Cyber Capacity Building

BAE Systems Digital Intelligence Catalogue

Digital
Intelligence

BAE SYSTEMS

Introduction

Capacity building is a well-established concept, with an endorsed set of principles owned by the United Nations. The application of these principles to the cyber domain has increasingly come to the fore over the last decade. This trend has been driven by the changing nature and distribution of power across the globe which in turn has come with a recognition that security at home is not possible without security abroad. Cyber threats increasingly pose one of the greatest challenges to national security and this has forced nations to recognise the need to engage in an increasingly collaborative manner with allies and partners to address this challenge. Cyber capacity building has emerged as one of the practical outcomes to address these challenges.

So what does the term Cyber Capacity Building mean and how does this translate into practical activity and capability delivered to the recipient?. At its essence is the ability for nations to protect and promote their interests in and through cyberspace. With cyber space being inherently international this has to mean not just being able to secure interests within your own borders but also internationally. From this understanding has come an increasing interest and conversion of this interest into strategy and practical activity to support partners and allies in developing their cyber capacity to raise a collective baseline required to effectively address the cyber threats.

BAE Systems has had significant engagement in all aspects of this process; from the initial assessment of determining what is the cyber threat, though creating the strategy to how to address is to delivering programmes of work against the defined policies and capabilities that span a nation's response. This catalogue is the reflection of the full breadth of cyber capacity building propositions that we are able to offer in their pursuit of raising cyber security.

There is huge opportunity in governments and citizens adopting Information and Communication technologies for the delivery and access of services. The challenge lies in realising this opportunity without an equivalent rise in the cyber threat.

Our cyber capacity building services are designed to support nations realise their strategy in the most efficient and safest way possible.

Why BAE Systems Digital Intelligence?

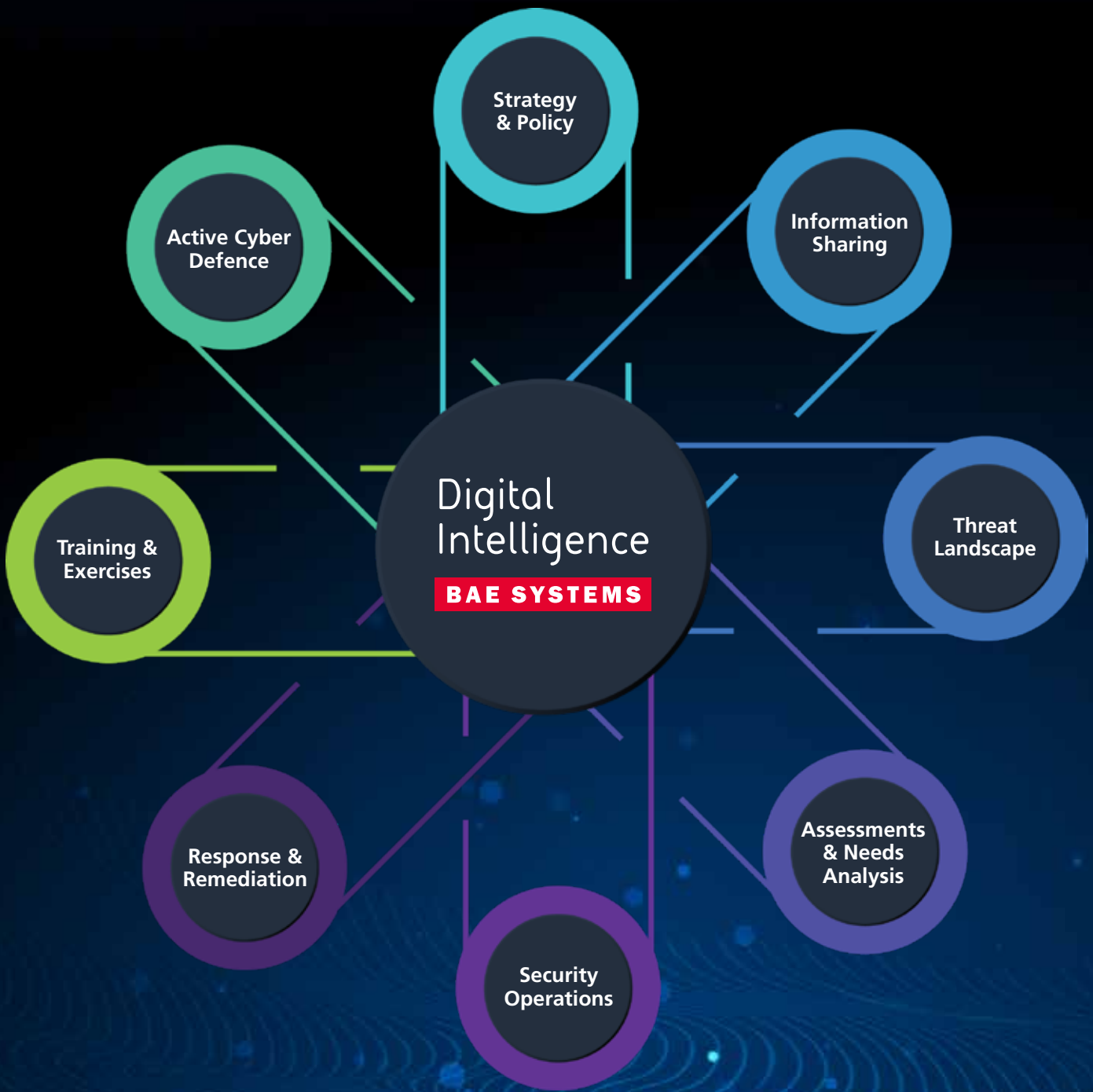
At BAE Systems Digital Intelligence, we are specialists at operating across national security, government, and commercial sectors. Unlike other businesses where these would be strictly separate divisions, we embrace the benefits in bringing the best practices from one to the other, and our customers recognise and value this unique position.

At the core of our cyber capacity building business is a deep understanding of the threat landscape, derived from over a decade of research and providing incident response services following complex attacks. Many of these involve state actors or organised criminal groups – both adept at evading traditional security controls in enterprise networks.

Through this understanding we are able to deliver capacity and capability that will drive real change and help ensure a demonstrable uplift in understanding and addressing the cyber threat posed to a nation. This covers the full spectrum of operational capability; from a tactical solution to address specific concerns though to national scale strategy creation and delivery.

More broadly, we have extensive experience delivering cybersecurity services for customers in government, financial services, and other critical national infrastructure (CNI) organisations. Relevant services include security advisory and consultancy, definition and delivery of national cyber programmes (such as the establishment or transformation of National Cyber Security Strategies and Agencies) and systems integration (such as for Security Operations Centres). In addition, we can provide specific technical services (such as Incident Response, Threat Intelligence and Penetration Testing) and offer our own suite of cyber security products (such as secure gateways enabling the integration of Operational Technology and Information Technology for CNI organisations).

Our Cyber Capacity Building Portfolio



Strategy & Policy
Delivering cyber security at a national scale is a hugely broad remit. It is essential that at the heart of this sits a national strategy and underlying policies that set the foundation for developing and growing capability and capacity. Our services extend from creating strategy, through design and building of national capability to all the associated frameworks, standards and legislation. Our approach encompasses broader aspects of capacity building such as gender mainstreaming

Information Sharing (Public-Private Partnership)
The one advantage cyber defenders hold over attackers is the sharing of information; an attack on one can be converted into the defence of all. However, realising this advantage needs government and commercial companies to work together (public-private partnership). Our services support the creation of an end-to-end capability to enable this working and sharing of information

Threat Landscape
Understanding the adversary, and the latest tools, techniques and procedures they use is critical to ensuring the capacity building activity actively reduces the risk to the nation. We provide a range of services to help our customer understand the nature and scale of the threat landscape they operate in that can then be used to inform tactical, operational and strategic activity

Assessments & Needs Analysis
Capacity building programmes of work are significant investments. Our assessments and needs analysis services ensure that the capacity being delivered is appropriate to the maturity, risk and associated levels of tolerance as well as builds on any investments already made. The findings of our assessments flow through into any programme delivery and drive the benefits realisation approach we follow

Security Operations
Protective monitoring gives a critical capability of threat detection, utilising threat intelligence as well as creating it. Our services are underpinned by a proven blueprint and aligned to a flexible framework that means we can support the end-to-end programme of designing, implementing and efficiently and effectively operating a security operations centre

Response & Remediation
Being able to respond in an appropriate manner to incidents and use the lessons learned to help ensure it will not happen again is essential to minimising the impact of a cyber attack. We are an assured provider under the UK NCSC Cyber Incident Response (CIR) scheme which means the response and remediation services we provide are proven to the highest standards

Training & Exercises
Informed by our threat intelligence, we provide a range of specialist training and tailored exercises. In addition, we can provide services to ensure training is appropriate to the intended audience and delivers benefit rather than just another attendance certificate. All of our training and exercise propositions are proven from an individual team up to multi-national regional scale

Active Cyber Defence
Active Cyber Defence (ACD), is intended to tackle the high-volume commodity attacks that affect people's everyday lives by providing a range of tools and services, free at the point of use, to protect from a range of attacks. Specifically designed to operate at scale, our offerings fall into four categories: self-service checks; protection and detection capabilities; disrupters; and enablers

Strategy Development, Policy Creation & Enforcement

National Cyber Security Strategy

BAE Systems will assist with identifying cybersecurity capability needs for the nation, in line with the national and domestic cyber threat, regional relationships, economic trajectory and digital footprint, and drafting a national cybersecurity strategy that identifies targets.

National Cyber Security Programme

A programme of work to identify responsibilities and ownership, and a series of action plans for achieving the national cyber security strategy. This will include setting priorities and targets, based on risk, maturity and threat assessments.

NCSA Operational Framework

We will define and write the operational framework for effectively and efficiently delivering national cyber security. This includes but is not limited to the target operating model (TOM), associated concept of operations (CONOPS) and all associated policies and procedures for the how national cyber security strategy will be realised through operational capability.

National Cyber Security Agency Design

BAE Systems will design and build a national cybersecurity centre, with a remit to deliver the national cybersecurity capability; tools for monitoring, threat intelligence and intelligence sharing, and training/upskilling/mentoring local staff to run the operation over a period of time.

National Standards

We will review existing, or draft new national cybersecurity standards to ensure a complete policy suite exists laying out best practice and targets for organisations to follow, based on policy frameworks used in other countries (e.g. UK SPF) and international benchmarks.

National Legislation & Regulation

BAE Systems will review existing or draft new legislation and regulations for debate and publication. These typically cover areas that cyber capacity building will highlight as lacking or being deficient in, such as privacy legislation or the use of offensive cyber.

Information Sharing (Public-Private Partnership)

Information Sharing Framework

BAE Systems will define and establish the framework, and where necessary relevant legislation or regulation, to enable information sharing from and between the government and private companies, or the general public at large.

International Collaboration

We will identify and support access to, or the creation of collaboration opportunities with relevant international organisations, partner nations and industry to enable grow capability or raise maturity.

Information Sharing Ecosystem

A turnkey technical solution that BAE Systems have designed. As well as the technical solution we will provide all accompanying policies, procedures and operating models to optimise the practical application of the information sharing framework.

SCIF Review

BAE Systems will review and advise on the physical, socio-technical and logical controls to ensure a secure, compartmentalised information facility (SCIF) is appropriately controlled to enable the receipt and holding of (typically classified) material from partners, allies and stakeholders.

Civil Society Awareness

We will conduct assessments of the level of awareness and understanding of the nature and scale of the cyber threat by the civil society and what can be done to identify and prevent these. Our assessments can be conducted at any scale between individual organisations and the entire general population.

At BAE Systems Digital Intelligence, we are specialists at operating across national security, government, and commercial sectors.

Threat Landscape

Threat Intelligence

BAE Systems are a world leading provider of unique research and investigatory cyber threat intelligence reports, signatures and rules. These cover expert analysis and research into cyber threats, the actors behind these and vulnerabilities to technologies used in critical systems. Our product enables a broad spectrum of users to improve decision making on technology security.

Threat Assessment

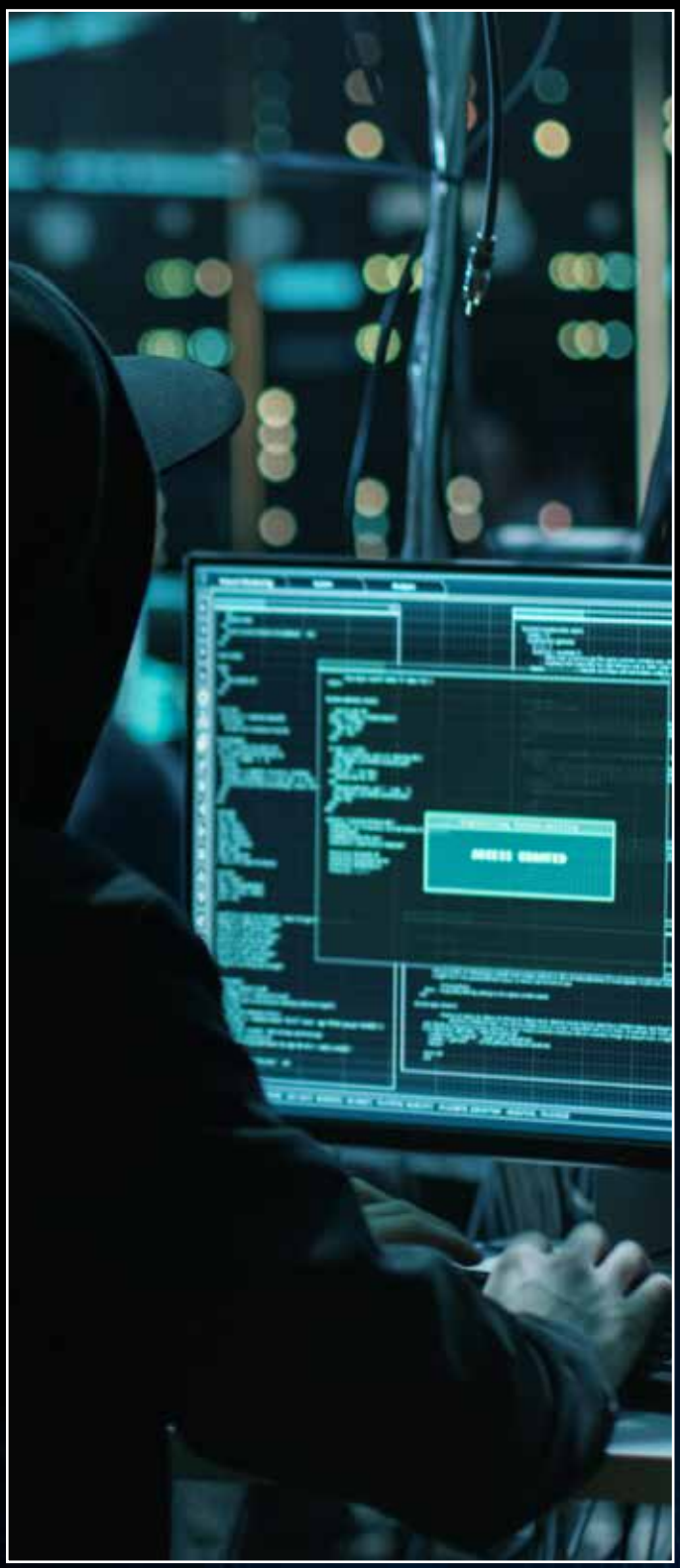
We conduct assessments into the nature and scale of the cyber threat to specific organisations, sectors, countries or regions to inform strategy, prioritisation of capacity building and tactical operations. Our threat assessments typically form the starting point for any subsequent activity as they establish prioritised action that will addresss the greatest threat first.

Threat Hunting

Covering the full spectrum of hunting activity, from researching legacy data sets for evidence of compromises, through supporting security operations to intelligence led hypotheses we support organisations create and mature these functions. Our service has knowledge transfer at the heart to enable sovereign capability to be established and own the capability going forward.

National Networks Cyber Centre

For organisations who are charged with monitoring for cyber attacks taking place within their country, BAE Systems NNCC solution provides nation-wide coverage of threats from a single data source, using technology designed specifically to meet the demands of running at this scale.



Awareness & Needs Analysis

Cyber Maturity Assessment

BAE Systems have a flexible framework that can be used to deliver assessments against the maturity model of choice (e.g., CMM), to determine the current level of cyber security of an organization or industry and benchmark this against the desired state to give an indication of any gap and improvement opportunities to be identified.

Capacity & Capability Assessment

Achieving the cyber security strategy of a nation is only possible with the appropriate combination of people, process and technology. Our assessment reviews the capacity and capability of the resources assigned to realising the strategy and making a judgement on what is possible and highlighting any gaps that may exist.

Threat and Risk Assessment

BAE Systems have a comprehensive approach and methodology to enable an holistic approach to threat and risk assessment. Under our STARA® framework we consider all domains, including physical security, human behaviour and security culture, technical and cyber security, and different types of organisational exposure, to provide a comprehensive view of the threat and risk landscape, including vulnerabilities for an organisation.

Technology Strategy

We help organisations determine what the most appropriate technology strategy should be in the context of their current as well as desired future state of maturity, resourcing and remit.

Security Operations

SOC Needs Analysis

Organisations are continually evolving, as is the cyber threat landscape they operate in. We analyse the current and future security operation needs of the organization and highlight any differences between existing investment and the optimal state of the SOC.

SOC Maturity Assessment

The primary aim of a security operations centre is to be able to detect the cyber threats that are of greatest concern to the organization. Our diagnostic assessment determines the ability of the SOC to achieve this and will make recommendations for addressing any areas of limitation.

SOC Technology Strategy

Cyber security technology is continually evolving. Based on a combination of need, desired maturity and operational requirement BAE Systems will deliver a security operations technology strategy that will best support these three factors.

SOC Design & Build

Based on a flexible framework and underlying open, modular design blueprint our approach can deliver from a greenfield site or develop existing investment. Our approach enables increasing maturity, expanding capability or evolving tools without disrupting the core operations of the facility.

SOC Operational Framework

Staff with the right skills and following the most appropriate policies and operating process will ensure the operational success of a SOC, not the technology. Our operational framework is based on having successfully operated and trained staff across multiple SOCs.

Response & Remediation

Incident Response

For organisations that have either suffered a security breach or incident, or want to have expert support available in the event of an incident in the future BAE Systems are one of 13 UK NCSC assured and certified companies with the skills and experience to deliver a range of incident response services to government and critical national infrastructure.

Reporting & Sharing

The silver lining of security breaches and incidents is the ability to learn from the failings to ensure they do not happen again, both within the affected organisation and more widely. We will establish a framework whereby these learnings can be captured and shared to realizing these learnings.

Incident Remediation & Hardening

BAE Systems will either lead or support the work required to revert the estate back to a position of known good. We will also identify and address any vulnerabilities or control gaps that enabled the breach or incident to occur in the first place to ensure the same vector cannot be used again.

CSIRT Operational Framework

Staff with the right skills and following the most appropriate policies and operating process will ensure the operational success of a CSIRT, not the technology. Our operational framework is based on our own certified service and having successfully operated and trained staff across multiple CSIRTs.

Response Playbooks

BAE Systems will either build a library of playbooks or expand the breadth of scenarios covered to ensure an appropriate and consistent response to incidents and events. These playbooks are dynamic in their nature as the threat and organization evolves and we will transfer the knowledg for how to ensure the library remains up to date to allow an efficient and effective response.

CSIRT Design & Build

Building a CSIRT is more than just having the latest suite of incident response tools. It is about aligning policies and procedures to ensure that these tools can be deployed most effectively. We will deliver the full suite of standard operating proceedures and all other relevant documentation and personal development to the ensure the service can not only operate the relevant technology but do so in a coherent workflow.

Training & Exercises

Training Needs Analysis

BAE Systems will identify the training needs for the roles and their associated remits within specific organisations. The outcome of this assessment enables subsequent personal development plans to be generated. These plans are recognised as a critical factor in both recruitment and retention of staff.

Workforce Development

Providing training at a national or sectoral scale requires a different approach to needs anlaysis in a specific organisation. We work with national bodies to determine the most appropriate level and delivery mechanism for workforce development.

National Skills Development Framework

Building skills at a national scale, not only in the existing workforce but for future generations, requires a flexible framework to guide this multi-year activity. BAE Systems will develop an appropriate national skills development framework taking into account strategy, existing skills levels and educational facilities.

Digital Skills Hub

Where educational facilities do not exist in country, BAE Systems can design and build a training campus for the deliver of cyber security training at a national scale.

Incident Response Training

Generic training can be acquired from any number of providers. We deliver specialist training aimed at organisations dealing with the most advanced and sophisticated threats.

Table Top Exercises

Practicing scenarios as part of incident preparedness helps ensure reacting to actual security breaches and incidents is second nature. BAE Systems have developed and successfully delivered table top exercises for all parties from C-suite to regional collaboration events.

Capture the Flag

BAE Systems have considerable experience in participating, designing and operating CTF exercises at a broad range of scales. These permit the honing the specialist skills of white-hat testers against each other in a gamified environment.

Threat Intelligence Training

As with incident response training we provide specialist threat intelligence training that is aligned to the specific requirements of your threat intelligence cell to enhance skills beyond what is available from commercial training providers.

Active Cyber Defence

My NCSA

BAE Systems will stand up a platform to act as a single point of entry to a number of ACD services. While each service is standalone, the platform enables tailoring of individual users experience with a focus on the service(s) most of interest to them.

Mail Checks

We will deliver a mail check service that helps organisations adopt secure email standards to prevent spoofing of their email domains or the reading of their email traffic by helping to implement the latest standards.

Web Check

BAE Systems will enable an automated web configuration and vulnerability scanning service to help find and fix common security vulnerabilities in websites for organisations signed up to the scheme.

Protective DNS

Protective domain name service (PDNS), prevents users from accessing domains or IPs that are known to contain malicious content and stops malware successfully installed on a network from calling home. We will work with relevant internet service providers (ISPs) to enable this service.

Host-based Capability

BAE Systems will deploy a software agent to agreed (typically government owned), devices that collect and forward security event data to be processed for the prevention and detection of malicious activity.

IP/Domain Discovery

We will set up a service for users to be able to report suspected malicious IP addresses or domains. This service will typically flow through to the Web takedown service so these sites can be removed and cause minimal harm.

Web Takedown

BAE Systems will help establish a service that proactively finds and/or is informed about malicious websites and sends notifications to the host or owner to remove the site from the internet before significant harm can be done.

Vulnerability Disclosure

We will establish a service that allows anyone to responsibly report a vulnerability they have found in a government website, application or service.

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) 1483 816000

BAE Systems Digital Intelligence
8000 Towers Crescent Drive
13th Floor
Vienna, VA 22182
USA
T: +1 720 696 9830

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

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

@BAESystemsDigi

BAE SYSTEMS