Defence technologies stuck in the pilot phase

Why MDI can propel nations towards full adoption

Digital Intelligence

BAE SYSTEMS

Introduction

According to our global 2023 study of more than 400 defence and aerospace decision makers around the world, as many as 95% of respondents agree that ongoing digitalisation has led to a more dynamic and complex battlespace. A battlespace based around not just information, but the accuracy, speed and seamless connectivity of that information.

At first glance, such a strong statistic would suggest focused investment into solutions that enable intuitive and proactive defence as part of a more collaborative ecosystem. However, when delving a little deeper, it would seem that this awareness of innovation's impact is yet to convert into a wholehearted effort to harness its full potential. Acknowledgement of various solutions' attributes hasn't yet blossomed into a connected network of vital, reliable data that would keep those on the frontline safe. In fact, when it comes to the evolution of defence technology adoption in the modern context, you could argue we're still stuck in the pilot phase.

Delving into those statistics a little further, defence leaders from the UK, Canada, Nordics, Australia and the Middle East largely came to the same conclusion; that the future battlespace will indeed be an information battlespace (86%). However, it is also interesting to note that the evolution of processes was seen as more essential for navigating the complexities of modern defence – with 98% globally coming to that conclusion.

This suggests a slight conflict or confusion around how to get the best stranglehold on the information battlespace in front of them. Technology is key, but is it those other strands of people and process that need to be optimised first? Amid this conversation, investments into new defence technologies are occurring, but once brought in, the enablers are not being developed to extract their full potential.

This brings to mind the need for a Multi-Domain intelligence model, which would encourage the construction of digital threads where these technologies can connect seamlessly and securely. This connectivity would enable a change of mindset that should bring people and processes along in tow, and ultimately force the technologies at our disposal out of the pilot phase.

95%

of more than 400 defence and aerospace decision makers around the world agree that ongoing digitalisation has led to a more dynamic and complex battlespace

The biggest pressure on defence

To take a step back, it's important to acknowledge that investments into new and advanced defence technologies really are ramping up.

Dissecting the adoption matrix further, 96% of defence decision makers around the world confirm that emerging technologies like AI and quantum computing will shape the future battlespace, a figure that rises closer to complete agreement in the UK (98%) and Canada (97%). As many as 89% agree that cyber and hybrid warfare will be major challenges in the future battlespace, while 89% also agree that space will become an essential component of national defence in the years to come.

Defence technologies that encourage greater collaboration and information sharing are also high on the agenda, in theory, with 94% agreeing this level of coordination will be critical to success moving forwards. Increased integration across all five domains – land, air, sea, space and cyber – is also seen as a leading requirement in the future.

Bringing these visions of the future together, it is clear that technological change is 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.

Digital innovation is increasing the information battlespace's size and with it the volume of grey zone attacks. On the one hand, the majority showing awareness and vigilance to these threat vectors is promising. And yet, there is another side to these statistics.

> The most prominent tech trends we're currently seeing in defence are related to **autonomy, artificial intelligence, machine learning, and hypersonics.**

Pavandeep Bhogal
Head of Product Engineering
BAE Systems
Digital Intelligence

89%

agree that space will become an essential component of national defence

The gap between partial and full adoption

When the question pivots from initial levels of adoption, to full adoption levels, percentages take quite a steep nosedive.

With AI and ML for example, 85% confirmed that their nation has already adopted it for defence operations. However, only 57% can say that they have reached full adoption where it is extensively implemented and integrated into all defence operations. Little more than a quarter (29%) conceded they are only at partial adoption levels, where AI/ML is not yet fully integrated or utilised.

It is a similar story for robotics and autonomous systems. Here, the 73% contingent who claim to have adopted such solutions are quite evenly split between 39% (full adoption), and 34% (partial adoption). Here, one-fifth still confirmed they are not even past the pilot/testing phase.

CEMA technology paints the same story, with 41% full adoption, 31% partial and 18% at the pilot stage. When it comes to battlespace technology the ratios read 41%, 33%, 20%; and for synthetic environments, 35%, 34%, 17%.

Even when it comes to data and intelligence analytics software, where 91% claim to have adopted critical solutions to help get a better grasp of critical information, only 58% can boast full implementation and integration. One-third are still only scaling up to that level.

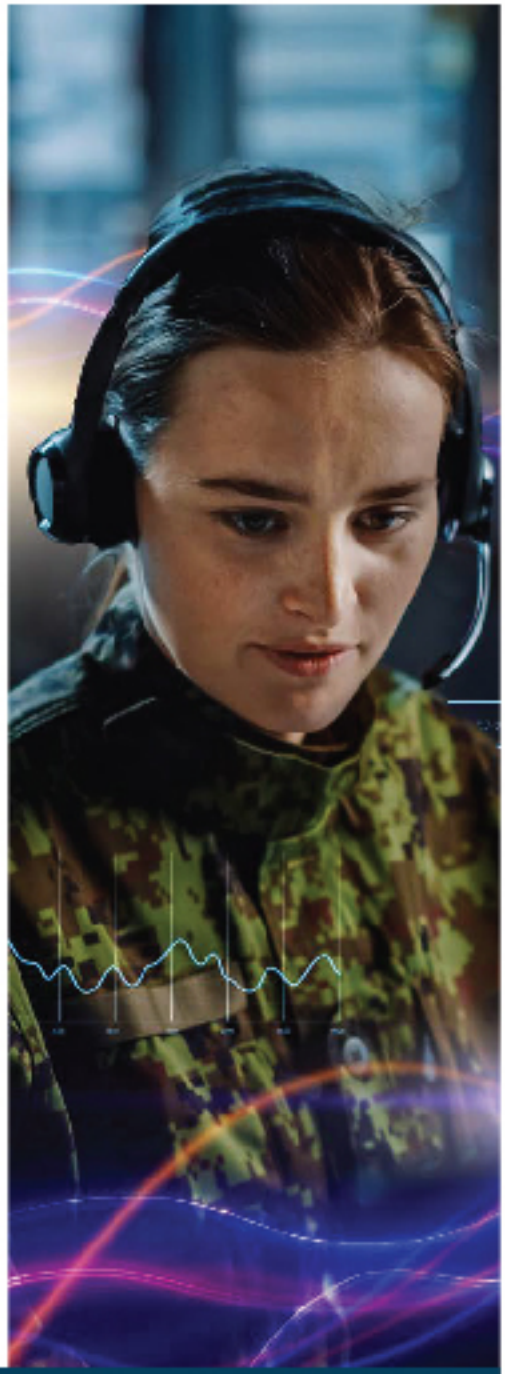
So, maybe most are technically out of the pilot phase, but it's clear that challenges remain. Challenges that would leave nations and militaries exposed to cyber-attacks. A sizeable 61% agreed that difficulties in attributing cyber activity is the most concerning factor about the grey zone, for example, which is concerning when only 58% have fully implemented intelligence analytics software that would help in the attribution effort.

This is compounded by 54% of respondents citing a data glut actually blocking intelligence. They're aware of the overload, and yet only partially equipped to filter more effectively. And, critically, 94% adhere to the notion of a 'digital Berlin Wall', pointing to difficulties in sharing and collaborating with allies and partners. The slow integration of automation and CEMA technologies will only compound this particular challenge.

61%

agreed that difficulties in attributing cyber activity is the most concerning factor about the grey zone

The right people, with the right information, at the right time



We're seemingly in a situation where modern solutions are on militaries' radars. More than that, investment and adoption of such solutions have also begun – another box ticked. The final hurdle that is proving difficult, is that phase of full integration and connection to the broader ecosystem.

What nations need in order to make this important leap, is an overarching model that naturally encourages and depends upon complete adoption. Multi-Domain Integration (MDI) is seen as mission critical by 98% of defence leaders, and would drive an ecosystem that relies on digital threads – where data is seamlessly and quickly analysed – and then shared to those who need to know (both domestically and across the broader ecosystem).

MDI as an enveloping model would promote quicker and more effective integration of new and developing technologies; assurance of those new solutions to ensure they are robust and fit for purpose; cyber security measures as a priority throughout all integrations; compatibility and interoperability between different systems and platforms; and ongoing R&D to ensure that militaries are constantly ahead of the digital curve.

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

"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. Without access to the full spectrum of desired information, it is difficult to make effective decisions and thus quantify the operational risk.

"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."

Making a real difference in the future battlespace

With an MDI model in place and a clear push towards the formulation of digital threads, it is more than just the technology box being ticked. Simultaneously, aspects of culture, people and processes are also addressed to establish more workable regulations, to break down siloes, to encourage ongoing training and development, and to spark improved collaboration.

Involvement of the private sector and of tech providers will be critical, not only to introduce platform mission planning solutions, but to also help manage the ever-growing suite of technologies being threaded together. To this end, digital asset management is an additional consideration that will determine the ultimate success of an MDI approach.

Nobody is denying the need for automation, for information sharing, for more seamless and intuitive data analysis. It is perhaps the speed at which enabling defence technologies are implemented that brings cause for concern – whether the slow transition from testing, to partial adoption, to full adoption is caused by a lack of prioritisation, or the lack of an enabling structure.

However, the time to ramp up defence technology progress really is now.

As Linton confirms:

> "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."

There is no lack of innovation within the defence community. Before it's too late, it's time to ensure that innovation is being harnessed to its full (not just a partial) extent, to make a real difference in the battlespace of today and the future.

Defence technologies stuck in the pilot phase

We are Digital Intelligence

Digital Intelligence is home to over 4,700 digital, cyber and intelligence experts across 16 countries. We operate at the cutting edge of digital innovation and at the heart of organisations that keep vital infrastructure running, national security protected and armed forces prepared.

Our teams provide advanced digital capability, products and solutions that weave together digital threads of data so that customers get the vital insight they need – from the fine detail to the bigger picture, providing the power of perspective to confidently make the critical decisions that keep our societies safe and able to thrive.

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. Whether on land, in the air, at sea, in space or cyberspace, we're your digital mission partner, with you every step of the journey.

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

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

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 28, Menara Binjai
2 Jalan Binjai
Kuala Lumpur
50450
Malaysia
T: +60 327 309 390

E: learn@baesystems.com
W: baesystems.com/digital

linkedin.com/company/baesystemsdigital
@BAESystemsDigi

Copyright © BAE Systems plc 2024. 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 Applied Intelligence.

Digital Intelligence

BAE SYSTEMS