STARA®: Phased Security Threat and Risk Assessment

Countering the security threat in 'Breadth,' not just 'Depth'

Digital Intelligence

BAE SYSTEMS

Introducing STARA®

A Phased Security Threat and Risk Assessment Programme

Cyber security is now commonly on the agenda of board room budget discussions. However, before investing in any new security arrangements, we advise that organisations should ensure they assess all sources of risk and security threats so that they can minimise the successful exploitation of attack vectors, through a proportionate deployment of resources and controls in line with their risk appetite. To assist organisations in this process, BAE Systems offers a Security Threat and Risk Assessment (STARA®) framework which provides a holistic approach to helping large organisations determine and assess security threats and risks covering the full spectrum of threats, and assists them in determining how best to deploy resources to reduce risk and enhance security.

Why a new approach to enhanced security, risk minimisation and threat remediation is required

In recent years, the issue of cyber security has become a normal part of board level discussions and budgets. However, the threat landscape is continuously evolving and many organisations are finding that even with the best intentions and most advanced cyber security technology deployed, threat actors are still managing to penetrate their defences, impact their business operations, or obtain exposure to corporate intellectual property rights (IPR) and assets. Understandably frustration levels are high, however in order to break this cycle, and before allocating new resources or funding to achieve it, organisations need to consider the relationship between security, threat, and risk.

At a high level, security is enacted in response to a threat, where the risk of compromise necessitates action in line with the organisation's attitude to the risk.

The security of an organisation, its people, or business processes can be enhanced through the implementation of different safeguards, procedures and processes, of which cyber security may form only one of several components. With this in mind, a new approach to enhanced security, risk minimisation and threat remediation is required. This involves Chief Information Security Officers (CISOs), Chief Risk Officers (CROs) and Heads of Security widening the scope to include not only security threats, but all threats to an organisation and its business operations, in conjunction with a full risk assessment, covering both the potential effect of threats being realised and the corporate attitude towards those risks.

This is important because in today's digital world, no amount of money spent on cyber security can guarantee that threat actors will not be able to breach the perimeter, potentially leading to a successful attack on an organisation. Instead, the focus of security leaders is now to understand the risks they face and minimise the successful exploitation of attack vectors, through a proportionate deployment of resources and controls in line with the organisation's risk appetite.

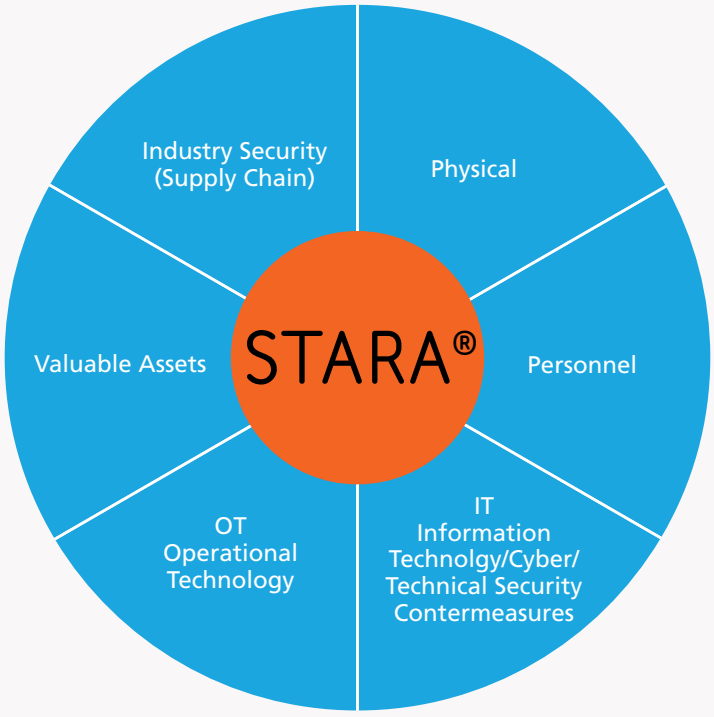
Consider this example: if threat actors are aware that a target organisation is protected by layers of cyber defence (defence in depth) but lacks effective governance, or has weaknesses in physical or personnel security, they may decide that the easiest, most cost effective and quickest way to penetrate an organisation, steal or gain control of a critical asset, is simply to walk through the front door or gain access through open, unsecured doors/windows and take what they wish; possibly target an employee, social engineer or extort cooperation from them in order to achieve a goal. Experienced threat actors seeking to attack an organisation may seek to circumvent strong defences (such as cyber defence) and select the easiest route, wherever possible.

In view of the evolving threat scenarios and landscape, an in-depth, holistic review of all possible sources of threat and associated risks covering the following domains is required:

- Physical: All tangible physical elements constituting a business environment, its security architecture (i.e. buildings, walls, fences, doors, windows, locks), and electronic hardware (CCTV, entry systems). This includes evaluating the potential impact of hostile electronic surveillance measures targeting the physical infrastructure of an organisation.
- Personnel: Consideration of all human factors – behaviour, how are systems used, policies, processes and procedures; business and security training, security clearances, recruitment practices, governance, managing insider risk, the use and handling of materials and documents; including controls around the existence or use of electronic devices within business environments.
- Information Technology (IT): Everything relating to information and communications technology crucial to business operations, and the defence of these systems. This includes:
    - Securing software, hardware, telecommunications equipment and communications devices; on-premise and cloud hosted systems, products and services; establishing processes and controls to protect the confidentiality, integrity and availability of IT and the data generated by, belonging to, or handled by the organisation.
    - Practicing good operational security (OPSEC), and where appropriate, deploying Technical Security Counter Measures (TSCM) to identify and protect against Radio Frequency (RF) and Electromagnetic compromise of IT systems.
- Operational Technology (OT): Securing hardware and software used in monitoring or controlling enterprise and industrial operations for example within Critical National Infrastructure (CNI), and the defence of these systems, with a focus on ensuring the safety of operations, the availability and reliability of systems, and the integrity of commands that flow between the components of OT that enable Industrial Control Systems and automated processes. This includes practicing good OPSEC, and where appropriate, deploying TSCM where appropriate to identify and protect against the compromise of OT systems.
- Valuable Assets: Securing information assets (e.g. databases, system documentation, IP) and physical transferable assets of value (e.g. business equipment).
- Supply Chain: Consideration of the organisation's supply chain relationships with third-parties to ensure its resilience to attack, and ensure partners may not become an attack vector.

Introducing the BAE Systems Security Threat and Risk Assessment (STARA®) framework.

From decades of experience gained from working with many large government organisations, BAE Systems has developed a holistic approach to helping organisations determine and assess security threats and risks covering the full spectrum of threats, and assisting them in determining how best to deploy resources to reduce risk and enhance security.



BAE Systems has developed a holistic approach to helping large organisations determine and assess security threats and risks covering the full spectrum of threats

Figure 1: Scope of Security Threat and Risk Assessment for Business and Industrial Operations

STARA® is a unique and repeatable framework of services and tools that deliver actionable insights into the true vulnerability of organisations to their own specific technical and physical threats.

Designed by BAE Systems and delivered in a modular format that allows customers to invest at their own pace, our subject matter experts define the real threat an organisation faces, and assess how this threat actually materialises as risk.

This may first be done through table-top analysis of the technical operations, human behaviours, physical facilities and/or supply chain all enriched by our Threat Intelligence insights, which is then subsequently demonstrated and proven on the ground with our experts undertaking highly targeted intelligence led physical and cyber intrusion testing within the organisation.

STARA® delivers results in easy to consume reports with clear descriptions of findings and actionable recommendations for change.

The STARA® framework spans the seven areas of security threat and security risk, shown in Figure 1, and allows an organisation to evaluate its current security posture in comparison to industry standards, understand the threat to its operational environment, its vulnerability to a targeted or full-spectrum attack, and the risk it is carrying. The STARA® framework includes collaborative workshops which enable organisations to make informed decisions, which help them move from a two dimensional security structure to a comprehensive, adaptive and hybrid defence model, implemented in depth and breadth.

STARA® delivers results in easy to consume reports with clear descriptions and actionable recommendations for change.

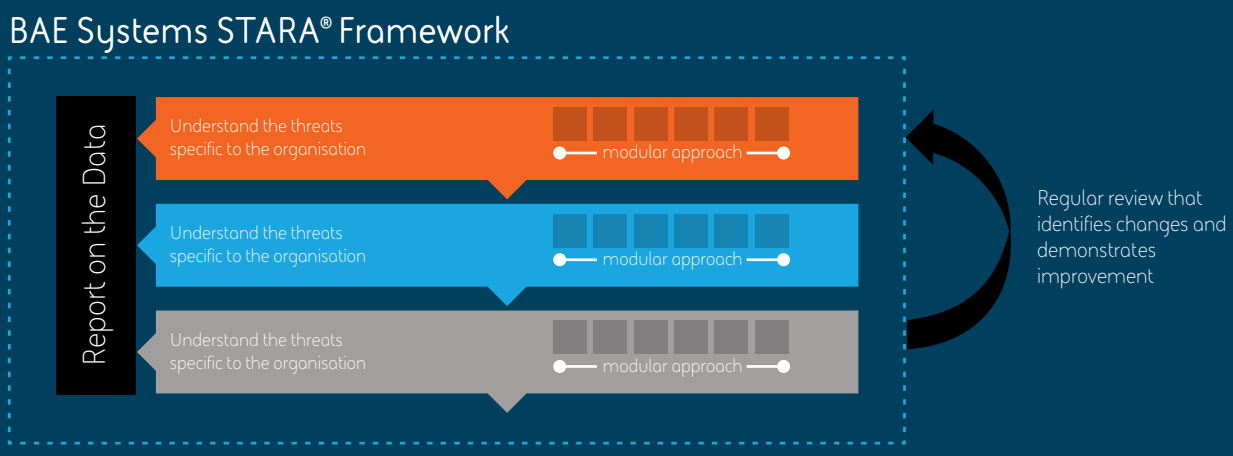


Figure 2: The phasing of the BAE Systems STARA® framework.

Each phase of the STARA® framework is aimed at helping an organisation develop a better understanding of the threats it may face or is already facing, its actual security posture in relation to those threats, and the risks of significant events occurring as a result of threats being realised. Progressively, through the programmes of investigations, interviews, workshops, reports and plans, STARA® provides the answers to a framework of logical questions, which enable security managers and corporate executives to make better, informed decisions.

As outlined below, through cooperation between the customer organisation and BAE Systems, the different phases of the STARA® framework enable a methodical approach to the analysis of the security threats and associated risks:

Phase 1: Understand the threats

- We will conduct stakeholder workshops to understand what your organisation does and how it conducts its operations.
- We will leverage our threat intelligence and Open Source Intelligence (OSINT) expertise to capture evidence and assess the sector you operate in.
- We will help you define your current threat landscape and assess how it relates to your organisation's core strategy, mission and operations.
- Together we establish your attitude to risk (e.g. acceptance, avoidance) and approach to corporate security.
- In recognition of the above, we consider the personas and motivation of threat actors who may be motivated to attack your organisation, and evaluate your current security focus.
- Based on the very high level information of your infrastructure and assets gathered during Phase 1, we validate the existing threat landscape by postulating principle attack vectors that threat actors may utilise to breach and attack your organisation.

Summary:

What is the High Level threat? Identify the risk.

We will identify, understand and define the current threat landscape in which an organisation operates, whilst modelling the delivery of its core strategy, mission and operations.

The different phases of the STARA® framework enable a methodical approach to the analysis of the security threats and associated risks

Summary:

What is the threat? Assess the risk.

We will review and understand physical, people and digital assets and all documentation, in order to understand their criticality to the organisation and its operational environment.

Phase 2: Predict the risks

- We use stakeholder interviews, workshops, and document reviews to gain a detailed understanding of your operational environment, and physical, personnel and digital assets and their criticality.
- A detailed gap analysis will be carried out to assess your baseline controls against industry standards.
- Asset criticality will be reviewed against CNI categories/ classifications in relation to your mission and core operations.
- Effects of concern and their impact on your organisation will be assessed and validated through collaborative workshops with stakeholders and industry experts.
- We define your security architecture, attack surface, the vulnerabilities of your people, assets and processes that could be exploited, and any attack vectors which they may enable.
- We assess the maturity and effectiveness of your current security posture against industry standards (e.g. NIST, CSMA).

We help you build a Security Improvement Plan to enact the recommendations

Phase 3: Prove the vulnerabilities

- Intelligence led security testing can build on any vulnerability analysis, as well as our earlier consideration of the threat actors who may be encountered. Our Security Testing teams undertake real-world testing of systems in a manner similar to how those threat actors would normally behave.
- Physical penetration tests of facilities can be carried out to show how non-technical attacks could result in system compromise or data exfiltration.

At the end of the assessment activities, BAE Systems will provide appropriate reporting and recommendations to remediate any issues found:

- We assess the different risks identified across all the domains investigated including your risk profile, then create a report to explain our findings and reasoning to you.
- We discuss and evaluate the findings with you, and jointly agree a set of recommendations that outline what you should do to mitigate risks, remediate vulnerabilities and enhance your secure posture.
- We help you build a Security Improvement Plan to enact the recommendations which will help you to rapidly mature your security posture.

Summary:

Is the risk only hypothetical? Can we demonstrate it in the real world?

Where appropriate, we will utilise our subject matter experts to undertake real world security testing, be that technical or physical, or a blend of both. This might include intelligence led technical security testing, or a physical test of the security facilities.

The BAE Systems Differentiator

In conducting STARA®, we employ a unique threat led and evidence based approach. This ability is derived from our experiences detecting and protecting some of the largest and most targeted organisations in the world from cyber-attack, our own threat intelligence services, and from over a decade of experience in assessing and working with owners of CNI to reduce their risk and make them more secure.

The success of the STARA® programme is, we believe, down to our philosophy that in order to succeed, STARA® must first view the organisation as a whole to truly understand all sources of threats, risks and vulnerabilities, rather than focus on the traditional approach of building layered levels of security in depth, or prioritising limited resources and budgets to meet expected compliance requirements.

Our STARA® framework is a tried and tested methodology which has been validated by the UK and other governments. Where necessary, we bring a mix of specialist skills, the combination of which others are not able to provide. These include, amongst others, counter intelligence, covert methods of entry, RFID hacking, surveillance, hostile reconnaissance, forensics and malware analysis. In addition, we have developed the only OFQUAL accredited Covert Operations and Threat Management (COTM) course, a standard to which all of our testing team are certified. Moreover, our Physical Penetration Testing is one of only a handful which are both certified by CREST[1] and The Security Institute.

When engaged, our Red Team consider all hazards and threats, not only those you would expect to find. Consequently, our approach is both proactive (looking for threats, vulnerabilities and risks), and reactive (if approved by the customer, the results of investigations often necessitate prompt corrective action that cannot wait).

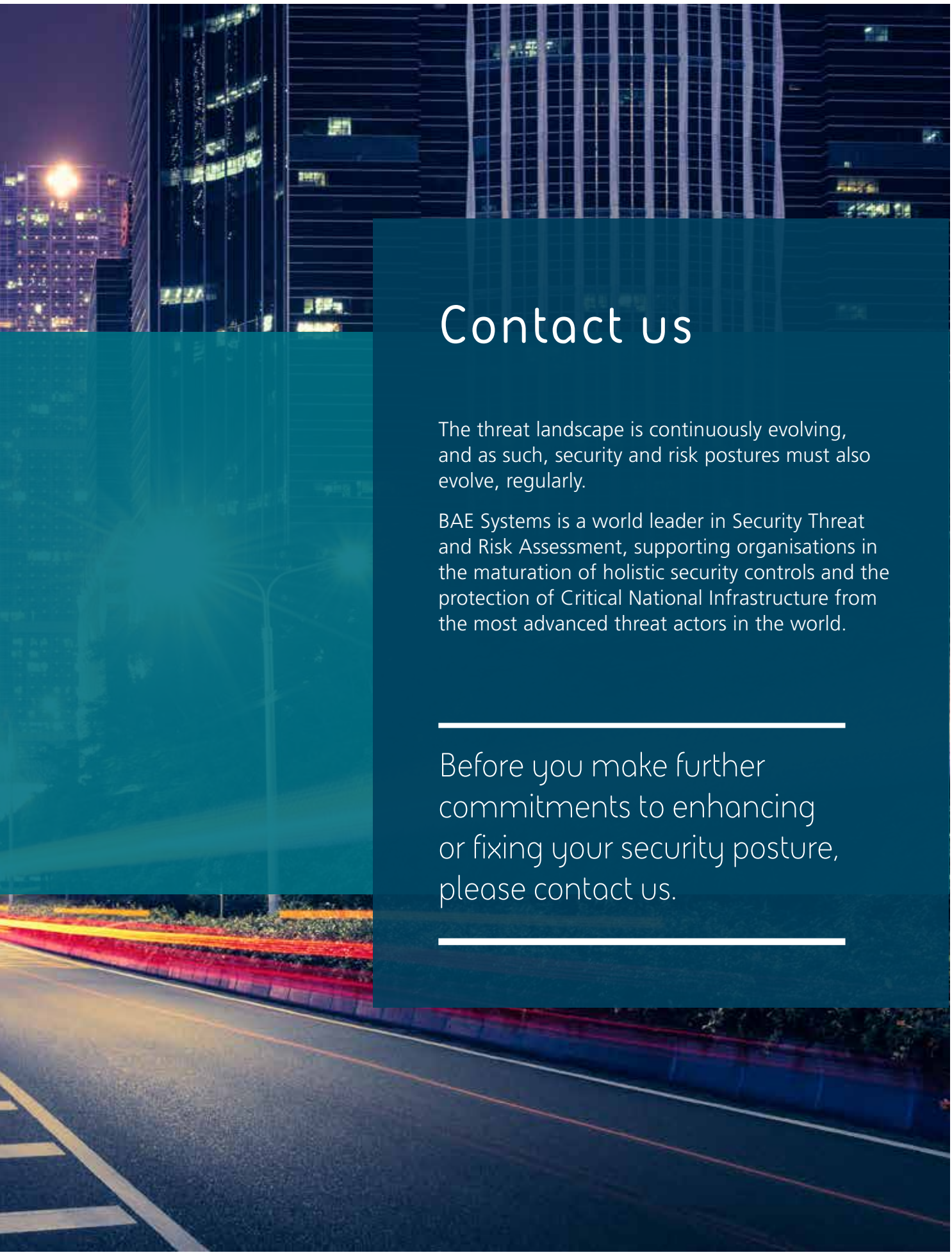
For CNI organisations, the STARA® programme has a further, immediate advantage: we already have a rich heritage of experience gained from having embedded teams investigating and mitigating security threats for many other CNI organisations. Based upon this experience, we have templates, artefacts and processes which are ready for immediate deployment.

Our STARA® framework is a tried and tested methodology which has been validated by the UK and other governments.

[1] Crest is an international not-for-profit, membership body representing the global cyber security industry: https://www.crest-approved.org/about-us/who-are-crest/

Our Customers

Typical customers for the STARA® programme include large government organisations (UK & International), financial services, as well as the full range of organisations who provide a nation's CNI (health, chemicals, energy, communications, transport, utilities).



Contact us

The threat landscape is continuously evolving, and as such, security and risk postures must also evolve, regularly.

BAE Systems is a world leader in Security Threat and Risk Assessment, supporting organisations in the maturation of holistic security controls and the protection of Critical National Infrastructure from the most advanced threat actors in the world.

Before you make further commitments to enhancing or fixing your security posture, please contact us.

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
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

BAE Systems Digital Intelligence
Surrey Research Park
Guildford
Surrey, GU2 7RQ

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

BAE SYSTEMS