Digital defence innovation is a **team sport**:

Here's how to play

Digital Intelligence

BAE SYSTEMS

Our customers need to see faster, decide faster, act faster and adapt faster. They need to do all of this in environments where networks are degraded, the electromagnetic spectrum is contested, and adversaries are actively trying to disrupt every stage of an operation.

In this environment of digital warfare, digital defence is essential.

Mark Todd
Innovation and Technology Director,
BAE Systems Digital Intelligence

Digital defence is a must-have… but it's not just about the technology

Advantage is no longer created by any single platform, sensor, weapon or data feed. It comes from the ability to connect them into a coherent mission system. The side that can integrate, understand and act at tempo gains the edge. For this reason, digital defence is no longer simply about technology. It's about bringing together people, platforms, data and decisions in ways that create operational advantage.

And increasingly, that's exactly what our customers are telling us.

Defence is converging on a common goal

The UK's Defence Investment Plan states we must "invest in capabilities fit for the next war, not the last one." It's a theme that I have seen discussed and explored at multiple recent industry and Defence events. The discussions I have witnessed, have been remarkably consistent: future advantage will come from integrating capabilities, people and information more effectively across domains.

> The UK's Defence Investment Plan states we must "invest in capabilities fit for the next war, not the last one."

For example, at the recent RUSI Land Warfare Conference, discussions centred on modernisation, combat power regeneration, operating in the electromagnetic spectrum and adapting to rapidly evolving threats. The theme, Land Power: The Foundations of Deterrence, highlighted the enduring importance of land forces while recognising that tactics, structures and capabilities must continue to evolve.

That thinking extends far beyond the land domain. At the Battlespace Advantage Symposium, the focus was on achieving advantage across land, maritime, air, space, cyber and the electromagnetic spectrum. The emphasis was clear: success depends on integration across domains, enabling forces to operate effectively in congested, contested, degraded and denied environments.

The same theme is visible at sea through the Royal Navy's Hybrid Navy concept, which combines crewed, uncrewed and autonomous systems into a single interconnected force. Rather than concentrating capability within individual platforms, functions such as sensing, decision-making and effect can be distributed across a digitally connected fleet.

Viewed together, these initiatives point towards the same future. Defence is moving away from platform-centric thinking and towards integrated force advantage.

The challenge, as the Defence Investment Plan shows us, is no longer simply building great technology. It is connecting technology into mission-ready capability.

Across Defence, initiatives such as the Digital Targeting Web, are taking this thinking even further. By connecting sensors, deciders and effectors through shared data, AI-enabled capabilities and common architectures, Defence is creating new ways to generate speed, resilience and choice.

What does it take to deliver integrated force advantage?

If Defence is converging on a common goal, what are the foundations required to achieve it? For me, three ingredients stand out.

1. **First, a resilient digital backbone.** Without resilient connectivity, there is no integrated force. Data, decisions and effects can only move at speed if the underlying network can survive disruption and continue operating in contested environments. Capabilities such as NetVIPR™ are designed to provide secure, deployable military communications networks using multiple communications infrastructures rather than relying solely on satellites or fixed infrastructure. Its node-based design helps maintain the flow of information even if parts of the network are degraded or damaged.

NetVIPR™ is a deployable networking product which provides intelligent and secure military communication networks linking everything from small reconnaissance drones to combat vehicles, fighter jets, aircraft carriers or military commands.

Find out more ↘

2. **Second, command and control that reduces friction**. Effective C2 turns data into understanding, supports human judgement and helps commanders operate inside an adversary's decision cycle. Building on open platforms such as the TAK ecosystem to unify operational awareness, and extending it with AI-enabled plugins, offers a cost-effective and operationally relevant approach. Our work in this space is also reflected in our investment in Oxford Dynamics, an innovative organisation developing AI-enabled systems for defence decision-making.

"The landscape of warfare is rapidly evolving and embracing emerging technology is vital to keeping the UK safe."

"By working with companies such as Oxford Dynamics, we can help ensure that the nation is ready to unlock the advantages that innovation brings and help strengthen the UK's sovereign defence and security landscape."

Andrea Thompson, Group Managing Director of BAE Systems' Digital Intelligence business

3. **Third, cyber and electromagnetic integration**. Cyber and electromagnetic activities can no longer sit in specialist stovepipes. They need to be embedded within the wider mission system, with every platform contributing to a richer operational picture. BAE Systems' acquisition of Kirintec strengthened our CyberEM capabilities, bringing expertise in counter-IED, counter-UAS and electronic warfare solutions, alongside open-architecture technologies designed to operate across domains and platforms.

Kirintec's battle-proven technology protects military platforms and personnel from cyber and electromagnetic attacks. The open architecture of the products enables them to work together across all domains and a range of military platforms. The acquisition brings together complementary capabilities in CEMA and multi-domain integration and will enable BAE Systems to support growing customer requirements and address increasing demand for these capabilities.

Find out more ↘

What is particularly striking is how these capabilities are converging. We see it in land modernisation programmes. We see it in the Digital Targeting Web. We see it in the Royal Navy's Hybrid Navy concept. And we see it in future combat air thinking.

The future force is neither platform-led nor software-led.

It is mission-led.

Innovation is not the problem. Transition is.

Defence doesn't lack innovation. Across the sector, SMEs, technology specialists, academia, government organisations and primes are developing outstanding ideas and capabilities. The challenge is that too many innovations struggle to make the journey into operational use.

Too often, solutions are developed without sufficient consideration of how they will integrate into existing architectures, align with standards, satisfy assurance requirements or scale into operational environments.

As a result, promising technologies can become trapped in the space between demonstration and deployment.

Closing that gap requires a different mindset. Whether innovation begins with industry or with the customer, the model should be the same:

Innovation only becomes valuable when customers can adopt it with confidence.

Open architectures make teamwork possible

If innovation is a team sport, open architectures are the rules that allow everyone to play together.

Our customers increasingly want freedom of action. They want the ability to evolve capability as threats change, avoid vendor lock-in and draw upon innovation from across the defence ecosystem.

Open architectures enable exactly that. They make it easier to integrate new capabilities, support upgrades over time and create opportunities for multiple suppliers to contribute to a common mission system. They also help deliver better long-term value by reducing dependency on any single technology provider.

This philosophy is reflected across frameworks such as NATO Federated Mission Networking (FMN), STICS and SAPIENT. While each serves a different purpose, they share common principles: interoperability, modularity and the ability to connect capabilities from multiple suppliers into a coherent operational system.

Ultimately, open architectures are not just a technical preference. They are an operational advantage.

Why SMEs are central to the team

SMEs bring specialist expertise, agility and fresh thinking. They are often closest to emerging technologies and can move quickly to solve highly specific operational challenges.

But speed alone is not enough. To succeed in Defence, innovative technologies also need access to customers, integration environments, operational context, security expertise and pathways into programmes that can scale. This is where collaboration becomes critical.

As a prime contractor, we are passionate about helping innovative ideas make the journey into operational capability. That means providing integration expertise, helping align solutions with standards and architectures, supporting assurance activities and creating routes into programmes customers already trust.

Most importantly, it means treating SMEs as partners rather than simply suppliers. Because a great idea only creates operational value when it can be deployed, trusted and sustained in service.

The prime's role is changing

The modern prime is not expected to own every answer. Instead, the role is increasingly about bringing the right team together.

That means combining the strengths of customers, SMEs, government organisations, academia and industry partners. It means creating architectures that allow innovation to plug in. And it means helping customers benefit from new technology without compromising assurance, resilience, security or long-term support.

Across our own ecosystem, we see this every day. Whether through cyber and electromagnetic capabilities, secure networks, AI-enabled decision support, battlespace integration, data services or mission software, the real value comes from bringing capabilities together in ways that solve customer problems.

Because customers don't need disconnected innovation, they need mission-ready capability.

> Through our flagship incubator, Launchpad, we help to turn promising technology into scalable businesses, enabling agile businesses to commercialise advanced technology more quickly, while strengthening innovation across sectors such as energy, advanced manufacturing and defence.

How to play

If digital defence innovation is a team sport, how do we play?

- Start with the customer's mission
- Design for integration from day one
- Use open architectures wherever possible
- Bring SMEs into the conversation early
- Create practical routes to adoption
- Test in realistic environments
- Generate evidence customers can trust
- And focus relentlessly on transitioning innovation into operational capability

The direction of travel is clear. The conversations happening across Defence – from the RUSI Land Warfare Conference to the Battlespace Advantage Symposium, from Hybrid Navy to the Digital Targeting Web – all point towards the same future: an integrated, digitally enabled force operating across domains at speed.

That future won't be delivered by a single platform, a single supplier or a single breakthrough technology; it will be delivered by teams.

Primes, SMEs, academia, government and end users all have a role to play. Our job is to help bring that team together and turn innovation into capability the customer can trust.

Because in modern defence, the side that integrates, decides and acts fastest creates the advantage that matters most.

Digital Intelligence is home to over 4,500 digital, cyber and intelligence experts across 13 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. Digital Intelligence is part of BAE Systems, which has a rich heritage in delivering technology today to protect our tomorrow. BAE Systems partners with governments, communities and companies large and small to design, build and maintain advanced defence and security solutions.

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
@BAESystemsDigi

Digital Intelligence

BAE SYSTEMS