Multi-Domain Integration
The view from Australia

Digital
Intelligence

BAE SYSTEMS

Decision Making in the Battlespace of the Future

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 commentary with data from our broader global study of more than 400 respondents in the UK, Canada, 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

Methodology

50

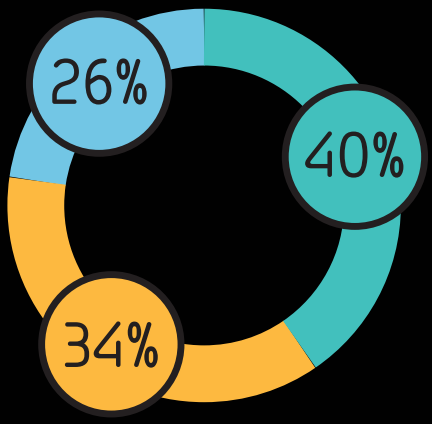
Senior IT decision makers and senior business decision makers working in aerospace or defence

90%

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



Story in numbers

We surveyed 50 senior business and IT decision makers in defence and aerospace from Australia about the evolving battlespace and their perspectives on **Multi-Domain Integration.**

The Modern Battlespace is Digital

94% 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

100% agree an evolution of processes will be essential for navigating the complexities of modern defence

Multi-Domain Integration is Mission Critical

96% of respondents say that Multi-Domain Integration is important in shaping military operations today

100% 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 **(50%)** and national security breaches **(44%)**

86%

Ready to deploy

86% of respondents across Australia feel their nation is 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

90% agree

Diverse defence technology ecosystems to offer an opportunity to promote resilience

52% agree

The ability to use data to improve operational readiness and availability

52% 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.

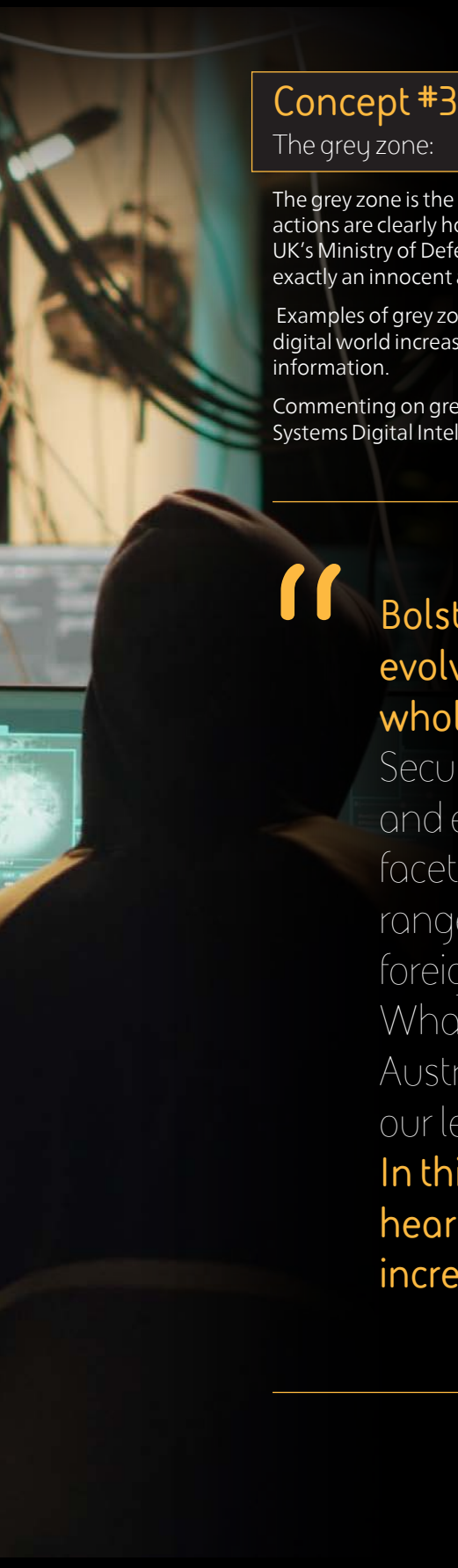
Concept #2.
The information battlespace:

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.

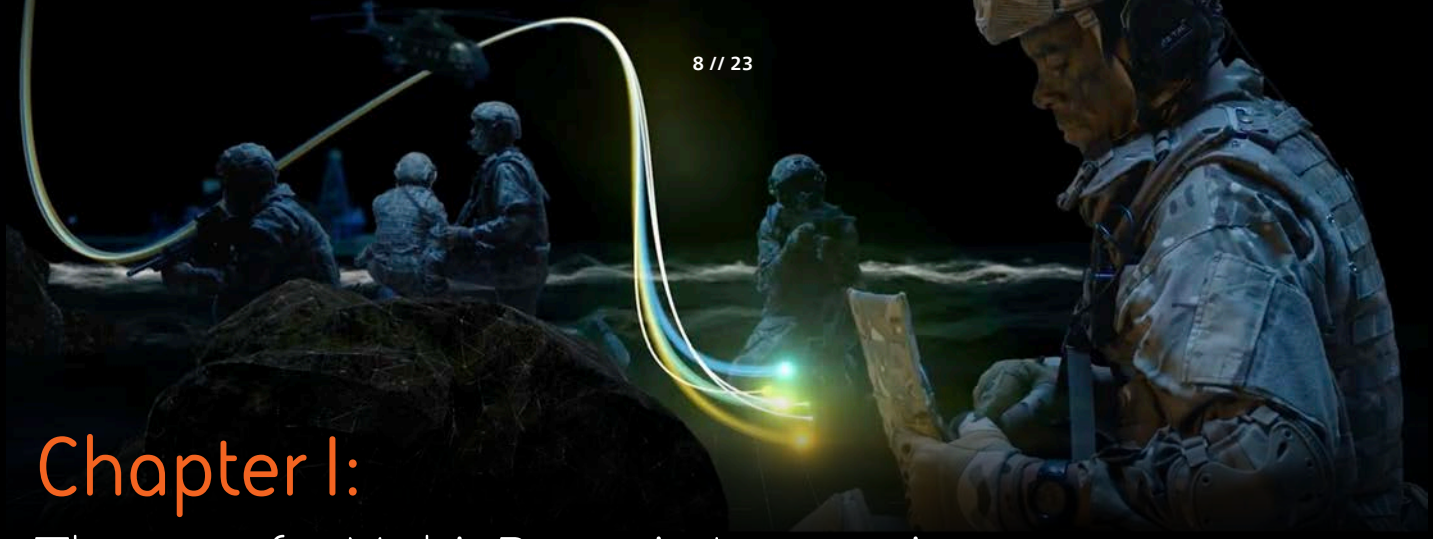
The grey zone:

The grey zone is 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 UK's 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 cyber-attacks (the most common form of grey zone attack as the digital world increasingly becomes an important part of the battlespace), to espionage, to mis- and dis-information.

Commenting on grey zone activity in Australia, Andrew Robertson – Head of Business Development, BAE Systems Digital Intelligence Australia – said:

> "Bolstering security measures to address and mitigate evolving threats is a constant challenge across the whole defence spectrum. The Director-General of Security has identified the significant foreign interference and espionage threat to Australia. This is a multi-faceted threat which must be countered through a range of measures. Given public reporting suggesting foreign agents use social networking apps such as WhatsApp, LinkedIn and even Tinder to approach Australians with the knowledge of government secrets, our legislative and policy responses continue to evolve. In this context, it's important to put security at the heart of our defence systems, especially in a world of increased integration."



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 **76%** across Australia saying it is crucial or very important to shaping their military operations today.

As defence organisations adopt cutting edge technologies such as data and intelligence analytics solutions **(96%),** AI and Machine Learning tools **(88%),** and robotics and autonomous systems **(88%)**, it's important to recognise that these technologies need to be integrated effectively to achieve their full potential.

The top three benefits of Multi-Domain Integration

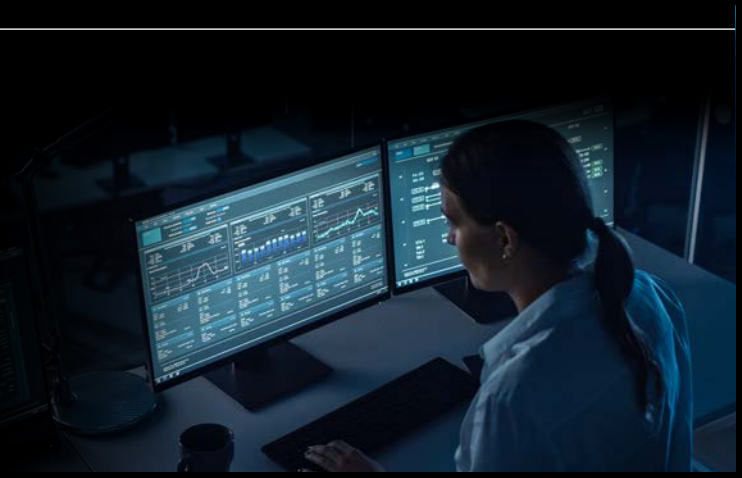
Which benefits do Australian respondents think their nation can reap from implementing Multi-Domain Integration?

Most respondents recognised the many benefits of Multi-Domain Integration. The top three benefits all point to Multi-Domain Integration's powerful value in supporting better data use in a fast-paced battlespace to give nations the advantage against the adversary – either in advance of or during operations.

01 Improved situational awareness

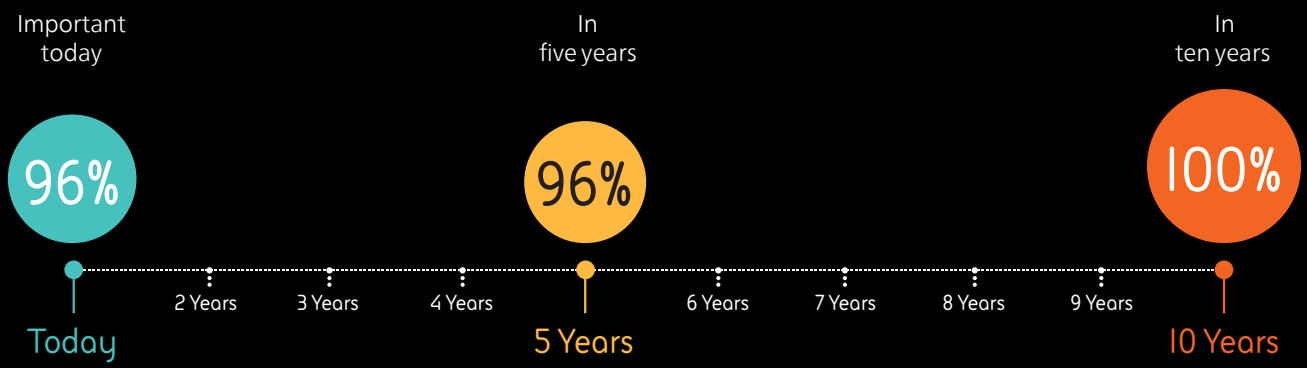
02 Improved quality of decision making

03 Improved preparation for potential warfare



Why Multi-Domain Integration adoption is a matter of urgency

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



The importance of Multi-Domain Integration in shaping military options today versus in 10 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

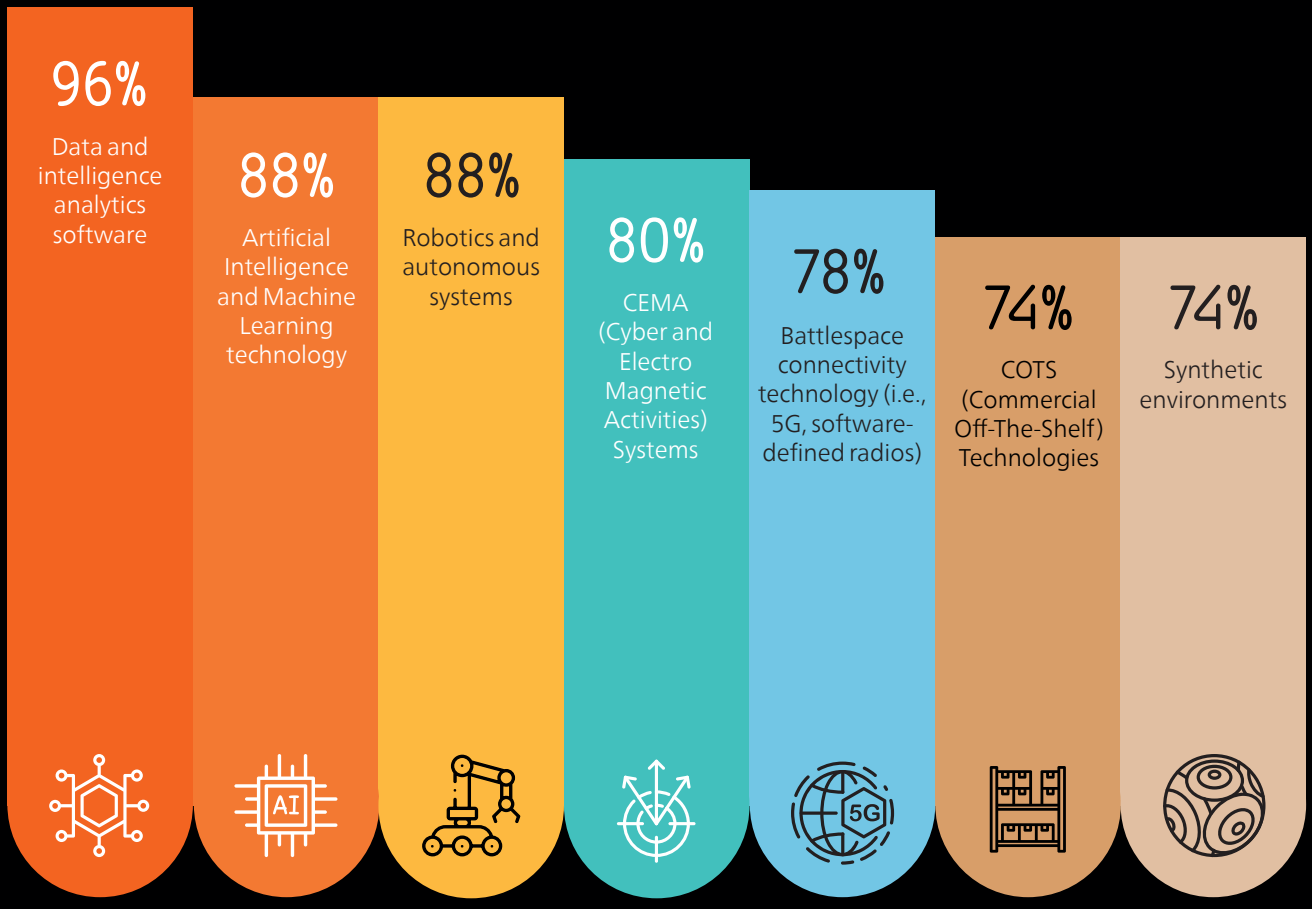
04 The introduction of new forms of warfare

05 Lack of safety in society

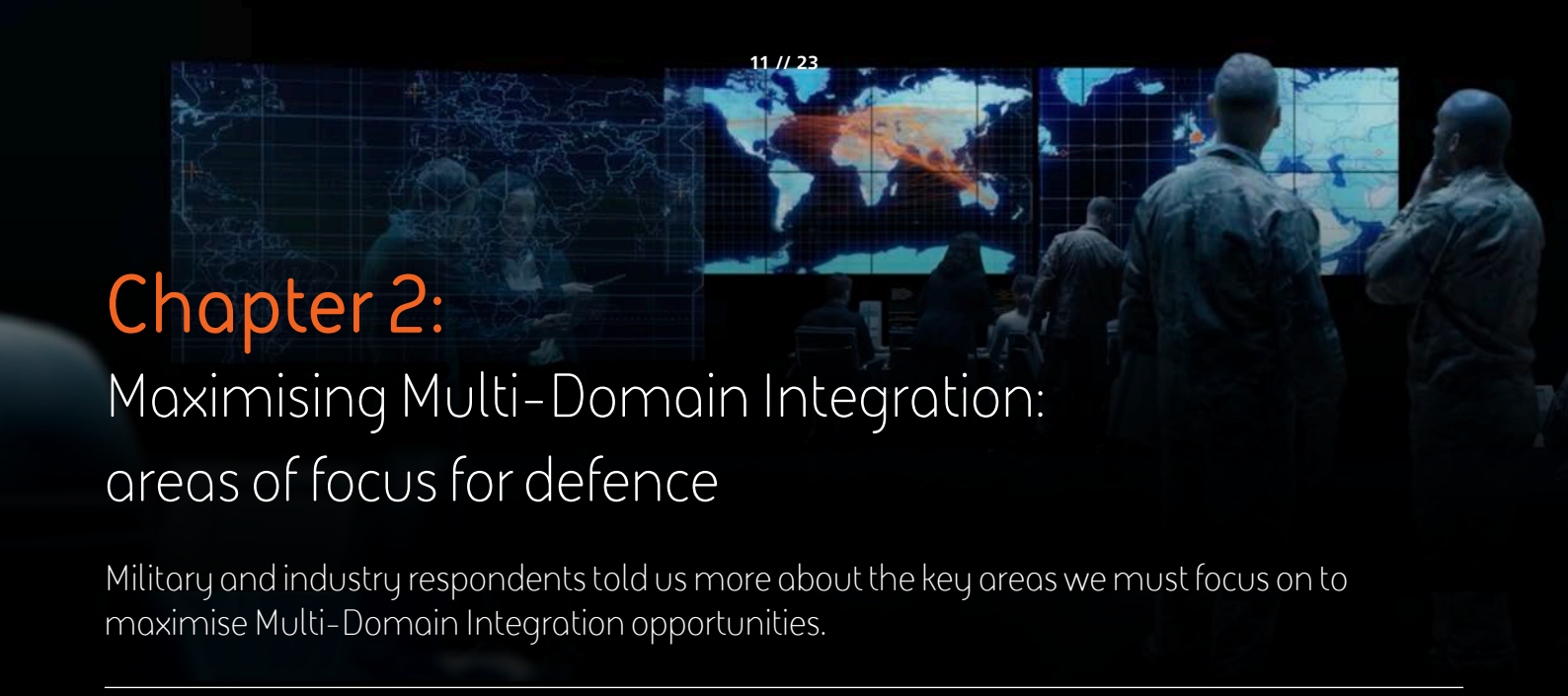
Multi-Domain Integration and the adoption of new defence technology

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.



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.

92% 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 Innovating despite time pressures

02 Willingness to collaborate across military departments

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

04 Providing training to support the adoption of new technology

05 Aligning priorities between military/defence departments

Focus on: process

01 Acquisition processes for Multi-Domain Integration technology

02 Collaborative working between different siloes and domains

03 Understanding and strategy around business change

04 Aligning priorities between allies

05 Effective strategic planning

Focus on: technology

01 Removing the siloes that limit system collaboration in technology development

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

03 Cyber security measures around systems integration

04 Overcoming legacy system integration challenges

05 Research and development for Multi-Domain systems

Technology for collaboration

Our research shows that Australia leads the way in several areas of technology adoption. For example, **88%** of respondents agreed that their military has adopted robotics and autonomous systems across its defence operations, compared to **76%** in the UK and **68%** in the Nordics. The same is true for cyber & CEMA, with Australia **(80%)** some way ahead of Canada **(69%)** and the United Arab Emirates (UAE) **(64%)** in terms of adoption.

Technological collaboration will be key to maintaining this position over the coming years, particularly in areas such as:

- **Full spectrum, multi-domain intelligence, surveillance and reconnaissance (ISR):** 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 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, powering join operations against adversaries with well integrated and resilient capabilities.

Cross-industry standards, legislation and policy

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.

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.

Decision Making in the Battlespace of the Future

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 industry (54%) and government (50%) should play a role in providing resources to develop and implement Multi-Domain Integration strategies, such as R&D, training and new technology acquisition.

Respondents also highlighted industry's role in defining and developing standards and best practices for Multi-Domain Integration to ensure interoperability and effective collaboration (58%), with the government focus shifting towards building partnerships that enable effective collaboration (56%) and sharing their expertise to help develop more effective strategies (56%).

> "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. Achieving Multi-Domain Integration requires a degree of continued transformation across all areas of defence. The good news is that Australia recognises this and is now implementing strategies within its wider social and economic plans for the future.

For example, the Australian Defence Force (ADF) is already addressing multi-domain operations from a planning perspective by drawing on the Joint Targeting Cycle (JTC) framework to synchronise joint force kinetic and non-kinetic effects for MDOs. This is taking a step forwards from more stove-piped approaches that have traditionally been used to orchestrate operations across the physical domains of land, sea and air.

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.

Other areas of focus could include:

- Fostering a more open culture to promote collaboration: the research has told us that collaboration is key, with 90% of respondents in Australia agreeing that better coordination is important for national resilience.
- Establishing an open standards framework: Respondents cited standards and best practices as important for the implementation of Multi-Domain Integration. Australia respondents had the joint highest response with the UAE (58%) in recognising industry's role in defining and developing these standards.

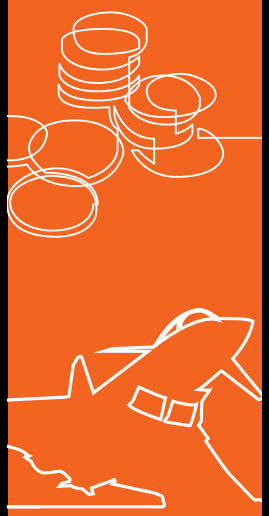
In particular, the concept of open standards when it comes to defence technology and Multi-Domain Integration is currently being debated and discussed in a number of forums. Standards have the potential to prevent vendor lock-in, create incentives that encourage and enhance collaboration, and ultimately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

The defence ecosystem working together

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

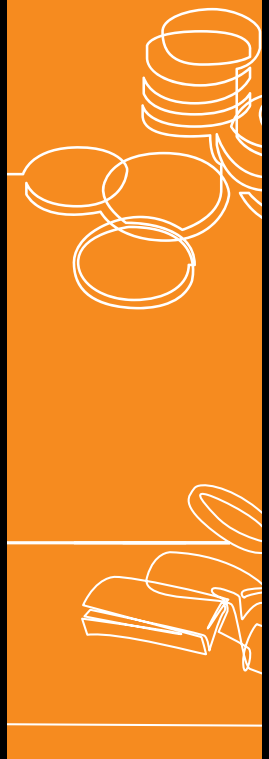
Define and develop standards and best practices for Multi-Domain Integration to ensure interoperability and effective collaboration

58%



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

54%



Share their expertise on Multi-Domain Integration to develop more effective strategies

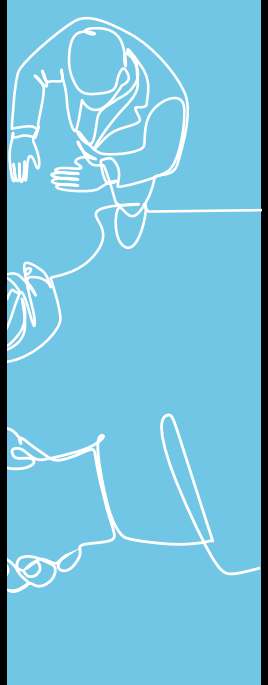
46%

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

44%

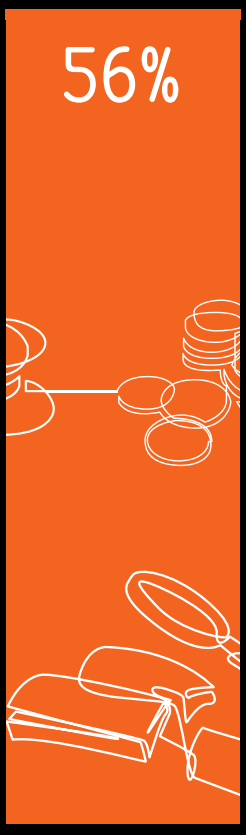
Become more involved in the provision of military operational services

44%



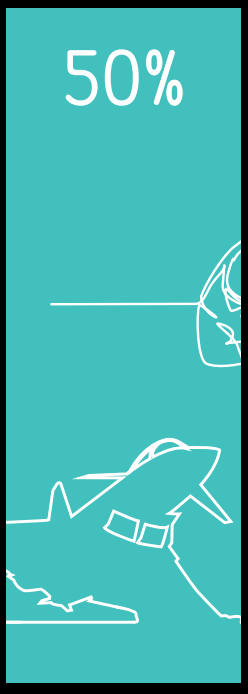
What role, if any, does the government, public and military play in shaping future military operations?

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



Share their expertise on Multi-Domain Integration to develop more effective strategies

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



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

Technology-focused solutions

Using data to improve operational readiness and availability

98% 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."

Decision Making in the Battlespace of the Future

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

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

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 satellite in our Azalea programme to deliver multi-sensor data in real-time to military customers across all domains and get intelligence to wherever it's needed.

Our Cyber Security teams 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.

Decision Making in the Battlespace of the Future

Use of synthetic environments to inform product/system development

90% of respondents agree that diverse defence technology ecosystems offer an opportunity for better resilience. Synthetic environments, are a key part of this with **74%** saying Australia has already adopted this technology across its defence operations.

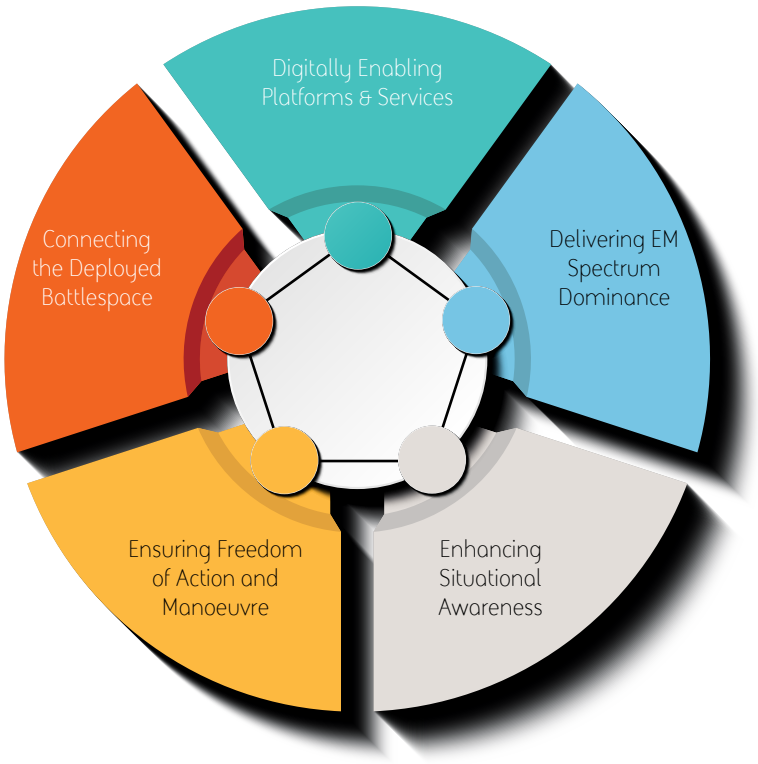
We support the creation of digital enabled platforms through digital asset management and synthetic environments to improve operational readiness and advantage. For example:

- 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 80% saying Australia has already adopted 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.



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

Embracing space for visibility and data insights

96% of Australian respondents – the highest in our global survey – believe space will become an essential component in national defence. Space-based infrastructure therefore forms 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. We have a long heritage in the space domain and are investing further in space to deliver a step-change in capabilities for our customers. For example:

- Through our Azalea programme, we will be launching a cluster of multi-sensor satellites with unique ISR capabilities into low Earth orbit. The satellites will collect data from a range of sensors – including RF and SAR (synthetic aperture radar) data – and analyse this information in-orbit, using on-board machine learning to deliver intelligence wherever it's needed.

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#

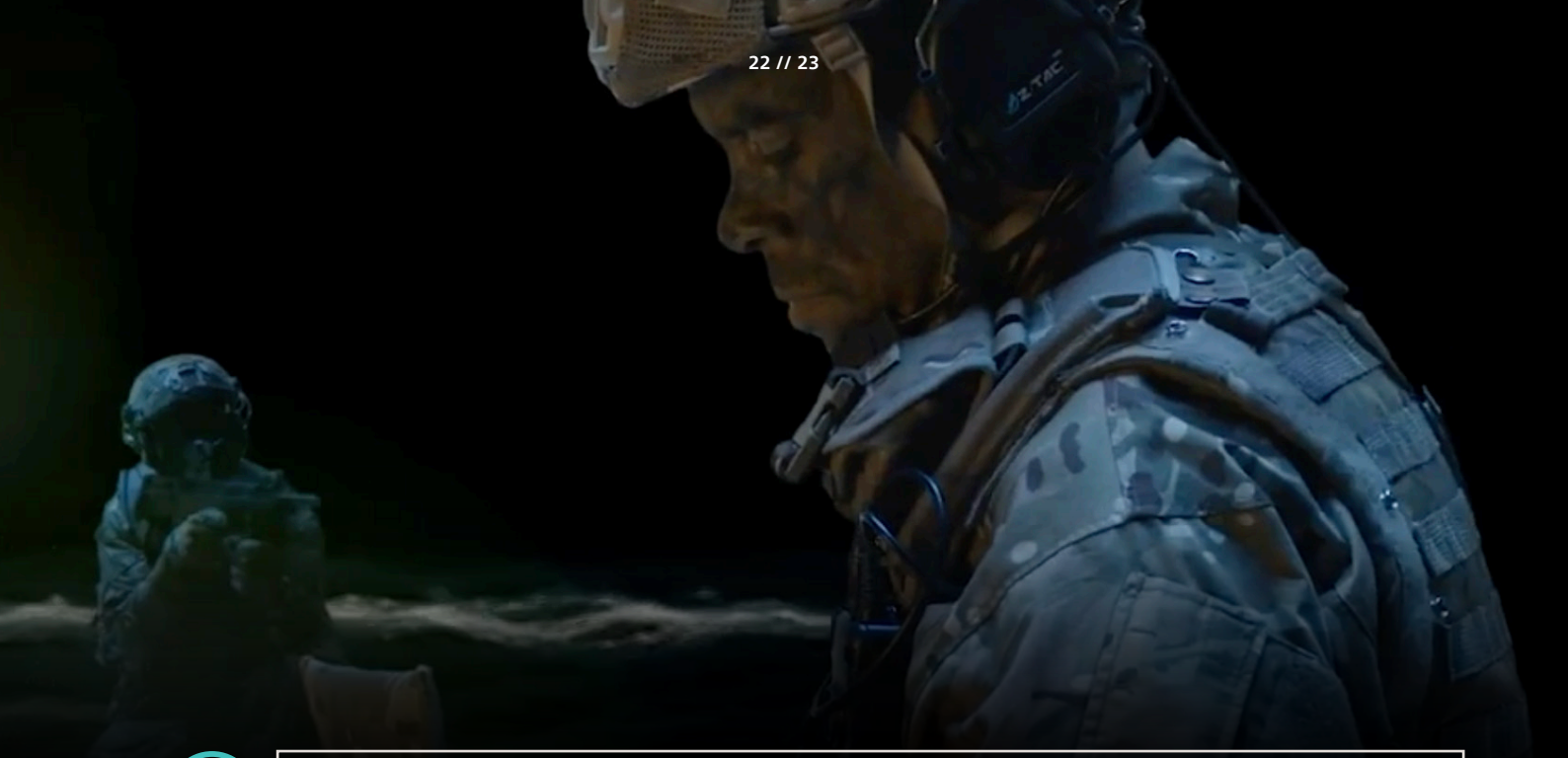
Multi-Domain Integration, which encourages data sharing and weaves digital threads between domains, gives nations a decision advantage against the adversary. Yet while its benefits are recognised by aerospace and defence respondents, even the most advanced nations are still at the beginning of their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



- Multi-Domain Integration enables a coordinated responses to emerging grey zone threats (98% agree)
- Multi-Domain Integration allows for a proactive response to cybersecurity attacks and AI developments (96% agree)
- Multi-Domain Integration programmes counter misinformation in the grey zone (94% agree)
- If Multi-Domain Integration is absent, increased complexity, uncertainty and volatility will be experienced by respondents' nations (90% agree)
- Multi-Domain Integration protects unmanned systems in the grey zone (84% agree)

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

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

BAE SYSTEMS