Enhancing an International Government's Security Capabilities

A National Cyber Security Centre strengthened its security posture, expanding operations and implementing a new strategy to fortify its critical national infrastructure and keep citizens safe

Digital Intelligence

BAE SYSTEMS

Introduction

Resilient critical national infrastructure underpins society. But what happens when it comes under attack? Across the globe, as geopolitical tensions mount and services become increasingly digitised, threats to critical infrastructure are at an all-time high. In the last few years alone we've seen malicious actors target everything from oil pipelines to hospitals and satellites.

An international government found itself in a similar situation when it fell victim to a cyber-attack that created real-world consequences, leading the nation to review its cyber security posture.

In the aftermath, its National Cyber Security Centre (NCSC) – the primary authority of the country's cyber domain – focused on strengthening its security capabilities with the ultimate aim of keeping citizens safe. The NCSC engaged BAE Systems Digital Intelligence to help enhance its security operations through a robust strategy.

STARA®

Working closely with the NCSC, our experts delivered our tried and tested **Security Threat and Risk Assessment (STARA®)** – a methodology that combines technical, cyber, personnel and physical domains to provide a holistic view of an organisation's security posture. Applying this approach while navigating a challenging external landscape, we collaborated to boost the nation's security capabilities. At the same time, through the deployment of innovative solutions, we reduced the impact of the NCSC's budget, **saving it a significant amount of money.**

The Challenge

Following the cyber-attack, the international NCSC wanted to build a sustainable and adaptable model that would bolster its security posture. Part of this involved expanding and scaling its delivery in line with the country's security strategy and EU directives. However, as with any transformation, the challenges it had to address were multifaceted – and the fact the project was delivered during the Covid-19 pandemic only added an extra layer of complexity.

A key consideration from the outset was physical security. The NCSC's expansion meant moving to a larger, more suitable facility – a transition that was easier said than done. While the permanent facility was under construction, an interim one was selected: a listed building. Any added measures therefore had to provide maximum security, while being mindful of the facility's protected status and transient nature. The building's weight and height constraints also posed difficulties. This required an innovative approach to create a secure working environment where classified information could be controlled.

Lastly, the project was undertaken against a tumultuous external backdrop. The work began as the world grappled with the global pandemic, so it was necessary from the outset that strategies and methods were adapted to ensure the safety of everybody involved. At the same time, the invasion of Ukraine created a rapidly changing, increasingly aggressive threat landscape. Not only were we faced with a challenging operating environment throughout the delivery, the need to enhance the nation's cyber capabilities had never been higher.

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

The Solution

We worked closely with the NCSC to navigate these challenges, deploying our BAE Systems Digital Intelligence STARA methodology.

Providing a comprehensive and scalable risk assessment, STARA applies evidence-based threat intelligence to assess an organisation's security risk across multiple, traditionally siloed domains – physical, technical, personnel and cyber. It looks at key threat actors from many angles; their capability and motivation to detect vulnerabilities, and the tactics, techniques and procedures they could use to launch an attack.

By applying STARA for the NCSC, our goal was to provide tangible recommendations, acknowledging the country's geopolitical background, to help drive impactful national security change. As part of this, we sought to address the immediate needs of the organisation, responding to the cyber-attack and, in turn, helping to fortify the nation's critical national infrastructure.

STARA® provides full-spectrum defence against advanced threat actors

Our team worked together with the NCSC to deliver technical solutions and a framework that helped to position the country as valued on a global stage. This included:

Implementing cutting edge security expertise

Drawing on the expertise of our subject matter experts across physical, cyber and personnel security, our framework ensured the NCSC had the right resources at the right time to deliver maximum impact. Recommendations from our team operating at a high level of expertise and security clearance were implemented and accepted throughout the programme, building all-important trust with the customer.

Enabling expansion through designing a secure working environment

Due to the nature of the NCSC facilities, a new design was needed when it came to creating its secure working environment. This required an innovative approach, departing from standard US, EU or UK Government blueprints. Thorough stakeholder engagement was needed to upskill all contractors involved and ensure everyone understood how to maintain the integrity of the secure working environment, while adopting a different design and specialist materials.

Delivering resiliency during a dynamic threat environment

Another dimension of complexity stemmed from the rapidly evolving threat landscape, which required a new level of resiliency and adaptability from both the NCSC and our team.

Developing a security culture

We also invested in developing a security culture and awareness programme. The aim was to educate existing staff and suppliers on key risks, and create an internal capability for inducting new employees into an evidenced-based, threat aware culture both now and in the future.

Creating a technology strategy

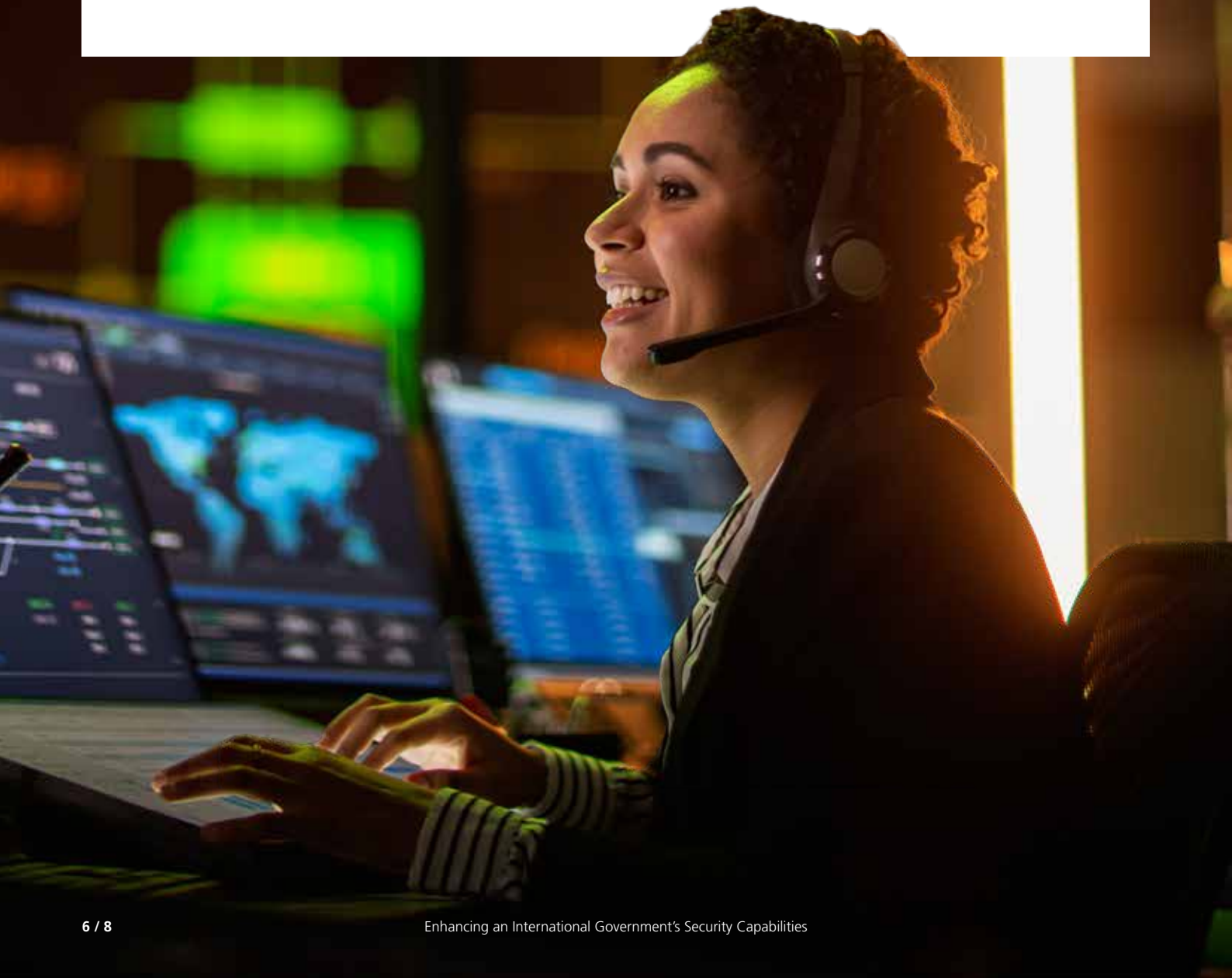
We designed a strategy which marries the NCSC's mission, vision and goals with necessary technology principles, while providing enough flexibility to ensure it remains relevant to the organisation's evolving mission.

The Results

Against a complex backdrop, the transformation project was a great success. Underpinned by STARA, the collaborative approach between our team and the country's NCSC, involving stakeholders, government bodies and partners, resulted in a comprehensive and unified approach to cyber security. Crucially, the secure working environment we built is being considered as a potential template in other government organisations and our work to upskill stakeholders involved has created a national capability.

The project's success is evident in positive feedback from key stakeholders who praised our in depth understanding of security and our ability to seamlessly incorporate experienced subject matter experts.

Not only that, by deploying innovative solutions, we reduced the impact of the NCSC's budget, saving it a significant amount of money. This meant the government was able to redirect the funds to navigate the challenging geopolitical environment that had escalated as the work was taking place, demonstrating the programme's wide-reaching impact.



Learn how our STARA solution can help you assess security threats and risks to your organisation across the full spectrum of attack types

- **STARA Security Threat & Risk Assessment**
  Holistic and modular security, yhreat and risk assessment framework (Find, Baseline and Build)
- **Physical Infrastructure Risk Assessment & Management**
  Full spectrum physical penetration testing and threat replication
- **Asset Vulnerability Assessment**
  Targeted and in-depth security review of an individual asset or platform
- **Security Transformation & Remediation**
  Team supporting organisations to advance and matures its security posture
- **Insider Risk & Personnel Assurance**
  Understand, assess and mature the insider risk, human factors security
- **Supply Chain & Risk**
  Understand, manage and mature the security of supply chains
- **Security Operations Needs Analysis**
  Analysis of current and future security operations needs
- **Security Operations Centre Maturity Analysis**
  Diagnostic assessment of a SOC and its capability to defend against APT

Click here to find out more

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