Building Next Generation Cyber Defence

For Government Organisations and Large Corporations

Digital Intelligence

BAE SYSTEMS

Moving from Cyber Security to Cyber Defence at a National Level

Looking back over the last fifty years, several key developments stand out which in hindsight, were clearly all stepping stones to the creation of the internet experience which now dominates and underpins all our lives: initial concepts of wide area networking by which networks could connect to each other, the development of packet-switching, routers and networking protocols such as TCP/IP, and the fabulous World Wide Web pioneered by Tim Berners-Lee in his research at CERN. Then came the mobility wave of new technologies, Smart Phones and their wealth of apps, social media, user forums, chat groups, gaming and e-commerce. Today all modern societies are dependent upon their ability to access the internet and benefit from the capabilities it offers: our businesses depend on it, our social lives revolve around it, and our children are growing up in an environment where it touches almost every aspect of their lives.

And yet, until only very recently, even though whole nations have become dependent on it, few countries have realised the full importance of ensuring that their businesses, citizens and partners are living and conducting business in a secure environment: for far too long, the defence of national cyber space has been left to individuals and private corporations, and the influence of market forces.

All this is changing. Governments are realising that their nation's prosperity, Critical National Infrastructure and national defence all hinge on ensuring a stable, free and secure national cyber space. Unfortunately, with this realisation, come four very important questions:

- How do you protect a whole nation from cyber threats?
- What are the cyber threats we face?
- What resources do we need to protect ourselves from them?
- What can we do to improve the efficiency and effectiveness of existing investments in cyber defence technologies?

Governments are realising that their nation's prosperity, Critical National Infrastructure and national defence all hinge on ensuring a stable, free and secure national cyber space.

A Multi-Pronged National Approach

To protect ourselves from threats that derive from cyberspace, we must first understand what cyberspace is: an interdependent network of information technology infrastructures that includes the Internet, telecommunications networks, computer systems, internet connected devices and embedded processors and controllers.

As such, cyber threats can originate and propagate through cyber space from many places: malware and cyber attacks can be delivered across corporate network links, transported across the communications links provided by our service providers, or injected or created on network devices, by external or inside parties. Once a foothold is found, the web of interconnectivity that facilitates the internet can then be exploited as a weakness, providing the opportunity for malware to spread, or for attackers to reach out from one device to access, control and manipulate another device somewhere else, either locally or on another interconnected network far away.

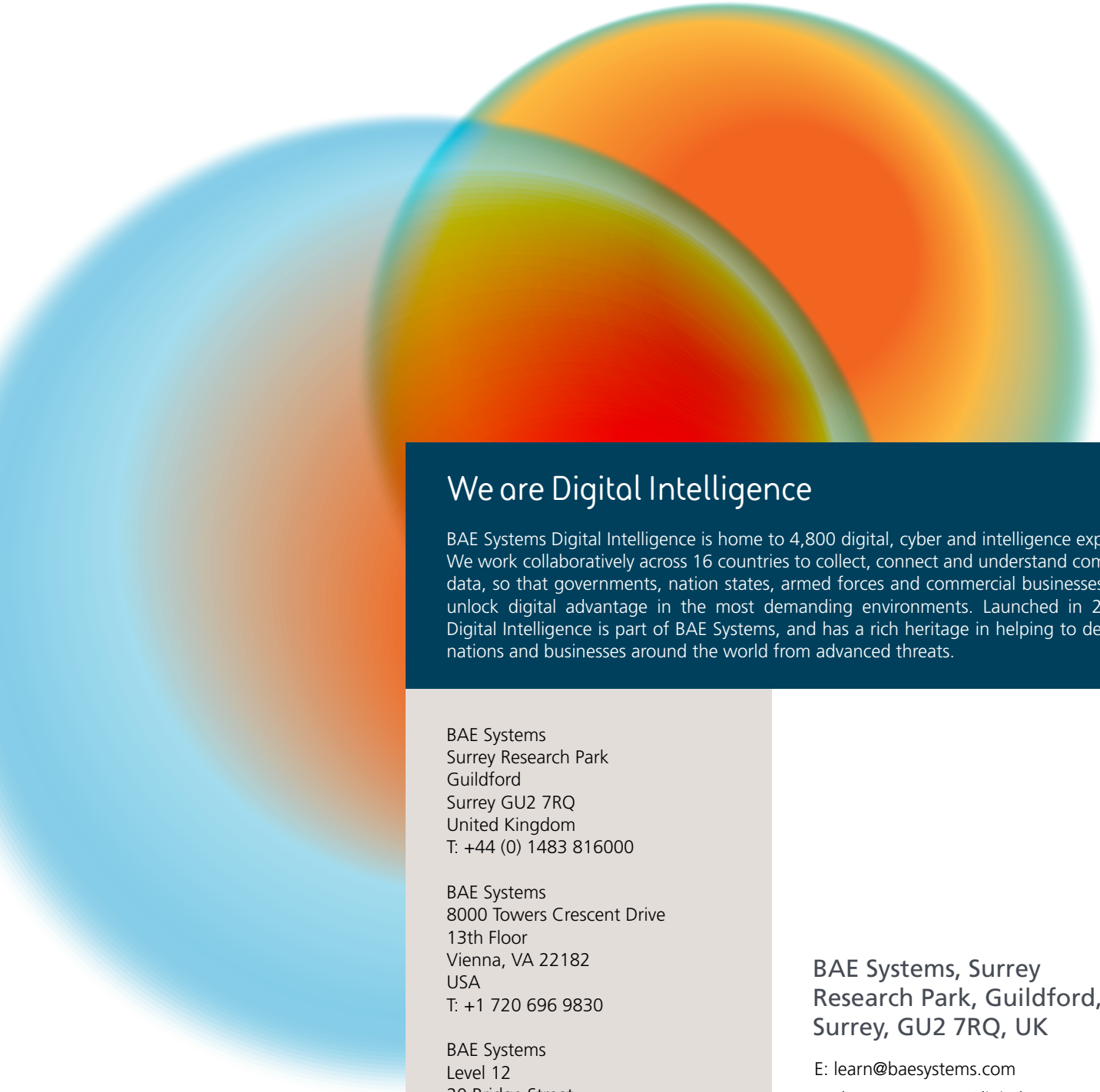
The varied reasons why cyber attackers – threat actors – wish to do this are of growing concern to governments when looked at through a national lens:

- to attack, steal from or weaken the nation's economy. When theft is involved, individual sums can be large and run into the billions
- to plan and conduct terrorist activities
- to threaten the day-to-day operational capability of a country through attacks on Critical National Infrastructure
- to challenge and undermine the nation's democratic process
- to conduct espionage
- to facilitate criminal activity
- to steal intellectual property
- to undermine business processes, influencing the awarding of high value international contracts or to gain competitive advantage
- to generate and spread false news and alternative ideologies.

Defending a nation from cyber threats will naturally be more complicated than simply securing an individual computer in someone's home or business. Resources will have to be deployed at national scale, in an architecture that spans the hierarchical network structure of the nation, providing cyber security at many different levels. It will have to cater for the many different types of threat, their intentions and varied origins. It will require a different mind-set, and to be effective, will require a new openness between affected parties or potential targets, based on a willingness and ability to share relevant information with each other in a timely fashion, in order to identity threats and remediate them before effective damage can be done. It will require new capabilities, to not only detect threats using large scale analytics, to address threats using national computer emergency response teams [CERTs], to issue threat advisories and enable threat intelligence sharing, but also to deter those behind the threats/cyber attacks from attempting them in the first place.

National cyber threat defence will however not simply be about deploying new forms of technology to counter the techniques being misused by others who would cause us harm. Ultimately, the technological resources which will be deployed can only be successful if sufficient and appropriate human resources are available to manage and support them. This in itself will be a national challenge. As the world's digital economy has evolved, a global shortage of IT and cyber skills has emerged. So much so, that a fundamental part of any national cyber defence plans must now include due consideration for the education, training and retention of a new generation of IT cyber experts to not only man government infrastructures and CNI organisations, but to also ensure sufficient supply to underpin national businesses, academia and social structures.

Lastly, to optimise the ability of IT security experts to utilise any new cyber security defences placed at their disposal, nations should seek to ensure that proven cyber best practices and work processes are learned and followed by all. For some nations to achieve this, it may be possible to fast track benefit from the shared knowledge of cyber best practices and work processes already accumulated by strategic partners who have a rich heritage in national cyber defence.



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
Surrey Research Park
Guildford
Surrey GU2 7RQ
United Kingdom
T: +44 (0) 1483 816000

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

BAE Systems
Level 12
20 Bridge Street
Sydney NSW 2000
Australia
T: +612 9240 4600

BAE Systems
1 Raffles Place #42-01, Tower 1
Singapore 048616
Singapore
T: +65 6499 5000

BAE Systems, Surrey Research Park, Guildford, Surrey, GU2 7RQ, UK

E: learn@baesystems.com

W: baesystems.com/digital

linkedin.com/company/baesystemsdigital

twitter.com/BAES_digital

BAE SYSTEMS