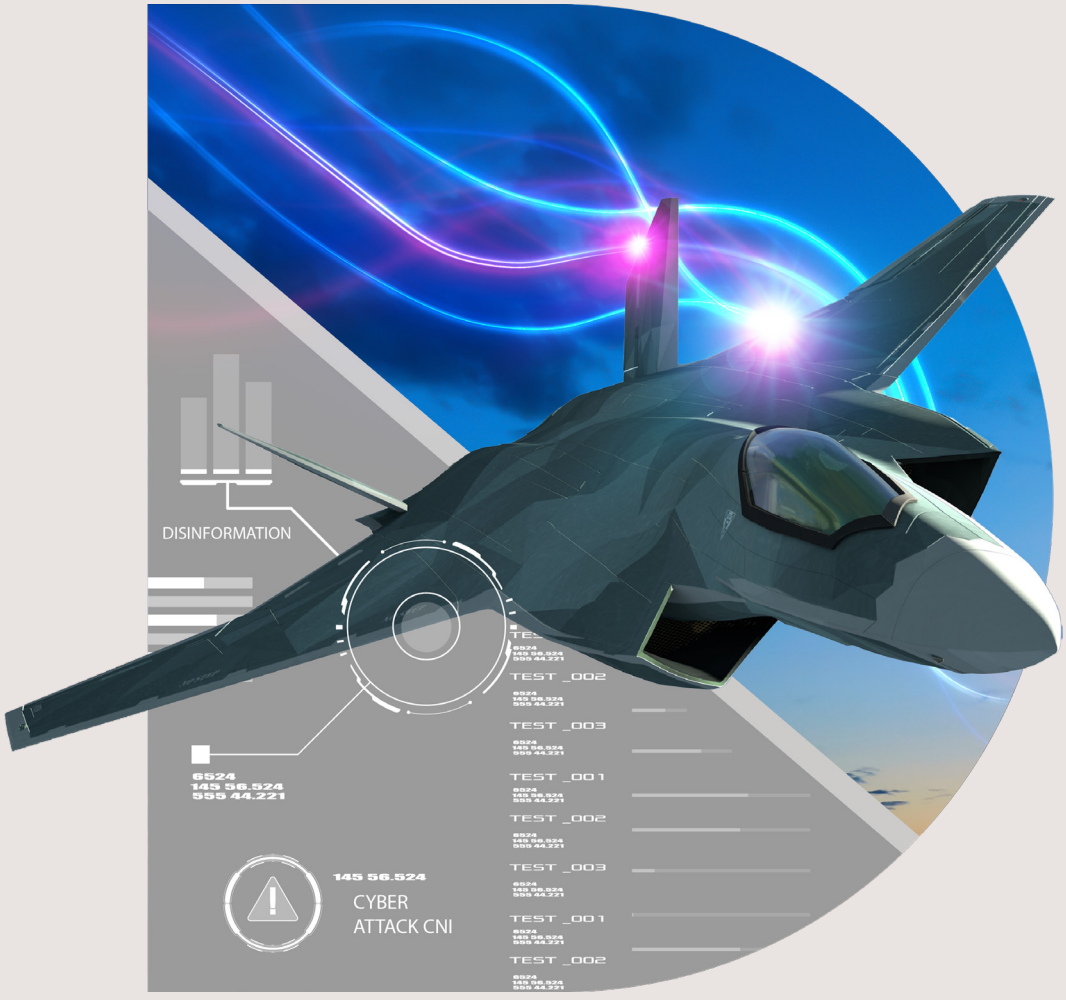
Cyber and CEMA

Threats from under the surface and within the grey zone



Digital
Intelligence

BAE SYSTEMS

Introduction

The security landscape over the past two years has understandably been dominated by kinetic warfare headlines. Across Europe, the Middle East and beyond, these very tangible situations are playing out in a way that aligns with many people's understanding of conflict. However, this doesn't necessarily paint the full reality of what military personnel deem as the biggest threat to global security moving forwards. Far from it, in fact. The future battlespace is one that will be dominated by a threat that – for the most part – remains unseen, under the surface, and lurking in the grey zone.

A global survey of senior defence leaders carried out by BAE Systems Digital Intelligence found that the weaponisation of cyber and the importance of cyber to defence (46%) is seen to be putting more pressure on the implementation of defence technology strategy than conventional wars such as the one being seen between Russia and Ukraine (44%). The former factor was only topped by a more general acknowledgement of cyber, where 52% pinpointed the speed of change in technological advancements as a critical factor adding pressure.

In military and defence contexts, cyber falls under the category of the grey zone – where damage can be done without physical interaction or traditional conflict methods.

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 MoD defines it** as "a murky area, consisting of everything which isn't full-on conflict, but isn't exactly an innocent act either".[1] Examples in the cyber realm span espionage and the spreading of misinformation, to ideological extremism and direct cyber-attacks designed to damage systems or disrupt operations.

Our research confirmed these concerns, with 61% citing the spread of misinformation as a concerning factor about the grey zone, joined by challenges in the attribution of cyber activity (61%) and the weaponisation of cyber itself (55%).

Knowing how to combat cyber threats from a military perspective begins and ends with technology… technology that is connected, delivers transparent and shared information, and that acknowledges cyber as one of the five key domains that make up our current and future battlespace.

[1] Contains public sector information licensed under the Open Government Licence v3.0

The grey zone

is where damage can be done without physical interaction or traditional conflict methods

61%

cite the spread of misinformation as a concerning factor about the grey zone

A Global Concern

Before exploring the potential of MDI as a model to address cyber concerns, it's important to understand just how complex the cyber domain is.

Cyber holds a dubious position in modern warfare because cyber-attacks are still not considered official acts of war. Attacks are often unseen and hard to attribute to particular threat actors or nation states. Yet, they can cause severe harm – either to society by attacking critical national infrastructure assets or utilities, or in physical battlespaces where electromagnetic signals can disrupt or corrupt communications. It's due to this range of threats that the concept of 'CEMA' (cyber and electromagnetic activities) has become so prominent in today's battlespace.

Unsurprisingly, given the rate of digital development more broadly, these attacks will only rise in the coming years. Globally, this leads to 68% of senior defence leaders believing that cyber-attacks pose the biggest vulnerability to national defence.

In some countries, like the UK (75%) and Canada (73%) this figure rises even higher. And even in regions such as the Middle East where only 52% of respondents listed cyber-attacks as their biggest threat, the awareness of cyber's influence in general is still clear. More than any other region, the UAE and Saudi Arabia highlighted the weaponisation of cyber and cyber's importance in defence, as a factor that is adding pressure to the implementation of defence technology strategy across their nations (58%). Only the Nordics (54%) came close to this level of response, confirming that cyber is very much a global concern, no matter how that concern manifests.

Ultimately, with 89% globally agreeing that cyber and hybrid warfare will be major challenges in the future battlespace, this grey zone threat poses a very real problem. However, it's not without a known solution.

68% of senior defence leaders believe that cyber-attacks pose the biggest vulnerability to national defence

Tackling Cyber with MDI

Multi-Domain Integration (MDI) is that solution, in that it fights technology with technology.

It serves as a proposed model where digital threads are created across domains, connected through state-of-the-art solutions that promote real-time information generation and the seamless connectivity and sharing of that data. This ensures that the right information is reaching the right people at the right time.

There is also a cultural element to this model, with a need to break down siloes across the ally ecosystem and encourage a level of sharing that has perhaps not been entertained before. In a cyber context where attacks have very little boundaries or borders, this need to connect domains, departments, sectors and even nations, is critical.

It seems the senior defence leader community agrees, unanimously. As many as 98% concur that MDI is important to shaping military operations today and in the future. Respondents note that MDI is key to navigating increased cyber warfare attacks and challenges in the grey zone, along with more general breaches in national security, threats to national economies, and to simply keep up with modern warfare.

Breaking down the benefits further into more operational military considerations, MDI can improve situational awareness (54%), quality of decision making (51%), preparation for potential warfare (49%), decision making speeds (48%), and levels of collaboration (45%).

Interestingly, when asked what risks they would be facing if an MDI model wasn't adopted in the next five years, increased cyber warfare attacks on nations (55%) was the most frequent response.

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

Andrea Thompson
Managing Director
BAE Systems Digital Intelligence

> 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

Martyn Orme
Head of Business Development
Techmodal

CEMA: MDI's Chief Enabler

Tellingly, 93% of senior defence leaders agree that MDI strategies allow for a proactive response to cybersecurity attacks and AI developments. A resounding 89% also agree that MDI programmes can either mitigate against, or build an understanding of, misinformation in the grey zone.

MDI in essence is defined by the UK government as an "effective integration of space, cyber and electromagnetic, maritime, air, and land" to achieve "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".[2]

CEMA integration is a vital strand of this summary, in that it exploits electronic warfare, cyber and security capabilities in order to deliver that much needed information and decision advantage within an MDI framework.

The integration and orchestration of CEMA enables full exploitation of the wireless spectrum to provide the operational flexibility that senior defence leaders are craving. At present, almost three-quarters (72%) of those surveyed have adopted CEMA systems as part of their MDI development, but its full potential when it comes to achieving decision advantage and operational flexibility in the cyber domain is yet to be realised.

CEMA solutions can help understand the electromagnetic environment defence leaders are operating in. This enables an 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 both the digital and physical battlefield.

As such, when trying to gain visibility of the grey zone and of threats lurking under the surface, by championing an MDI model, CEMA solution integration will be among the most pivotal steps taken by defence decision makers in the coming years.

[2] Contains public sector information licensed under the Open Government Licence v3.0

A clearer understanding of the electromagnetic spectrum

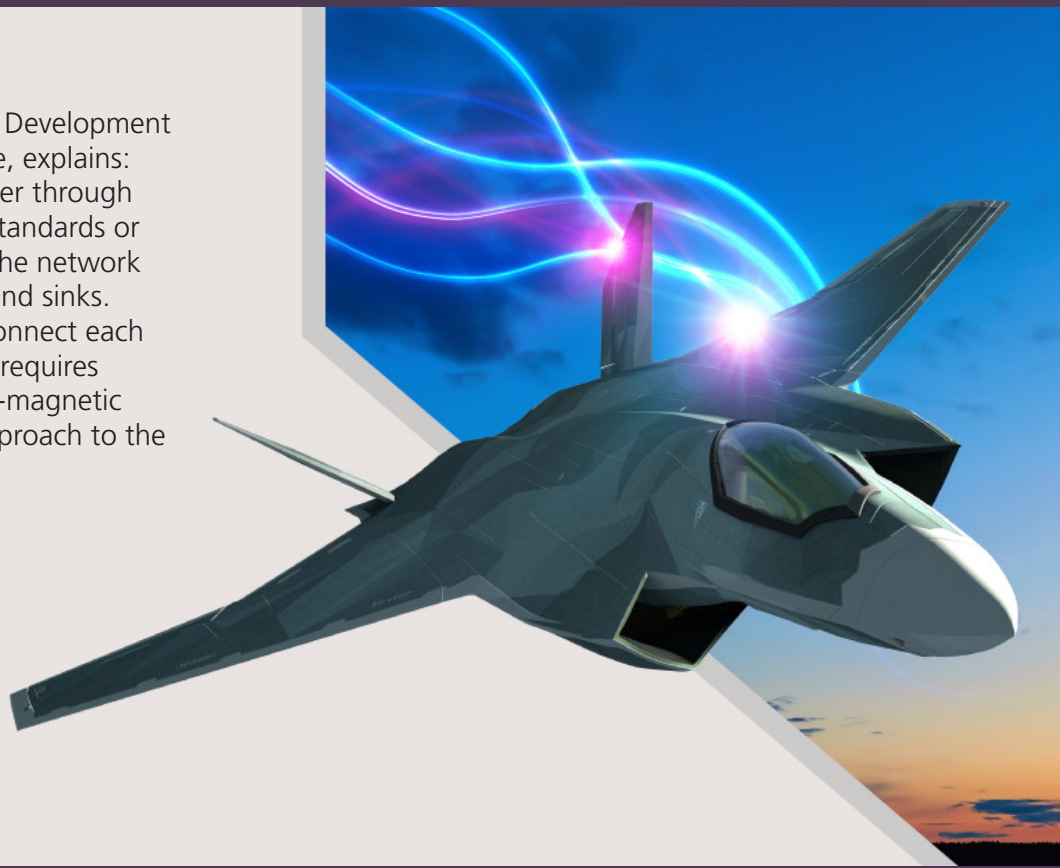
At present, only 41% around the world have fully adopted CEMA systems, despite the 72% who have adopted at least partially. A further 18% say they are in the pilot and testing phase with a view to future implementation.

However, only a third (34%) list gaining electromagnetic spectrum dominance as the most important area of focus for defence technology exploitation. Admittedly, this factor was being weighed up against both physical and digital threat landscapes and more general issues such as data to improve operational readiness (54%). Yet, it still suggests a need to embed CEMA into overall defence strategy more concertedly – a strategy built around MDI, and that reflects cyber's growing, unique threat.

When doing so, the result is a successful, MDI-centric fightback against that cyber vector, championing three critical elements: data, network layer and communication.

Mark Todd MBE, Head of Product Development at BAE Systems Digital Intelligence, explains: "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. Lastly, communications need to connect each of those network nodes, and this requires the ability to use all of the electro-magnetic spectrum and have a common approach to the use of waveforms."

Mark concludes that the success of this integration relies on the characteristics of the data and the resilience of the systems, but also on a clearer understanding of the electromagnetic spectrum.



When tackling such a unique attack domain lurking under the surface and within the grey zone, improving this understanding as part of a broader MDI journey might not be a bad place to start

We are Digital Intelligence

BAE Systems Digital Intelligence is home to 4,800 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) 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

Digital Intelligence

BAE SYSTEMS