Department for
International Trade

Cyber Security

Export Strategy

Contents

Foreword

The cyber security challenge – an opportunity for UK business

A thriving UK cyber security sector is a key national security and prosperity aim as set out in our five-year National Cyber Security Strategy.

The Government is committed to making the UK one of the most secure places in the world to do business, and cyber space is an important and expanding part of our economy. The UK is dedicated to working with all states to develop a common understanding of the benefits of a free, open, peaceful and secure cyberspace.

The world is experiencing an unprecedented transformation as relationships between organisations and their customers and stakeholders take place in increasingly digitised environments.

The rapid rise in disruptive digital technologies inevitably exposes system vulnerabilities, as seen in recent high-profile cyber attacks on large businesses and public organisations.

This new reality poses huge challenges as businesses and organisations evaluate urgent investment decisions in a fast-changing world where tomorrow's technology hasn't been invented yet.

The accelerated pace of digital change brings a great opportunity to promote the UK's cyber security expertise to international markets. Robust export control regimes will ensure that human rights are a key part of the process.

Exporting to existing and new markets will help build a Britain that is fit for the future.

This strategy sets out how the UK Government will strengthen support to world-leading British firms with innovative offers emerging from the nation's vibrant cyber security ecosystem.

The Rt Hon Dr Liam Fox MP

Secretary of State for International Trade and
President of the Board of Trade

A new cyber security export strategy

The Department for International Trade (DIT) works to achieve UK and global prosperity by promoting and financing international trade and investment, and championing free trade.

This new strategy harnesses DIT offices worldwide, working in close partnership with other parts of government, trade and commercial experts, academia, industry and industry-leading bodies such as the City of London Corporation and Healthcare UK.

Specialised support for companies

DIT will focus on three tiers of support:

Pursue

In priority markets, DIT will act as a trusted advisor to support UK companies bidding for major opportunities, primarily selling to overseas governments and Critical National Infrastructure (CNI) providers.

Enable

DIT will focus on six key sectors which are threat actors' biggest targets and have significant cyber security budgets. DIT will curate bespoke offers for the top buyers in these sectors worldwide, running trade missions and pitching UK companies to address identified capability gaps.

Respond

To showcase the best of UK cyber security, updated branding and marketing will be developed and deployed around the globe alongside new cyber content on great.gov.uk

The growing importance of cyber security

DIT works to deliver both commercial and national security objectives.

In 2016 the Government published an updated National Cyber Security Strategy (2016–2021)[1]. The strategy is supported by £1.9billion of transformational investment. It sets out ambitious policies to protect the UK in cyber space. Our vision for 2021 is that the UK is secure and resilient to cyber threats, prosperous and confident in the digital world.

The strategy is delivering policies and capabilities, building on three core pillars and supported by international partnerships, to:

- Defend our people, businesses and assets across the public and private sectors;
- Deter and disrupt our adversaries – states, criminals and hacktivists;
- Develop critical capabilities to build skills, support growth and stimulate science and technology.

DIT works closely with the National Cyber Security Centre (NCSC) and all parts of government to support these objectives.

National Cyber Security Centre, London

[1] www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf

The cyber security environment

The UK Government defines cyber security as the protection of networked information systems.

The field is increasing rapidly in importance as a security issue for businesses and governments worldwide.

Recent major cyber attacks have disrupted and threatened large global and UK organisations.

The global cyber security industry has evolved from protecting critical information systems, data and networks. Global spend on cyber security products is expected to exceed £759 billion cumulatively from 2017 to 2021.[2]

Despite this record spending on cyber security, the Hiscox Cyber Readiness Report 2017 found that 53% of 3,000 companies surveyed were ill-prepared to deal with a cyber attack.[3]

The cyber security sector is vast. The market is a unique 'borderless' environment and threats change constantly due to the shortening shelf-life of technology.

While buyers' understanding of cyber security risks is improving, there is no dominant international standard or body of best practice.

Buyers may need advice on what they need, especially in less cyber mature economies. This presents an opportunity for UK cyber security companies to provide trusted solutions.

The UK ecosystem combines technical expertise and a world-leading research base with a history of cyber security excellence and leadership on developing global standards. UK companies are ideally placed to provide expert, trusted advice and services to buyers across the world.

The Government's Industrial Strategy[4] seeks to build a Britain fit for the future, with the UK at the forefront of innovative industries. The Government will work with the UK cyber security industry to capitalise on its strengths in these areas, particularly as applicable to artificial intelligence (AI) and the digital economy.

GCHQ Building Cheltenham

[2] Q2 Cyber Security Market Report 2017 published by Cyber Security Ventures – https://cyber securityventures.com/cyber security-market-report/ [3] Hiscox Cyber Readiness Report 2017 - https://www.hiscox.co.uk/cyber-readiness-report/ [4] https://www.gov.uk/government/publications/industrial-strategy-building-a-britain-fit-for-the-future

The megatrends driving cyber security investment

The 'digitisation of everything'

The world is experiencing an unprecedented rate of disruptive innovation built around the use of internet-based technology to better connect people and things.

Public organisations are increasingly investigating how to use these technologies for citizens' benefit.

The Government's Grand Challenges and the establishment of an Office of AI positioned the UK at the forefront of these developments as technology changes the way people live and work.

Emerging technologies such as blockchain are entirely web-based, and commercially available applications now range from personal identification to asset verification and contracting.

The increase in digitisation brings benefits, but also presents challenges for data security and user privacy as the quantity of hackable data increases exponentially.

Data protection and the ability to secure information

Companies are experiencing more frequent and damaging breaches. Firms failing to protect their customers' data face increasingly large fines and reputational damage and those investing in good cyber security will gain a competitive advantage.

The availability of cyber skills will be a major factor in securing critical systems, providing opportunities for firms that specialise in training and education.

New regulation such as the EU's General Data Protection Regulation is driving organisations to build information security into their wider strategy.

Countering criminal networks and hostile state actors

Data remains the primary target for hackers. Cyber criminals and hostile state actors are increasingly exploiting vulnerabilities in users' apps, connected devices, and platforms to gain unauthorised access to personal information.

High-profile examples show that critical operational technology can also be vulnerable to cyber attack. Recent ransomware attacks have shone a spotlight on the vulnerability of CNI, causing business disruption and remediation costs.

The increasing complexity of cyber attacks by criminals, nation states and hacktivists has created high demand for effective cyber security across the enterprise market and public sector.

- **Data volumes online will be 50 times greater than today by 2020, says Microsoft.**[5]
- **Businesses such as Airbnb, LinkedIn, Facebook and Amazon hold data on more than 1 billion users.**
- **94 million connected cars are expected to ship in 2021, 82 percent of the total number of cars shipped that year.**[6]
- **It is forecast that the cost of data breaches will rise to £6.07 trillion globally by 2022, almost six times the estimated cost of breaches in 2016.**[7]

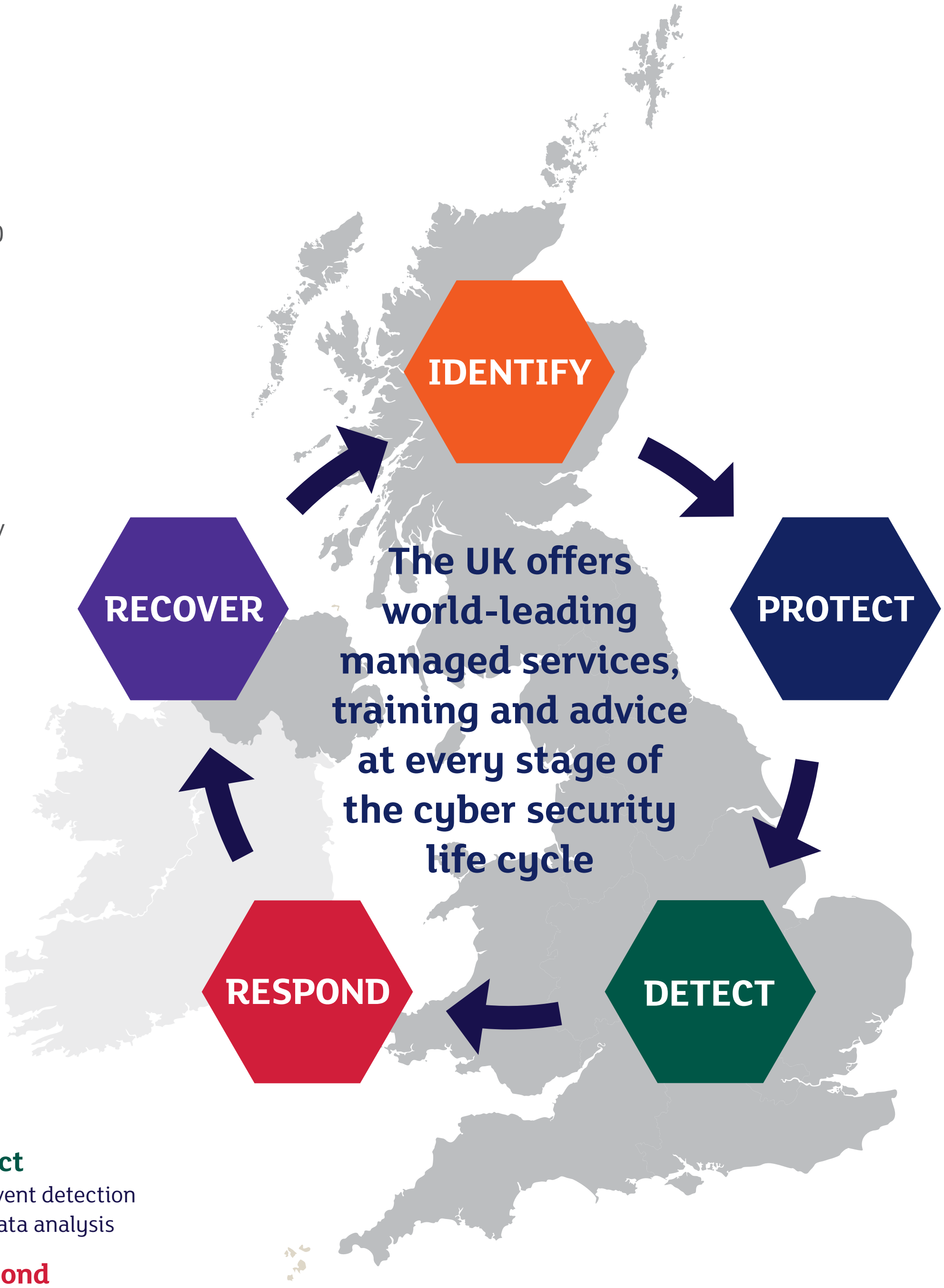
[5] CSO Online Cyber security Business Report 2017 - https://www.csoonline.com/article/3110467/security/cybercrime-damages-expected-to-cost-the-world-6-trillion-by-2021.html [6] Business Insider Intelligence Report 2017 - http://www.businessinsider.de/internet-of-things-connected-smart-cars-2016-10?r=US&IR=T [7] The Future of Cybercrime & Security: Enterprise Threats & Mitigation 2017-2022 - https://www.juniperresearch.com/researchstore/innovation-disruption/cybercrime-security/enterprise-threats-mitigation

How prepared is business?

Research shows there is a critical need for better understanding around cyber security risks, and for advice on which solutions can safeguard users, businesses and governments.

A Lloyd's 2016 survey found that, while 90 percent of big businesses have been hit by a major cyber attack, less than half are worried about suffering another breach in the future.[2]

Having secure systems means thinking about **people, processes and technology** rather than simply buying the right hardware and software. This is illustrated by the National Institute of Standards and Technology cyber security framework, and the UK has the world-leading capability that underpins this approach.



The UK offers world-leading managed services, training and advice at every stage of the cyber security life cycle

Identify

1. Asset management
2. Strategy development
3. Governance
4. Risk management

Protect

5. Access control
6. Training
7. Secure network infrastructure
8. Threat intelligence

Detect

9. Event detection
10. Data analysis

Respond

11. Response planning
12. Incident analysis
13. Mitigation

Recover

14. Recovery planning
15. Business continuity/ Disaster recovery
16. Communication and media

[8] Lloyd's Survey 2016 - http://www.insurancebusinessmag.com/uk/news/breaking-news/90-of-big-firms-hit-by-major-cyber-attacks--lloyds-survey-37932.aspx

The cyber security buying environment

The environment in which companies and governments are making buying decisions is fast moving and complex.

Changing technology, threats and regulations means buyers are frequently uncertain about what the gold standard is in the sector.

The 'half life' of technology is only a few months, and too few new pieces of technology are currently secure by design.

Organisations looking to invest in cyber security have a range of goals, including further automation of cyber security to limit human error, securing legacy systems and introducing secure by design systems.

UK companies have the capability to provide best-in-class services across a wide range of cyber security sector requirements.

Capability	Explanation
Incident investigation and cyber forensics	The identification and investigation of potential cyber security incidents
Threat intelligence collection, feeds and analysis	Monitoring of and response to emerging threats
Cyber security certification and training	Systems to ensure strong information security and data protection
Vulnerability assessment and management	Identification of risks of cyber attacks and development of response strategies
Professional services (e.g. supporting governance, compliance and regulation)	Helping companies understand cyber security standards, governance and reporting tools

CASE STUDY

Research Institute in Trustworthy Industrial Control Systems (RITICS)

RITICS is a partnership of five universities led by Imperial College London, working with the University of Birmingham, Queen's University Belfast, City University London and Lancaster University.

They work together on a range of issues affecting the security of industrial control systems and CNI: from assessing the physical harm that can arise from cyber threats, to analysing and communicating risk, to developing novel mitigations for cyber threats.

RITICS is already working with partners from across the world, including the US, Japan and the Middle East, and will continue to increase its collaboration with industry and academia.

Queen's University, Belfast

The UK offer to buyers worldwide

The UK has an established, expert and innovative cyber security sector made up of companies across a full range of capabilities.

The sector is growing, with forecasts showing exports rising to £2.6 billion by 2021.

Cyber security is beginning to be considered at board level, but procurement still tends to be led by technical specialists in line with company-specific issues and threats.

This means that broad awareness raising and brand building is unlikely to generate sufficient demand. Focused activity is key to successfully increasing UK cyber security exports.

DIT's new approach targets the needs of buyers based on high-value insight to deliver a tailored experience, supported by the relevant parts of the UK Government.

This curated approach will see large, high-profile buyers with significant budgets targeted with a bespoke UK cyber security offer.

CASE STUDY

Academic Centres of Excellence (ACE)

14 UK universities have been recognised as ACEs in Cyber Security Research by the NCSC and the Engineering and Physical Sciences Research Council.

This scheme aims to:

- Enhance the quality and scale of UK academic cyber security research and postgraduate training.
- Make it easier for potential users of research to identify the best UK cyber security research and postgraduate training.
- Help to develop a shared vision and aims among the UK cyber security research community, inside and outside academia.

How DIT will support the strategy: Pursue, Enable, Respond

DIT will support UK companies to seek, find and secure opportunities to export and supply them with updated marketing, market insight and training.

Reputation matters. The UK brand is strong globally. UK firms are trusted and reliable, but buyers need guidance about what products and services to buy from them.

DIT will use the UK's reputation to provide trusted advice to companies and governments, in partnership with the NCSC and the academia sector. Academics will join trade missions to build relationships between the ACEs and universities to create opportunities for UK companies.

DIT offices worldwide will introduce UK cyber security companies to buyers. UK SMEs in particular will also be connected to established market channels and potential partners, including large UK companies and local businesses in-market.

Many SMEs lack experience pitching to buyers. DIT will play a sales coach role helping SMEs prepare for detailed commercial and technical questions asked at pitches.

DIT will work with the devolved administrations to ensure firms from across the UK get the support they need.

Financial support

UK Export Finance is the UK's export credit department, which works to ensure that no viable UK export fails for lack of finance or insurance, while operating at no net cost to the taxpayer.

UKEF helps UK companies:

- win export contracts by providing attractive financing terms to their buyers
- fulfil contracts by supporting working capital loans
- get paid by insuring against buyer default

UKEF can support exports for any size of company and across all sectors, from capital goods to services and intangibles such as intellectual property.

Visit https://www.gov.uk/government/organisations/uk-export-finance or contact the national customer service helpline: +44 (0)20 7271 8010

CASE STUDY

Malvern Cluster

Malvern, Worcestershire, is also known as "Cyber Valley" due to the high concentration of cyber security companies clustered in the area.

QinetiQ in Malvern and the proximity to the NCSC in Cheltenham all add to the cyber supply chain, and many start-ups leverage the commercial value and connectivity by setting up there.

The cluster sits within "Midlands Engine Cyber", a new regional network to promote trade, investment and academic opportunities around the world.

CASE STUDY

BAE Applied Intelligence

After suffering a serious cyber attack, an Asian government department engaged BAE AI to plan, implement and sustain an advanced cyber security operations centre.

Supported by the UK Government, BAE AI assessed the maturity of its current security capability and the risk impacting the department.

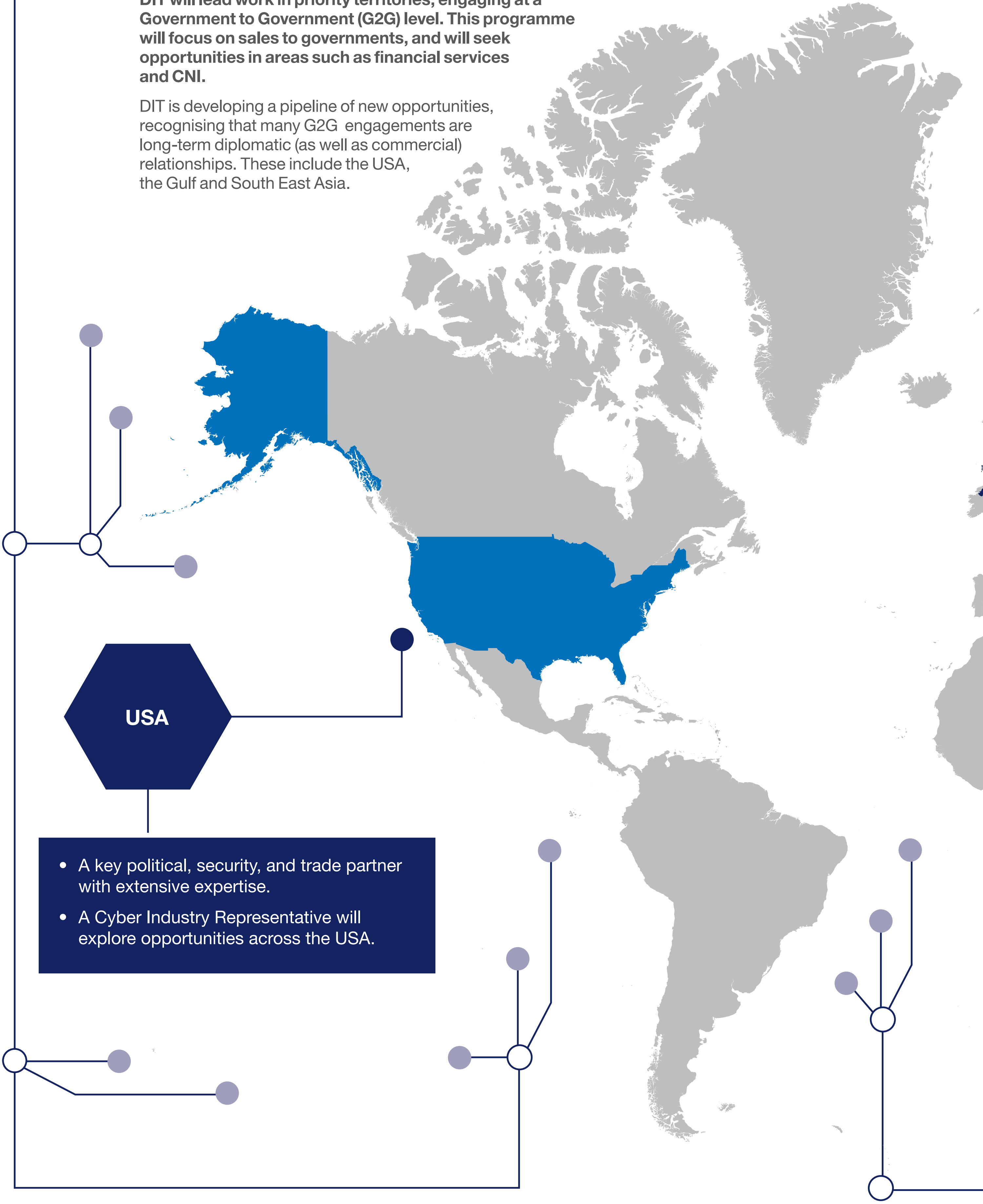
Working with local industrial partners BAE AI implemented a programme delivering advanced cyber defence capabilities.

BAE AI solutions for people, process and technology allowed the government department to rapidly implement advanced cyber defences and to build sustainable sovereign cyber defences.

Pursue

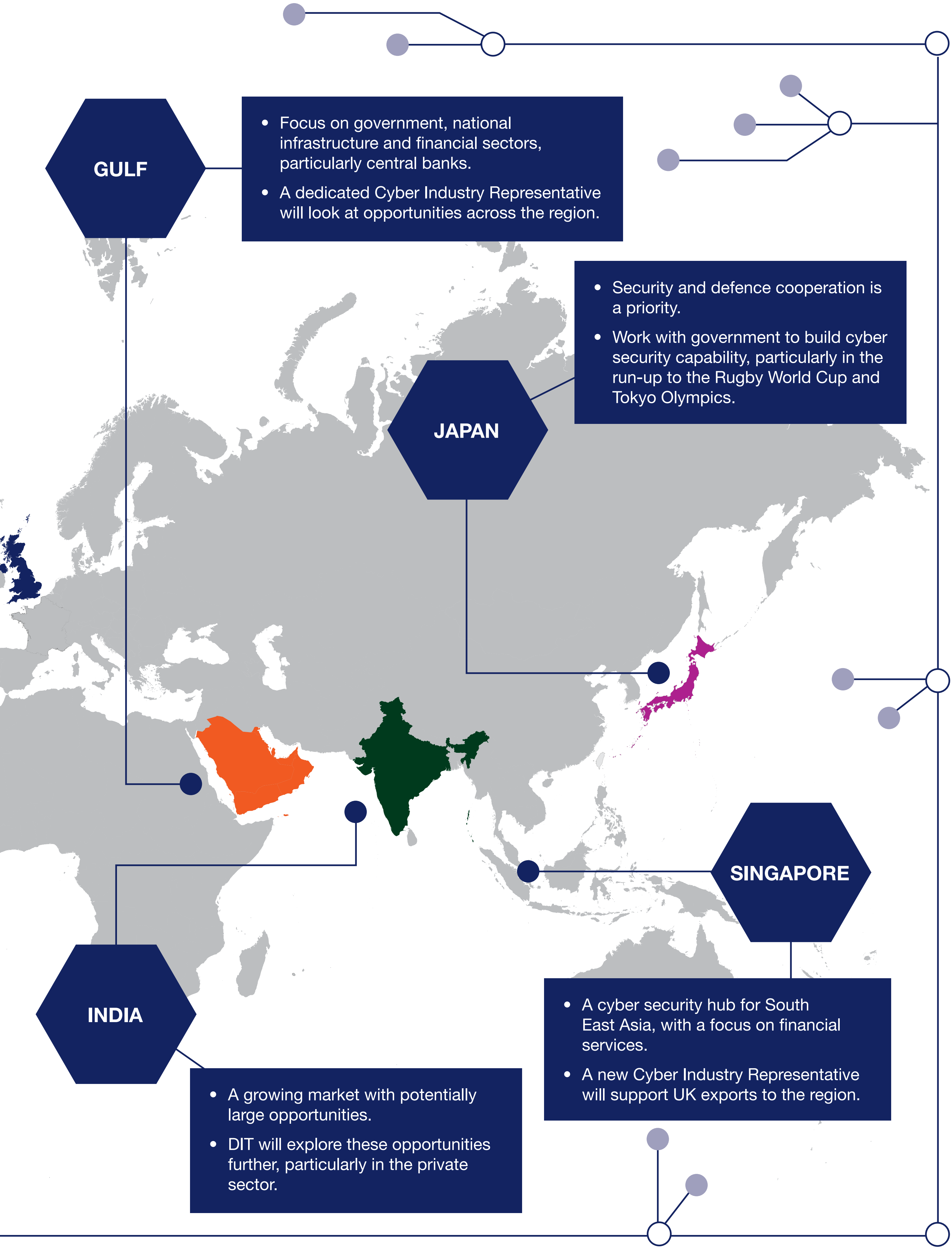
In collaboration with other parts of UK Government, DIT will lead work in priority territories, engaging at a Government to Government (G2G) level. This programme will focus on sales to governments, and will seek opportunities in areas such as financial services and CNI.

DIT is developing a pipeline of new opportunities, recognising that many G2G engagements are long-term diplomatic (as well as commercial) relationships. These include the USA, the Gulf and South East Asia.



USA

- A key political, security, and trade partner with extensive expertise.
- A Cyber Industry Representative will explore opportunities across the USA.



GULF

- Focus on government, national infrastructure and financial sectors, particularly central banks.
- A dedicated Cyber Industry Representative will look at opportunities across the region.

JAPAN

- Security and defence cooperation is a priority.
- Work with government to build cyber security capability, particularly in the run-up to the Rugby World Cup and Tokyo Olympics.

SINGAPORE

- A cyber security hub for South East Asia, with a focus on financial services.
- A new Cyber Industry Representative will support UK exports to the region.

INDIA

- A growing market with potentially large opportunities.
- DIT will explore these opportunities further, particularly in the private sector.

Enable

This strategy identifies the six most promising sectors for cyber security exports worldwide. These sectors are seeing the greatest spend globally and are areas of UK expertise. The strategy targets the largest buyers in each sector with a tailored UK offer. DIT will engage with decision-makers within target companies to build trusted relationships by sharing the UK's insight, experience, and expertise. This will allow the UK to help buyers define their specific cyber security requirements. DIT will create a personalised offer for each buyer, and guide UK companies to help them pitch successfully.

Government

Global 2016
cyber security spend

£27.66bn[9]

Drivers

- Overseas governments' growing awareness of the threats posed by inadequate cyber security.
- Significant increase in the adoption of digital transformation in government and public sector organisations.

Financial Services

Global 2016
cyber security spend

£16.09bn

Drivers

- Technology deployment and consumer trust are vital to the financial services industry and fintech is a growth area.

Automotive

Global 2016
cyber security spend

£0.9bn*

Drivers

- As vehicles get 'smarter', cyber threats are rising due to the vulnerability to hacking of new generation cars.

* Figures calculated as percentage of IT spend, as specific numbers on cyber security spend not available for 2016.

[9] All global cyber security spend figures are from Technavio 2017 – https://www.technavio.com/report/global-it-security-spending-market-2015-2019

The UK Government will engage with overseas governments, particularly Ministers, national technical authorities, and information security stakeholders. This will seek to encourage adoption of standards and position UK companies as best able to meet customer needs.

Energy and Critical National Infrastructure

Global 2016 cyber security spend

£0.77bn*

Drivers

- Digital infrastructure is increasingly ubiquitous, ranging from the emergence of smart grids and smart devices which can make the energy sector more vulnerable to cyber attacks.
- A large number of legacy systems require ongoing maintenance and support to remain secure.

Healthcare

Global 2016 cyber security spend

£4.06bn

Drivers

- Healthcare delivery services and pharmaceutical companies have large quantities of patient data and valuable intellectual property to protect.
- Medical innovations from medical data tracking to bedside life support systems create privacy, safety and security challenges.

Infrastructure

Global 2016 cyber security spend

£0.65bn*

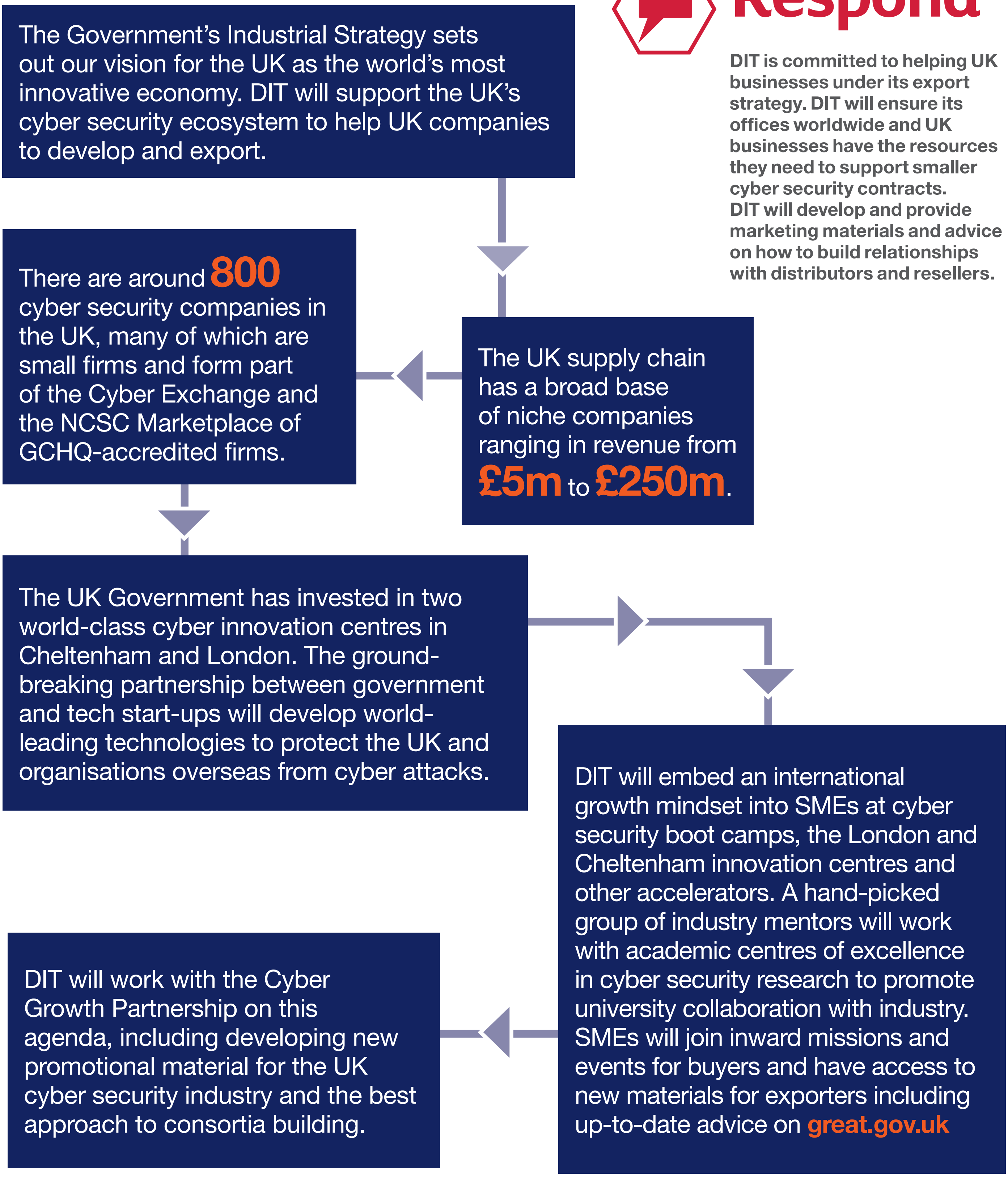
Drivers

- Digital infrastructure is increasingly ubiquitous, ranging from smart ticketing on urban rail to technology-enabled customer journeys through the world's airports.
- There is potential for severe disruption or loss of personal data if these systems are not secured.

Support through the UK cyber security ecosystem

Respond

DIT is committed to helping UK businesses under its export strategy. DIT will ensure its offices worldwide and UK businesses have the resources they need to support smaller cyber security contracts. DIT will develop and provide marketing materials and advice on how to build relationships with distributors and resellers.



The Government's Industrial Strategy sets out our vision for the UK as the world's most innovative economy. DIT will support the UK's cyber security ecosystem to help UK companies to develop and export.

The UK supply chain has a broad base of niche companies ranging in revenue from **£5m** to **£250m**.

There are around **800** cyber security companies in the UK, many of which are small firms and form part of the Cyber Exchange and the NCSC Marketplace of GCHQ-accredited firms.

The UK Government has invested in two world-class cyber innovation centres in Cheltenham and London. The ground-breaking partnership between government and tech start-ups will develop world-leading technologies to protect the UK and organisations overseas from cyber attacks.

DIT will embed an international growth mindset into SMEs at cyber security boot camps, the London and Cheltenham innovation centres and other accelerators. A hand-picked group of industry mentors will work with academic centres of excellence in cyber security research to promote university collaboration with industry. SMEs will join inward missions and events for buyers and have access to new materials for exporters including up-to-date advice on **great.gov.uk**

DIT will work with the Cyber Growth Partnership on this agenda, including developing new promotional material for the UK cyber security industry and the best approach to consortia building.

Export controls, risk assessment and human rights

This strategy takes into account UK Government defence and security export responsibilities. The UK operates one of the most robust export control regimes in the world and risks around human rights abuses are a key part of the assessment process.

The advanced technical nature of cyber security gives cause for some products, software or services to contain export controlled features. DIT's Export Control Joint Unit (ECJU) is the national export licensing body and, supported by NCSC, will advise companies on when a licence may be needed. The licensing process examines each application against the consolidated EU and national arms export licensing criteria. Throughout this process ECJU will be advised by Foreign and Commonwealth Office, Ministry of Defence and NCSC experts to ensure rigorous, well-informed and timely licensing decisions are reached.

The DIT Cyber Security Team and techUK will continue to publish guidance on assessing cyber security export risks, including where products do not reach an export control threshold.

City of London Corporation

"London is the world's leading financial services hub and has cutting-edge cyber security expertise to ensure a resilient and competitive financial sector." *The Rt Hon the Lord Mayor of the City of London.*"

Flight paths, Europe

gov.uk/dit

DIT

The UK's Department for International Trade (DIT) has overall responsibility for promoting UK trade across the world and attracting foreign investment to our economy. We are a specialised government body with responsibility for negotiating international trade policy, supporting business, as well as delivering an outward-looking trade diplomacy strategy.

Legal disclaimer

Whereas every effort has been made to ensure that the information in this document is accurate the Department for International Trade does not accept liability for any errors, omissions or misleading statements, and no warranty is given or responsibility accepted as to the standing of any individual, firm, company or other organisation mentioned.

Any enquiries regarding this publication should be sent to us at enquiries@trade.gov.uk

Published March 2018 by
Department for International Trade.

Image credits:
P 10: Visualisation: ITO World.