
ACT 2601
Australia
T: +61 (0) 2 9053 9330

BAE Systems Digital Intelligence
Level 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

BAE Systems, Surrey
Research Park, Guildford,
Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

X.com/BAES_digital

Copyright © BAE Systems plc 2023. All rights reserved.

BAE SYSTEMS, the BAE SYSTEMS Logo and the product names referenced herein are trademarks of BAE Systems plc.

BAE Systems Applied Intelligence Limited registered in England & Wales (No.1337451) with its registered office at Surrey Research Park, Guildford, England, GU2 7RQ.

No part of this document may be copied, reproduced, adapted or redistributed in any form or by any means without the express prior written consent of BAE Systems Digital Intelligence.

BAE SYSTEMS