UK Trade
& Investment

Cyber Security

The UK's approach to exports

BUSINESS
IS
GREAT
BRITAIN

www.ukti.gov.uk

> “The UK is committed to building a secure, resilient, open and trusted internet. We are working with partners across the globe to ensure this vision becomes a reality.”
>
> Foreign Secretary William Hague
> September 2012

Contents

Establishing a vibrant and secure cyberspace

Cyber security, the protection of networked information systems, has grown rapidly in importance to governments around the world, likewise to national and international commerce. The great opportunities that the internet is providing, in terms of communications, innovation and new freedoms, need to be protected from those who would disrupt and abuse the benefits that we have come to depend upon.

This strategy aims to position the UK as the partner of choice for those seeking cyber security solutions. It sets out the UK's strengths and capabilities in cyber security and describes how the Government will provide immediate and practical support to UK exporters and to overseas customers who have requirements in this area.

In developing this strategy, we recognise the need to create actions and activities that match the relentless pace and scale of the international communications and IT industries. Many of the objectives laid out in this strategy have therefore been designed to foster close collaboration with industry. As readers of this strategy will observe, many activities will need to flex and change in response to the demands of the market – this has led us to identify the need for strong governance, both within Government and in collaboration with industry. These are just some of the challenges that we have addressed in the creation of this strategy and I will be monitoring with keen interest the progress we make as we strive to establish the UK as a global leader in this exciting new sector.

I would like to thank everyone who has contributed to this strategy, especially those private sector organisations who have put a significant amount of effort and time into sharing their ideas and issues with us.

Lord Green
Minister of State for
Trade and Investment

Stephen Green

Introduction

In March 2011, the UK Government published The Plan for Growth,[1] which outlined the urgent need for long-term, sustainable economic growth through a renewed focus on exports.

This was followed in November 2011 by the UK Cyber Security Strategy, which outlined a vision for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace. Objective 1 of the strategy's implementation plan recognised that cyberspace is an important and expanding part of our economy. It set out the approach for tackling cybercrime and making the UK one of the most secure places in the world to do business. One of the supporting actions of this objective was to develop a marketing strategy to promote the capabilities of the UK cyber security industry to international markets.

This paper is the response to that action and provides clarity for all UK Government and UK industry stakeholders, and other interested parties, on the UK's approach to the cyber security export market.

The global cyber security industry has evolved out of the need to protect valuable information systems and networks. It is now estimated to be worth in excess of £100bn per annum[2]. The UK is a strong player in this sector, bringing a variety of capabilities to bear, including technical innovation, a skilled workforce, sound legal and regulatory environments, and the experience gained from the adoption of internet technologies in nearly all parts of the economy. This combination of skills ranks the UK as the world's number-one cyber power in the Economist Intelligence Unit's *Cyber Power Index*[3]. The UK Government is committed to working closely with UK industry to capitalise on this position.

£11.8bn

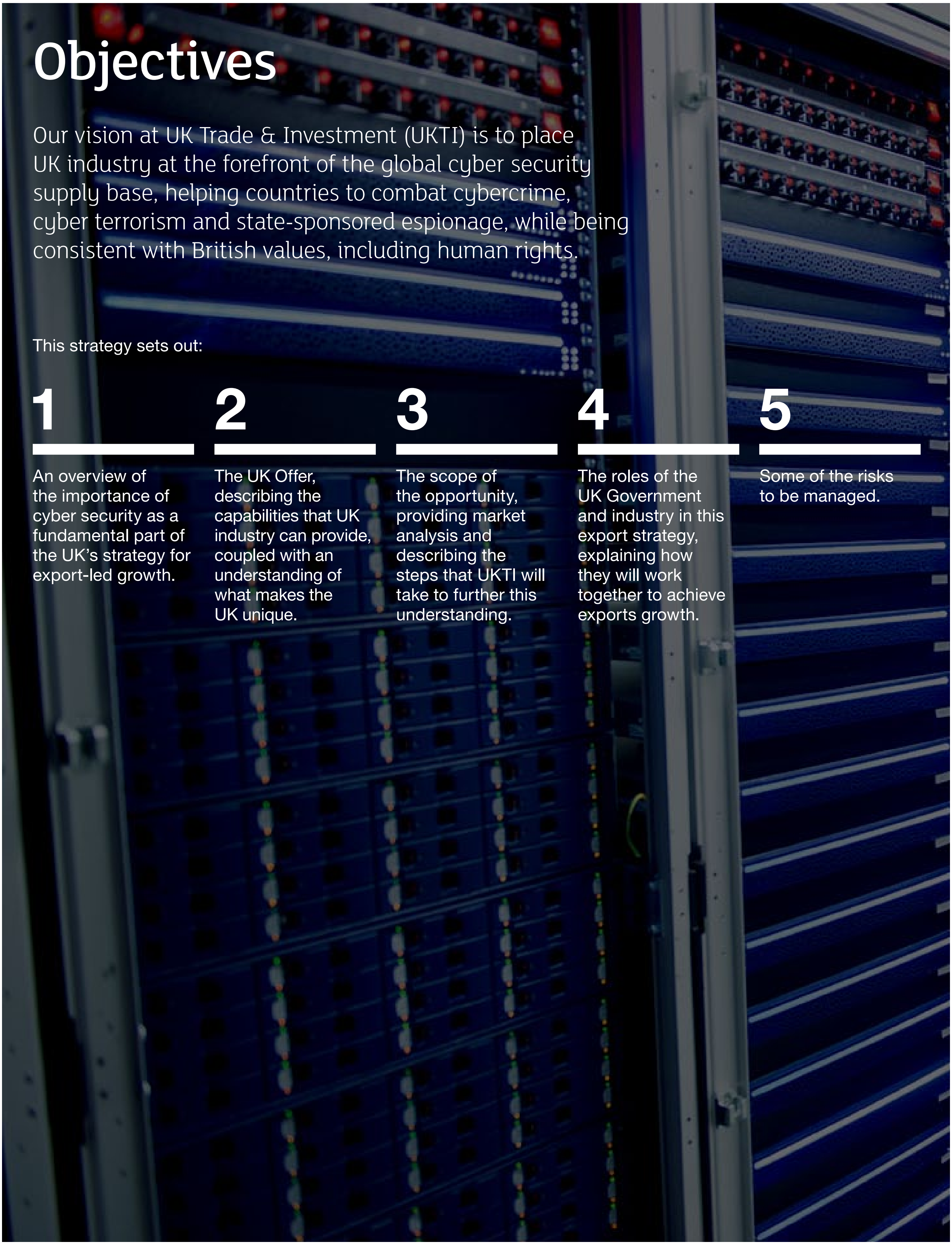
The UK security sector is worth £11.8bn, with a third of sales from cyber security.[4]

[1] *The Plan for Growth*, HM Treasury and Department for Business, Innovation and Skills, March 2011

[2] *UK Security Sector Report for 2011*, KMatrix Report, March 2012

[3] *Cyber Power Index*, an Economist Intelligence Unit research programme sponsored by Booz Allen Hamilton, 2011

[4] *UK Security Sector Report for 2011*, KMatrix Report, March 2012



Objectives

Our vision at UK Trade & Investment (UKTI) is to place UK industry at the forefront of the global cyber security supply base, helping countries to combat cybercrime, cyber terrorism and state-sponsored espionage, while being consistent with British values, including human rights.

This strategy sets out:

1

An overview of the importance of cyber security as a fundamental part of the UK’s strategy for export-led growth.

2

The UK Offer, describing the capabilities that UK industry can provide, coupled with an understanding of what makes the UK unique.

3

The scope of the opportunity, providing market analysis and describing the steps that UKTI will take to further this understanding.

4

The roles of the UK Government and industry in this export strategy, explaining how they will work together to achieve exports growth.

5

Some of the risks to be managed.

The growing importance of cyber security

The birth of the internet has had a profound impact on economies, societies and States. Many industries have undergone radical change, offering new models such as internet banking, online retailing and distance learning.

The use of the internet permeates all aspects of contemporary life and has led to unexpected changes. For example, social media technology has transformed the way that people communicate and share personal information, and has stimulated and enabled huge social and political change in many parts of the world in ways that couldn't have been envisaged just a few years ago.

But there is a growing realisation that these technologies contain vulnerabilities that are being attacked and exploited. And they can be abused in ways which are inimical to our values – for example to deny people their rights to privacy and freedom of expression. As awareness of this problem spreads, the dependence of modern economies and societies on internet technologies has become alarmingly clear. Attackers are growing in skills, scale and determination, making the so-called cyber threat one of the most complex and disruptive threats to security in recent history.

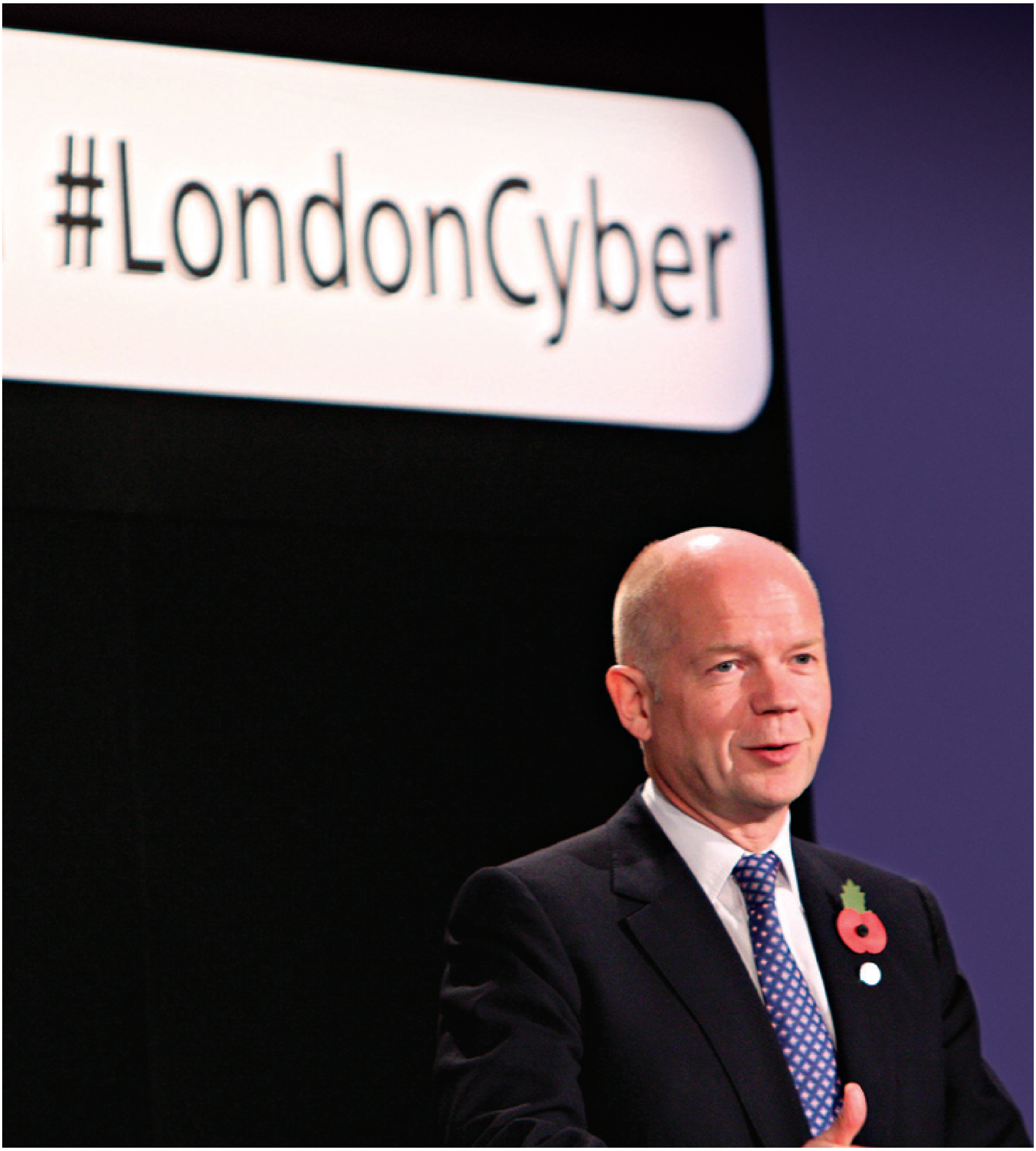
The UK responded early to this emerging threat. In 2010, the UK Government's Strategic Defence and Security Review committed £650m to a National Cyber Security Strategy, establishing the Office of Cyber Security and Information Assurance (OCSIA) within the Cabinet Office to co-ordinate the operational and policy response across Departments, agencies and the private sector.

In 2011, the UK ratified the Budapest Convention (a central plank in the international response to cybercrime) and hosted the first international Conference on Cyberspace in London, stimulating global debate on how to protect the economic and social dividends of cyberspace from growing threats. As a result of these actions, the UK has established a position of leadership in cyber security which can be used to boost the export of UK capabilities.

The London Conference has also shown us how the challenges of cyber security are inter-connected with other cyber policy challenges we face in the international debates about Internet governance, content control and protection of human rights in cyberspace. We need to ally our ambitions for economic growth with our objectives to maintain an open internet that supports rights and freedoms. Rapid innovation, new products and services mean we must learn fast and ensure policy is consistent.

The UK Government is committed to developing new procedures and analysis techniques, working with business and the public to manage risk and uphold the UK's legal obligations and policy commitments, as outlined in the UN Guiding Principles on Business and Human Rights. By working together to secure the safety of cyberspace, we can use the UK's strengths and capabilities to support progress that maintains the UK vision, and delivers growth for the UK economy.

Foreign Secretary William Hague speaking at the Conference on Cyberspace in London



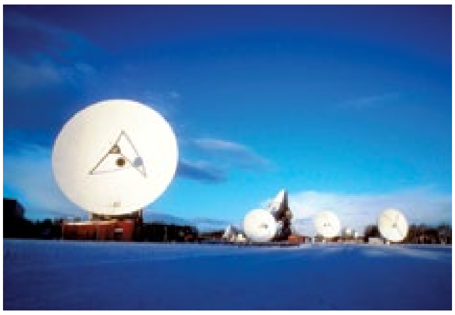
Market definition

Cyber security is the defence of networked computer systems against various forms of attack. These systems may be for use at home or at major commercial or government organisations.

These networked computer systems underpin our banking systems, health services and food supplies, as well as critical national and defence infrastructure. The term 'cyber security' has partly replaced the term 'information assurance' (IA), but it goes further than this to include areas such as 'cyber defence' (principally used by military organisations), protection of telecommunications equipment and the safeguarding of industrial control systems. Different organisations in different countries may attribute slightly different meanings to 'cyber security', some interpreting the term as 'high-end' or military in nature, others taking a broader definition that encompasses all of ICT security. Some flexibility in the term's use is therefore needed.

Figure 1 on page 7 breaks down and defines cyber security[5]. It shows a set of technical capabilities, surrounded by a number of service-based offerings that are used to complement or integrate the core cyber security technologies.

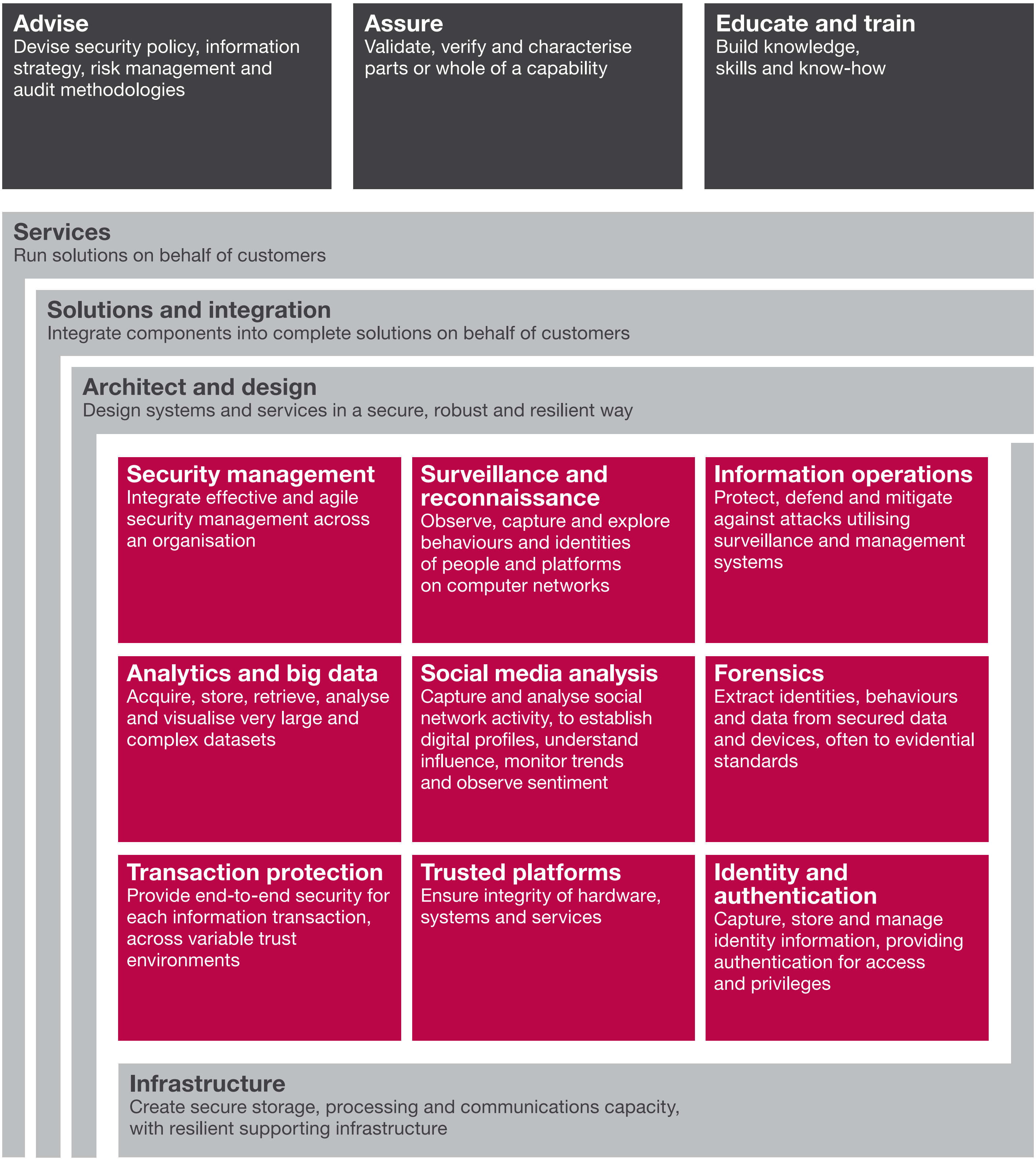
At the core of the model are nine technical groups, ranging from information operations to social media analysis. A number of services exists to support these technologies, including the design of a system, integration of multiple system components and operation of these systems as services. Additional services include advice, assurance and training, which can be applied to the whole or any part of the technical groups.



BT

[5] This model is an elaboration by Andrew Rogoyski of Roke Manor Research using a segmentation developed in the *Deputy Assistant Secretary of Defense for Cyber, Identity, and Information Assurance Strategy*, The Office of the Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer, August 2009. It is a framework for the present and will be updated as the cyber security market matures

Figure 1 Cyber Security Supplier Segmentation



Advise
Devise security policy, information strategy, risk management and audit methodologies

Assure
Validate, verify and characterise parts or whole of a capability

Educate and train
Build knowledge, skills and know-how

Services
Run solutions on behalf of customers

Solutions and integration
Integrate components into complete solutions on behalf of customers

Architect and design
Design systems and services in a secure, robust and resilient way

Security management
Integrate effective and agile security management across an organisation

Surveillance and reconnaissance
Observe, capture and explore behaviours and identities of people and platforms on computer networks

Information operations
Protect, defend and mitigate against attacks utilising surveillance and management systems

Analytics and big data
Acquire, store, retrieve, analyse and visualise very large and complex datasets

Social media analysis
Capture and analyse social network activity, to establish digital profiles, understand influence, monitor trends and observe sentiment

Forensics
Extract identities, behaviours and data from secured data and devices, often to evidential standards

Transaction protection
Provide end-to-end security for each information transaction, across variable trust environments

Trusted platforms
Ensure integrity of hardware, systems and services

Identity and authentication
Capture, store and manage identity information, providing authentication for access and privileges

Infrastructure
Create secure storage, processing and communications capacity, with resilient supporting infrastructure

Market characteristics

Given the relative immaturity of the cyber security market, the scale of global cyber security business is difficult to quantify accurately.

UKTI's research estimates that the global cyber security market was worth £123bn[6] in 2011, with annual growth rates of 10 per cent, positioning cyber security as the fastest-growing segment of the security market. Other more conservative estimates range from £35bn to £51bn[7]. These statistics illustrate some uncertainty in market size, mostly due to what is included in the analysis, but growth rates are consistently estimated to be high, between six per cent and 11 per cent[8].

UKTI estimates the UK cyber security market in 2011 was worth approximately £3.9bn[9], with over 2,000 companies operating in the sector. The UK Government's National Cyber Security Programme, with a budget of £650m over four years has added significantly to this spend, creating a focus on the subject in several Government Departments. In terms of total national spend on cyber security the UK is one of the leading cyber security nations in the world.

Sophos

UK exports of cyber security products and services were £805m in 2011, approximately one-third of all UK security exports. The US is the largest market, taking 31 per cent of the UK's cyber security exports, followed by China at 19 per cent, then Japan at 10 per cent[10]. Other rapidly growing markets such as India, which already represents nine per cent of UK cyber security exports, are proving to be increasingly attractive.

£123bn

The total global cyber security sector is worth £123bn.

[6] *UK Security Sector Report for 2011*, KMatrix Report, March 2012

[7] Global Industry Analysts: £51bn, Marketsandmarkets: $64bn, PWC: Global Market: $60bn, Visiongain: $61bn

[8] Marketresearchmedia: CAGR: 6.2%, Marketsandmarkets: CAGR: 11.3%, PWC: CAGR: 10%

[9] *UK Security Sector Report for 2011*, KMatrix Report, March 2012

[10] *UK Security Sector Report for 2011*, KMatrix Report, March 2012

Market drivers

Many factors drive the increased global interest in cyber security, including:

- a growing recognition that international businesses now depend on secure and resilient internet communications to build supply chains and reach new markets;
- an increased awareness of highly sophisticated state-sponsored attacks, which aim primarily for economic advantage by theft of intellectual property and sensitive market information[11,12];
- an improving awareness that information is a strategic asset that needs to be protected in accordance with its importance and value to the organisation;
- a rising concern that critical national infrastructure, including energy, utilities and transport is vulnerable to cyber attacks;
- an increase in 'hacktivist' activities aimed at propagating a political agenda by disrupting services or exposing sensitive information;
- a rising awareness of the importance of internet communications, such as social media, to support freedom of expression and political engagement, on an international basis;
- an increasing uptake in mobile technologies, which in some parts of the world are the main way to connect to the internet, resulting in economic growth, improving skills, education and financial systems with an associated reduction in corruption and anti-competitive practices;
- a rapidly increasing volume of software exploits – viruses, Trojans and worms – with thousands of new variants being detected every day; and
- an increase in large-scale cyber fraud.

UK companies that can address these issues will find business growth in overseas markets.

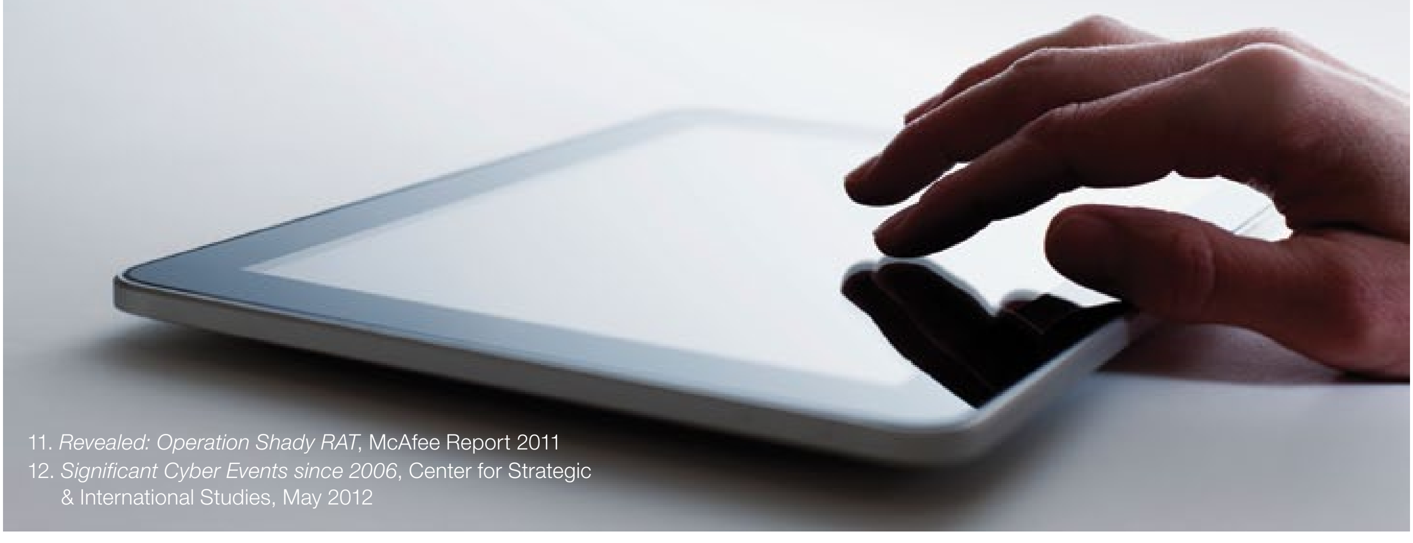
Market analysis

To help the UK Government and industry understand and prioritise the potential export markets, UKTI has started a campaign of market analysis.

We have drawn upon information from our overseas Posts, the Home Office, BIS, the Cabinet Office and other Government Departments. Brazil, India, the Gulf States and South East Asia will be the initial areas of focus as there is great potential for growth of cyber security exports.

The analysis will include:

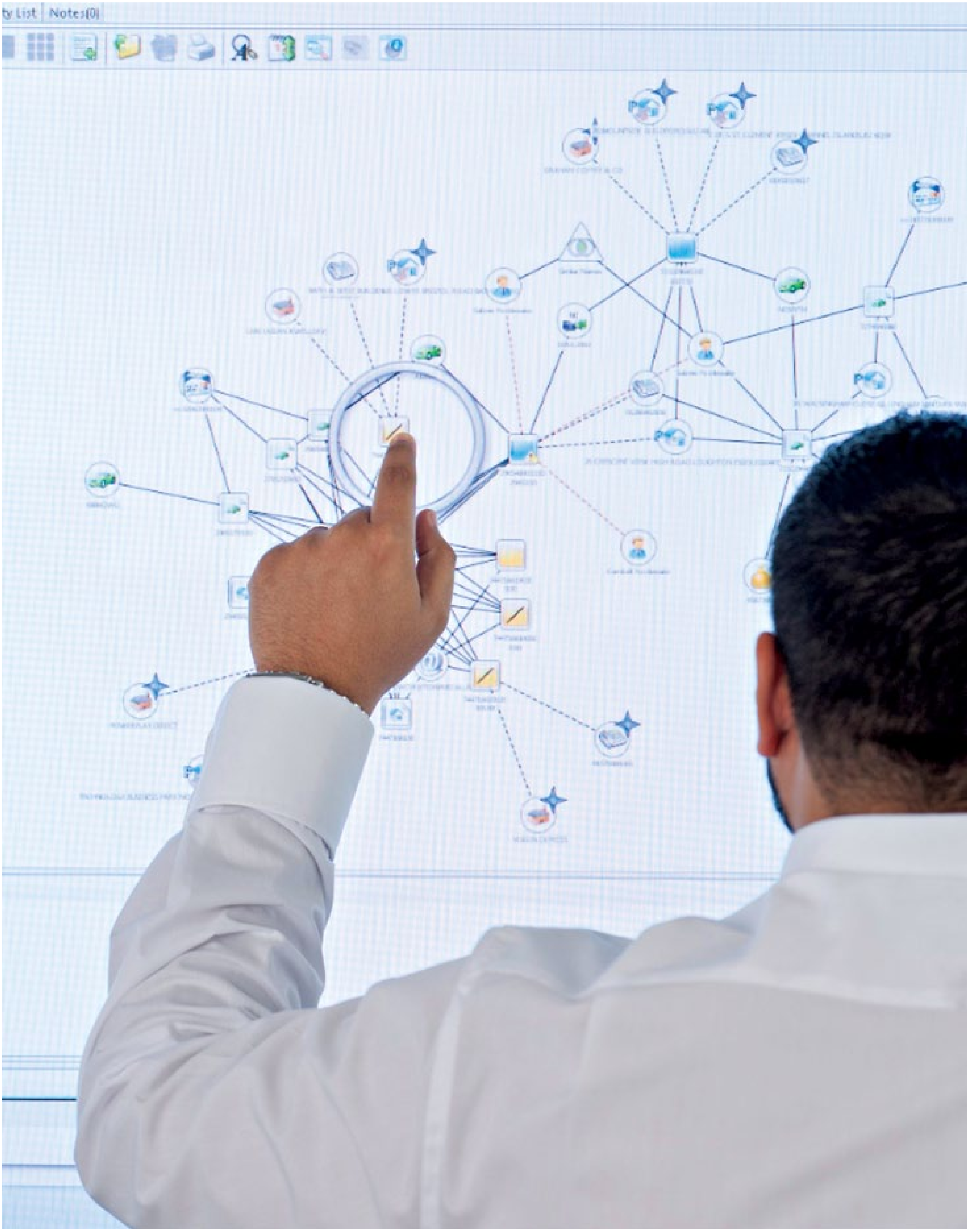
- up-to-date information on the market opportunities;
- local and regional drivers and priorities;
- specific high value or high-importance projects; and
- an assessment of the export risks posed by each market.



[11] *Revealed: Operation Shady RAT*, McAfee Report 2011

[12] *Significant Cyber Events since 2006*, Center for Strategic & International Studies, May 2012

BAE Systems Detica



The UK Offer

The UK Offer and the UK Government's role within it will vary, depending on the customer and the requirement; an export to a government organisation may require a very different approach from a business-to-business sale.

Many countries regard the UK as a preferred and trusted partner for cyber security. Our strength in cyber security stems from hosting some of the best defence and security innovators in the world in both the public and private sector, such as the internationally recognised Government Communications Headquarters (GCHQ). The UK Offer combines capability and know-how sourced from both the UK Government and UK industry experts.

The UK approach to building cyber security capability is crucial to our offer. In the UK, we understand that countries have diverse requirements that depend on the nature of the problems they face. One country may be concerned over protection of infrastructure, another over their banking industry. Countries have different maturity levels in cyber security, needing different levels of support from the UK.

Solutions may range from the provision of education services through to major facilities build. The UK's business culture is focused on listening to customer needs and responding innovatively, flexibly and quickly. The UK Government recognises its role in this process, enabling discussion and negotiation, exploring requirements and advising on best practice and solutions. UKTI is working across all departments to make available experts to help shape these discussions, whether advising or providing Government-backed services.

UK industry has particular capability strengths to offer the global cyber security market, including:

- network surveillance and analysis, including deep packet inspection and analytics, in support of network management, malware detection, anomaly detection (including data exfiltration) and the detection and mitigation of network attacks (eg denial of service attacks). UK industry can meet these demands with products and services, including several advanced security operations centres;
- advisory and assurance services (secure systems architectures, policy, audit and penetration testing services), including access to world-class schemes for the accreditation of products, services and people under the auspices of CESG[13];
- security endpoint technologies, including antivirus and firewall systems;
- social media analytics, including toolsets for data analytics;
- mobile device and infrastructure security, including LTE/4G, for network protection and law-enforcement purposes;
- world-class providers of high-end encryption technologies;
- a strong technology industry that has an established track record for creating innovative security solutions, including highly developed service providers, systems integrators, SMEs and specialists;
- excellence in education and research, including long-term research undertaken in the UK's eight designated University Cyber Centres of Excellence (see opposite); and
- specialist training applications and services (including the use of cyber ranges), behavioural analysis and risk management.

To improve awareness of the UK's key technological skills in cyber security, **UKTI will work with UK industry to build a detailed catalogue of UK cyber security suppliers, using a new products and services model. A core script will also be developed for the UK Government and industry use**.

To capitalise on the UK's key research and development capabilities, **UKTI will work with BIS and UK innovators in cyber security**, including UK academia, industry research labs, SMEs and government research groups. **We will promote leading research into selected overseas markets** and facilitate collaboration opportunities in cyber security.

Our universities

Announced in April 2012, eight UK universities were designated University Cyber Centres of Excellence. They are: the University of Bristol, Imperial College London, Lancaster University, the University of Oxford, Queen's University Belfast, Royal Holloway University of London, the University of Southampton and UCL (University College London).

They have been awarded 'Academic Centre of Excellence in Cyber Security Research' status by GCHQ in partnership with the Research Councils' Global Uncertainties Programme and BIS.

[13] CESG – the UK Government's National Technical Authority for Information Assurance

BAE Systems Detica

The UK Offer is enhanced by the UK's broader strengths relevant to cyber security, which include:

- a mature understanding of the nature of cyber security problems and their potential solutions;
- a sophisticated engagement between industry and the UK Government that enables a pan-economy collaboration against cyber threats through technology and information exchange;
- a world-leading set of institutions (eg CESG and the British Standards Institution (BSI)) that define and develop technical and professional standards that apply to cyber security;
- a strong academic base with mature links to UK industry;
- the recently announced Government initiative to build skills and resources in key international partners to counter cyber threats and cybercrime;
- a rich set of user sectors, including media, pharmaceuticals, oil exploration, retail and financial services, as well as defence and security, who understand and can advise on how security has become an enabler for their businesses;
- a strong consultancy base that can advise on security policy, practice and benefits, as well as providing security audit and assurance services;
- a highly reputable forensics industry, providing products and services to evidential standards;
- a group of world-leading infrastructure companies, from architects and programme management advisers to communications service providers;
- a legislative environment that is highly respected globally and that helps to make the UK a good place to do business – both for inward investment and export; and
- a set of expert legislative and regulatory advisers who can help drive the right behaviours within the public and private sector, including respect for human rights and the rule of law.

Export opportunities

Scope

UKTI will seek to prioritise export opportunities in areas where UK companies are likely to be most successful. Examples of business opportunities that are likely to play to the UK industry's strengths include:

- the provision of cyber security services that protect Government, commercial organisations and citizens from sophisticated and targeted attack;
- large-scale ICT systems or services that have a significant cyber security element, regardless of purpose;
- the creation of new and large-scale financial service systems, including settlement systems and financial trading systems;
- the creation of research capabilities, ranging from university education and research programmes, to dedicated cyber security facilities;
- the creation of sophisticated government intelligence-gathering systems;
- the creation of a major new communications infrastructure, including fixed-line fibre/cable infrastructure, broadcast or mobile telephony;
- the creation of new transport infrastructure, including ports, railways and airports; and
- the creation of new energy generation and distribution infrastructure, especially that which includes smart metering.

Ultra Electronics Ltd

The opportunity to provide UK cyber security capability is therefore often embedded in other major programmes and infrastructure builds, highlighting the need to avoid being too narrow when considering the scope of a cyber security opportunity, and to relate cyber security exports to the UK's wider security exports (e.g. designing out crime and counter construction fraud). A specific example of this is UKTI's current work on the concept of Smart Cities, Smart Living, which concentrates on sectors such as the built environment, education, energy and the environment, health, digital and transport.

£805m

Cyber security exports total some £805m, 33% of UK security exports.

Priority markets

UKTI will initially focus on cyber opportunities in the Gulf States, Brazil, India and Malaysia, working closely across the UK Government and industry to develop market campaigns. These are high-growth markets for security exports where there is also a political desire to engage with the UK. We will continue to monitor opportunities and extant requirements in other markets – primarily established cyber security export markets where the UK already has a presence, such as the US, China and Japan. The following paragraphs give an indication of the current emerging export opportunities.

The Gulf States

The UK Government's Gulf Initiative, launched in 2010, recognised that the region is critically important to the UK's security and prosperity objectives. It is a region where Government-to-Government relationships can create strong links that benefit the positioning of UK industry. All countries in this region have expressed a strong interest in the development of cyber security and have the economic strength to build formidable capabilities. Some of them already possess highly sophisticated technology industries, that will both provide local competition to UK companies and opportunities for partnerships.

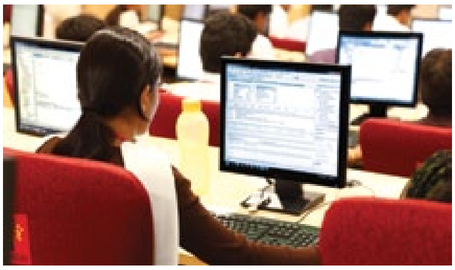
UKTI is tracking some 14 High Value Opportunities (HVOs) over the Gulf region, ranging from major transport infrastructure builds to programmes for the construction of new hospitals, many of which will have cyber security requirements. The US, France and Germany remain the UK's key competitors.

Kuwait: the Kuwaitis are undertaking a number of ambitious investment programmes, including the Kuwait Metro System, several new hospitals and the redevelopment of Kuwait Airport. All of these projects will have a requirement for cyber security.

Qatar: the Qatari government is investing in a comprehensive infrastructure programme in preparation for the FIFA World Cup in 2022. Security and fraud prevention measures are expected to figure strongly. As events of this magnitude increasingly become targets for cyber criminals and 'hacktivists', they require sophisticated cyber security protection to ensure they are successfully delivered.

UAE: the UAE is investing heavily in a variety of long-term programmes to build the high-tech industries that the country will depend on in the future. These include a civil nuclear programme with a significant investment profile, the Etihad Rail Project and the creation of the Khalifa Industrial Zone. Other projects include a new National Air Traffic Management Centre, the UAE Biobank and the UAE Vehicle Engineering and Test Centre. A significant proportion of the estimated security spend over the next three years will be in cyber security, including support for the newly established National Electronic Security Authority.

Saudi Arabia: current Saudi programmes likely to involve substantial cyber security elements include the Saudi Railway Development Programme, the Sadara Petrochemical Complex and the Healthcare Development Programme, comprising 138 hospitals and 12 new medical cities.



Latin America

Brazil: just over a third of all Brazilians now access the internet – the highest proportion of any emerging economy and the fourth-largest number of users in the world. By 2016, this proportion is expected to rise to half of the population. As with the UK, the number of mobile phones in use in Brazil exceeds its population, ranking fourth in the world.

Brazil is hosting a number of international events, including the Rio 2016 Olympic and Paralympic Games, with infrastructure builds including 12 sports stadia with 12 command and control centres, and airport, port and transport developments. The UK's recent success hosting the London 2012 Olympics offers a unique platform to promote capabilities, particularly as the UK has specific experience of delivering cyber security during the Games (including responding to Games-targeted attacks). Brazil is starting to invest in cyber security, recognising that there are significant cybercrime activities.

East and South East Asia

India: India is another large market for internet technologies, with 100 million internet subscribers in 2010, with mobile internet traffic having already passed desktop traffic in early 2012[14].

Sales of smartphones are expected to continue rising at 55 per cent per annum for the next five years, making India one of the fastest-growing markets for mobile telecommunications.

The Indian government is keen to provide online access to government services such as education, health and financial services. It is making a substantial investment in IT infrastructure, including laying fibre-optic communications to some 600,000 villages as part of the ambitious Indian National e-Governance Plan, placing further demand on imports of telecommunications equipment, already exceeding £6bn annually.

Indian interest in the global fight against cybercrime is growing and a recent report on engagement with the private sector recommended the creation of information sharing and analysis centres in various industry verticals, bringing together the private sector with sectoral Computer Emergency Response Teams (CERTs).

Malaysia: in 1997, CyberSecurity Malaysia was established as the country's national cyber security specialist agency under the Ministry of Science, Technology and Innovation. It is an example of Malaysia's leadership in this area, alongside the country's participation in the Asia Pacific CERT. Malaysia has put in place a strong response to cybercrime, creating the DiGi CyberSAFE Programme and the special task force to curb money laundering, income tax and customs fraud. Malaysia is also investing in the development of skills and the creation of academic links such as the Cyber Security Academy, a collaboration between CyberSecurity Malaysia and Kebangsaan University.

Other regional export opportunities

Parts of Asia, such as Indonesia, and South Korea, as well as parts of Africa, are experiencing substantial economic growth and investing in large-scale communications infrastructure. Countries such as South Africa, Nigeria, Egypt and Libya, are making significant investments in cyber security.

UKTI will continue to support mature and established markets such as the US, Canada, New Zealand, Australia, Japan, China, France, Germany, the Netherlands and the Nordics. These markets are the most likely to be open to specific niche technical capabilities from UK suppliers as well as the UK's broader expertise in cyber security. This incorporates education and skills, policy and regulation.

UKTI will also consider campaigns targeted at non-geographical groupings, based on similarity of requirements or interdependencies between the customers, for example NATO, EU and UN requirements. We will also consider a campaign to identify the opportunities and requirements of major financial services centres, matching UK capability to the joint requirements of the world's financial hubs such as New York, Tokyo, Hong Kong, Singapore, Shanghai, Paris and Frankfurt.

[14] Source: Forbes April 2012

Engaging with Government

The key outcome for this export strategy is to achieve greater engagement between the UK Government, the UK industry supplier base and overseas customers, whether they are led by government or industry.

The following paragraphs in this section describe how this will be achieved and outline specific stakeholder responsibilities.

Stakeholder co-ordination

UKTI will co-ordinate the UK Government response to export opportunities, managing the government stakeholder community.

A new cross-departmental group will be created to do this, and when appropriate will include representatives from UK industry. The group will **provide guidance, set priorities, consider the risks to be managed, co-ordinate resources and monitor progress against implementation of this strategy**.

2,380

The UK has an estimated 2,380 companies in cyber security.[14]

Stakeholder responsibilities

There are a number of stakeholders required to support the delivery of cyber security export growth:

UKTI DSO

UKTI DSO provides the lead in export initiatives, building relationships with potential export customers and working with UK industry to develop campaigns to target potential export customers.

Department for Business, Innovation and Skills (BIS)

The newly formed Cyber Growth Partnership, co-chaired by the BIS Minister for Universities and Skills, will help develop the UK Offer, capturing strengths and areas of innovation, as well as address barriers to growth of the UK cyber security sector. BIS will also continue to develop strategic relationships with companies of all sizes in the cyber security sector, and encourage the development of industry-led cyber security clusters in support of growth. In addition, BIS has responsibility for export control issues.

Foreign & Commonwealth Office

The FCO will broker high-level Government-to-Government relationships, supporting relationship-building events in Embassies and High Commissions.

Office of Cyber Security and Information Assurance (OCSIA)

OCSIA will provide strategic assistance across Departments, developing policy, strategy and insight on cyber security.

GCHQ

GCHQ will engage with overseas government customers as appropriate. Its information assurance arm, CESG, will support recognised supplier/assurance schemes and provide expert advice to UKTI. CESG is also the technical adviser to BIS on export controls relating to cyber security.

Ministry of Defence

MOD will employ its wide network of Defence Attaches and existing bilateral engagement programmes to provide support and credibility for export opportunities.

Home Office

The Home Office will help to broker and deliver Government-to-Government relationships and agreements which may often include cyber security requirements.

Trade Associations (Intellect, ADS and others, including industrial groupings such as RISC)

UKTI will communicate and market-test the strategy and detailed marketing initiatives with the trade bodies, including the further development of the UK Offer. UKTI will also offer to provide leadership on events such as Cyber Security Seminars.

Industry

UKTI will engage with the UK cyber security supply base, including specialists and SMEs, to co-operate on specific overseas opportunities and to facilitate introductions to overseas customers.

GCHQ, Cheltenham

15. *UK Security Sector Report for 2011*, KMatrix Report, March 2012

Government-to-Government engagement

Government must provide the leadership, facilitate the relationships and open the channels for industry to pursue global opportunities, some of which will be delivered on a business-to-business basis, but some of which will benefit from Government to Government participation.

UKTI, in conjunction with other Government stakeholders, will develop Government-to-Government relationships to pursue cyber security opportunities.

There is growing interest from several potential overseas customers in formal Government-to-Government mechanisms to provide cyber security advice and assistance, and work is underway across the UK Government to develop appropriate models of engagement and to manage and mitigate risks.

Business-to-business support

UKTI will help UK industry by organising, co-ordinating and supporting other services to facilitate business-to-business engagement, including:

- **Inward visits –** inward visits to the UK by overseas governments will generally follow Government-to-Government discussions. These will provide opportunities to promote UK industry capability, perhaps involving a mini exhibition or visits to UK facilities. Inward visits may also arise as a result of trade association or industry activities, requesting assistance from the UK Government as necessary.
- **Exhibitions –** exhibitions are the traditional method of assistance offered by UKTI. Overseas or UK exhibitions are a key vehicle to showcase UK products and services. Our key role is to position UK suppliers attractively to overseas delegations, with support from exhibition organisers.
- **Meet the Buyer Events** – organised by UKTI, often in conjunction with a trade association, the aim of these events is to facilitate introductions between UK companies and overseas buyers (government or industry). The events can be organised as part of our presence at an exhibition or as a standalone activity.
- **Seminars –** Cyber Security Seminars can be an effective method of follow-up once the initial Government-to-Government relationship has been established and there is further interest in potential UK solutions. The objectives of such seminars will include building the government relationship; promoting the UK Offer; and creating engagement between customers and suppliers. They will often take place in the target country to attract maximum attendance of key decision makers.
- **Business clusters –** UKTI will support BIS to develop cyber security industry 'clusters' of UK and overseas companies of all sizes working alongside academic institutions, with the main aim of finding industry-led solutions to common problems. Cluster activities could result in business partnerships being formed that might lead to trade and investment opportunities.

Much of the onus will be on UKTI and FCO staff overseas to identify opportunities, initiatives and risks.

UKTI will provide briefings to Posts to understand the cyber market, the UK Offer and to match UK capabilities to local requirements.

Export advice

UKTI will continue routinely to provide help and advice for UK businesses intending to grow in international markets. With a presence in over 100 countries, we can help in a variety of ways, including participation in trade fairs, outward missions and the provision of bespoke market intelligence.

UKTI will ensure that companies with interests and capabilities related to cyber security will be made aware of this strategy and its associated activities. We recognise that advice may need to be tailored to the company, especially the large community of UK SMEs that may be able to contribute to this market.

Export controls

UKTI will guide companies to seek advice from BIS on export controls for cyber security, acting as a conduit for discussions that may need to take place with a variety of Government Departments.

Traditional defence export controls do not always readily apply to cyber security systems. Complex issues such as dual use and the inclusion of export-controlled components within commercial systems need to be understood and addressed. Although traditional export controls do not always apply to cyber security, there are many that do. As an example, an export should not be facilitated when there is a clear risk that it might be used to violate human rights, have a negative impact on the preservation of regional peace and security, or that it may affect the UK's own national security.

In this context, the UK Government expects UK companies to conduct due diligence as to these export risks. All exports should support UK policy, respect human rights, manage risk and follow any statutory procedures. The UK Government is preparing fresh guidance on this issue.

Inward investment

Although this strategy is principally focused on the export of UK capability, **UKTI will encourage inward investment for cyber security opportunities**, bringing foreign businesses and organisations to the UK to create or use cyber security capabilities hosted in the UK and delivered to the country of interest.

Multinational organisations can, in essence, choose to site any part of their business in any location in the world, taking advantage of the most attractive business environment to meet the company's needs.

Considerations such as law, tax, skilled workforce, political stability and government incentives all play a part in a company's decision to site elements of their business in a particular country. The UK is an excellent location for many businesses, particularly if the security of data and people is a primary concern.

31%

The US is the top destination for UK cyber exports at 31%, followed by China (19%), Japan (10%) and India (9%).

Conclusion

This strategy has described the clear opportunities that exist for the UK to provide cyber security capabilities to a worldwide market.

Although not the largest, the UK represents one of the most advanced nations in its use of its digital infrastructure and in its protection. The UK's strength lies in the close engagement between the UK Government and its supply base, its innovative technology and security industry, its skilled workforce, its sound legal and regulatory environment and its high adoption of internet technologies across the UK economy. To exploit these opportunities and implement this strategy, UKTI will work with all stakeholders to address the actions.

UKTI will monitor progress against the delivery of actions, reporting quarterly to the cross-departmental group on achievements made. This strategy will be reviewed annually and updated to reflect the current export environment.

Cyber Security Export Strategy – Actions for 2013

UKTI will carry out a market analysis of the global opportunities for cyber security. This will initially focus on Brazil, the Gulf, Malaysia and India

UKTI will work with UK industry to build a detailed catalogue of cyber security suppliers, using a newly developed model of products and services

UKTI will work with BIS and UK innovators in cyber to promote UK-leading cyber security research into selected overseas markets

UKTI will develop a core script for the UK Government and industry use

UKTI will create a new cross-departmental group to provide guidance on the implementation of this strategy, set priorities and co-ordinate resources

UKTI will develop Government-to-Government relationships to pursue cyber security opportunities

UKTI will help UK industry by organising, co-ordinating and supporting other services to facilitate business-to-business engagement

UKTI will train Posts to understand the cyber market and the UK Offer and to match UK capabilities to local requirements

UKTI will ensure that companies with interests and capabilities related to cyber security will be made aware of this strategy and its associated activities

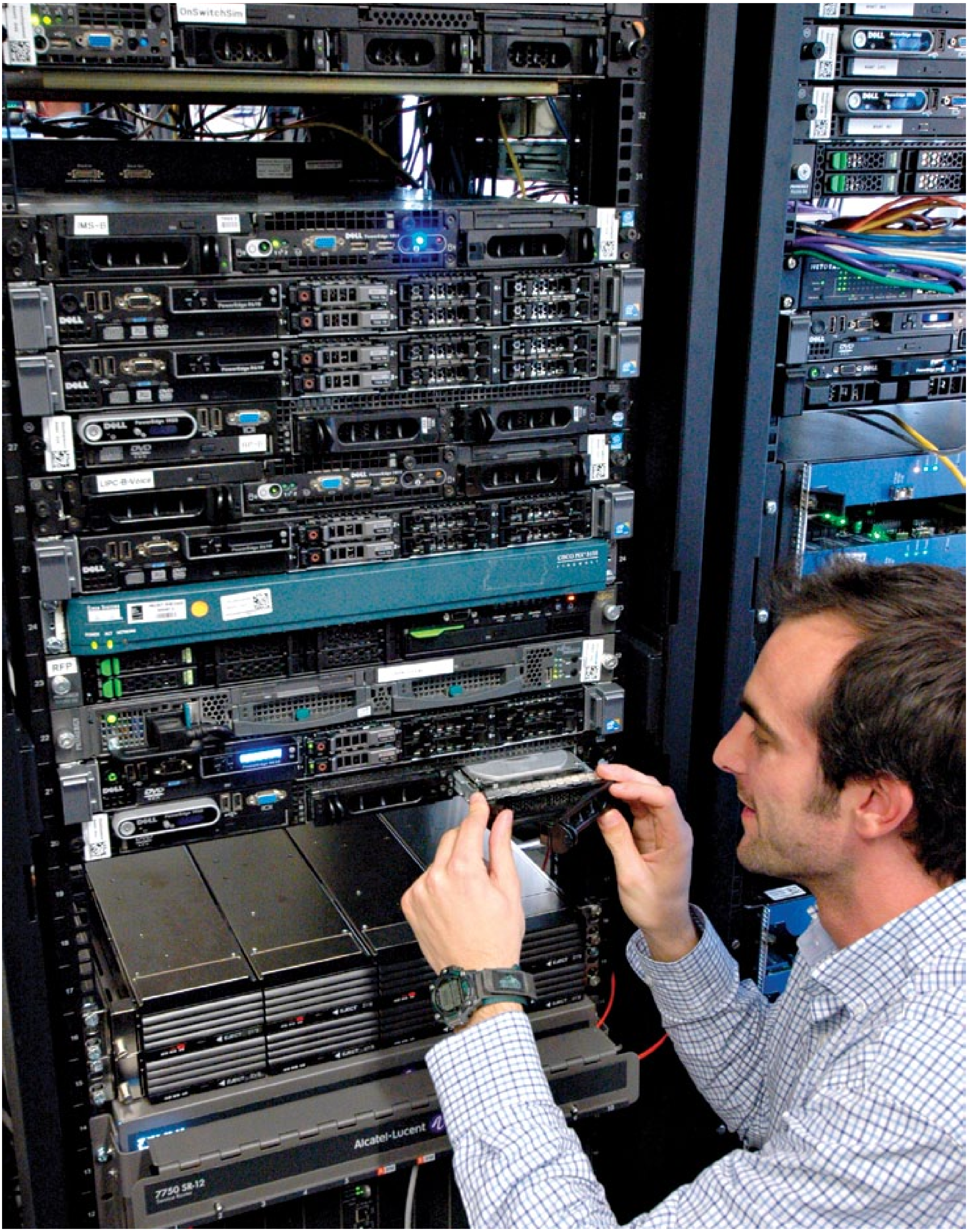
UKTI will guide companies to seek advice from BIS on export controls for cyber security

UKTI will encourage inward investment for cyber security opportunities

For more information contact us at:
cyber@ukti.gsi.gov.uk

Image credits
Front cover Getty Images, inside front cover iStock, p.2 Getty Images, p.3 iStock, p.4-5 Foreign & Commonwealth Office, p.6 Brian Lawrence/Getty Images, BT, p.8 Sophos, p.9 iStock, p.10 BAE Systems Detica, p.12 BAE Systems Detica, p.13 Ultra Electronics, p.16 MOD images Crown Copyright, inside back cover Roke Manor Research.

Roke Manor Research Ltd



To find out more, scan this code with your smartphone.
www.ukti.gov.uk
+44 (0)20 7215 5000

Solutions for Business
Funded by UK Government

UK Trade & Investment is the Government Department that helps UK-based companies succeed in the global economy. We also help overseas companies bring their high-quality investment to the UK's dynamic economy, acknowledged as Europe's best place from which to succeed in global business.

UK Trade & Investment offers expertise and contacts through its extensive network of specialists in the UK, and in British embassies and other diplomatic offices around the world. We provide companies with the tools they require to be competitive on the world stage.

UK Trade & Investment is responsible for the delivery of the Solutions for Business product "Helping Your Business Grow Internationally". These "solutions" are available to qualifying businesses, and cover everything from investment and grants through to specialist advice, collaborations and partnerships.

Copyright

Any enquiries regarding this document should be emailed to us at:
enquiries@ukti.gsi.gov.uk
Or you can call:
+44 (0)20 7215 5000

This document is also available at:
www.ukti.gov.uk

Whereas every effort has been made to ensure that the information given in this document is accurate, neither UK Trade & Investment nor its parent Departments (the Department for Business, Innovation and Skills, and the Foreign & Commonwealth Office) 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.

Published April 2013
by UK Trade & Investment
© Crown Copyright
URN 13/720