The UK Cyber Security Strategy

Protecting and promoting the UK in a digital world

November 2011

Contents

Introduction by the Rt Hon Francis Maude MP, Minister for the Cabinet Office

The growth of the internet has been the biggest social and technological change of my lifetime. It is a massive force for good in the world in the way it drives growth, reduces barriers to trade, and allows people across the world to communicate and co-operate. As we saw this spring in the Arab world, it can help give the unheard a voice and hold governments to account. It will have a huge role to play in supporting sustainable development in poorer countries.

At the same time our increasing dependence on cyberspace has brought new risks, risks that key data and systems on which we now rely can be compromised or damaged, in ways that are hard to detect or defend against.

The UK Government takes these risks seriously. That is why the 2010 National Security Strategy rated cyber attacks as a 'Tier 1' threat and why, despite a tight fiscal situation, we set £650 million aside over four years to develop our response.

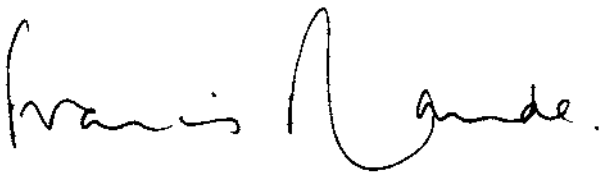
We are determined to tackle the threats, but in a way which balances security with respect for privacy and fundamental rights. At home and internationally the UK Government will continue to work to ensure that cyberspace remains an open space – open to innovation and the free flow of ideas, information and expression.

This strategy sets out the actions we will take to reduce the risk and secure the benefits of a trusted digital environment for businesses and individuals:

- If you are in business this strategy sets out what we will do to help ensure protection of your company; to promote the UK as a good place to do business online; and to foster opportunities for UK cyber security firms to leverage strength at home to sell their products overseas.
- If you are an individual concerned about your own personal security from crime, fraud and identity theft this strategy outlines what we will do to tackle these threats and ensure you have the support needed to protect yourself.

In a domain where technology and change are fast-moving, responding effectively will require a consistent and extensive effort. By 2015, the aspiration is that the measures outlined in this strategy will mean the UK is in a position where: law enforcement is tackling cyber criminals; citizens know what to do to protect themselves; effective cyber security is seen as a positive for UK business; a thriving cyber security sector has been established; public services online are secure and resilient; and the threats to our national infrastructure and national security have been confronted.

We will report back next year on progress; in the meantime I would welcome your feedback on this strategy and the plan it sets out. Please send your comments care of the Office of Cyber Security and Information Assurance in the Cabinet Office (ocsia@cabinet-office.x.gsi.gov.uk).



The Rt Hon Francis Maude MP
Minister for the Cabinet Office and Paymaster General

Executive summary

The internet is revolutionising our society by driving economic growth and giving people new ways to connect and co-operate with one another. Falling costs mean accessing the internet will become cheaper and easier, allowing more people in the UK and around the world to use it, 'democratising' the use of technology and feeding the flow of innovation and productivity. This will drive the expansion of cyberspace further and as it grows, so will the value of using it. Chapter 1 describes the background to the growth of the networked world and the immense social and economic benefits it is unlocking.

As with most change, increasing our reliance on cyberspace brings new opportunities but also new threats. While cyberspace fosters open markets and open societies, this very openness can also make us more vulnerable to those – criminals, hackers, foreign intelligence services – who want to harm us by compromising or damaging our critical data and systems. Chapter 2 describes these threats. The impacts are already being felt and will grow as our reliance on cyberspace grows.

The networks on which we now rely for our daily lives transcend organisational and national boundaries. Events in cyberspace can happen at immense speed, outstripping traditional responses (for example, the exploitation of cyberspace can mean crimes such as fraud can be committed remotely, and on an industrial scale). Although we have ways of managing risks in cyberspace, they do not match this complex and dynamic environment. So we need a new and transformative programme to improve our game domestically, as well as continuing to work with other countries on an international response.

Chapter 3 sets out where we want to end up – with the Government's vision for UK cyber security in 2015.

Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

To achieve this vision by 2015 we want:

Objective 1:

The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace

Objective 2:

The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace

Objective 3:

The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies

Objective 4:

The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

That means a UK where:

- Individuals know how to protect themselves from crime online.
- Businesses are aware of the threats they face, their own vulnerabilities and are working with Government, trade associations, and business partners to tackle them. We want to see UK companies building on our strengths to create a thriving and vibrant market in cyber security services around the world. In the current economic climate the UK needs more than ever to identify and exploit areas of international competitive strength to drive growth. We believe that being able to show the UK is a safe place to do business in cyberspace can be one such strength.
- Government has: sharpened the law enforcement response to cyber crime; helped the UK take opportunities to provide the cyber security services that will be needed across the world; encouraged business to operate securely in cyberspace; bolstered defences in our critical national infrastructure against cyber attack; strengthened our capabilities to detect and defeat attacks in cyberspace; enhanced education and skills; and established and strengthened working relationships with other countries, business and organisations around the world to help shape an open and vibrant cyberspace that supports strong societies here and across the globe.

To achieve this we have set aside £650 million of public funding for a four-year, National Cyber Security Programme. Chapter 4 sets out what

Government will do, in partnership with the private sector and other countries, to deliver the vision.

As part of this action plan Government will:

- Continue to build up in GCHQ and MOD our sovereign UK capability to detect and defeat high-end threats.
- Pursue the agenda defined at the recent London Conference on Cyberspace to establish internationally-agreed 'rules of the road' on the use of cyberspace.
- Work with the companies that own and manage our critical infrastructure to ensure key data and systems continue to be safe and resilient.
- Establish a new operational partnership with the private sector to share information on threats in cyberspace.
- Encourage industry-led standards and guidance that are readily used and understood, and that help companies who are good at security make that a selling point.
- Help consumers and small firms navigate the market by encouraging the development of clear indicators of good cyber security products.
- Hold a strategic summit with professional business services, including insurers, auditors, and lawyers to determine the role they might play in promoting the better management of cyber risks.
- Bring together existing specialist law enforcement capability on cyber crime into the new National Crime Agency (NCA). Encourage the use of 'cyber-specials' to make more use of those with specialist skills to help the police.
- Build an effective and easy-to-use single point for reporting cyber fraud and improve the police response at a local level for those who are victims of cyber crime.
- Work with other countries to make sure that we can co-operate on cross-border law enforcement and deny safe havens to cyber criminals.
- Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for online offences.
- Seek agreement with Internet Service Providers (ISPs) on the support they might offer to internet users to help them identify, address, and protect themselves from malicious activity on their systems.
- Help consumers respond to the cyber threats that will be the 'new normal' by using social media to warn people about scams or other online threats.
- Encourage, support, and develop education at all levels, crucial key skills and R&D.
- Build a single authoritative point of advice for the public and small businesses to help them stay safe online.
- Foster a vibrant and innovative cyber security sector in the UK, including exploring new partnerships between GCHQ and business to capitalise on unique Government expertise.

Because of its links to intelligence and national security, some of the activity the Government has set in train is necessarily classified. The full range of unclassified actions is set out in Annex A.

1. Cyberspace: Driving growth and strengthening society in the UK and around the world

A networked world...

1.1 The internet and digital technologies are transforming our society by driving economic growth, connecting people and providing new ways to communicate and co-operate with one another. The World Wide Web only began in 1991, but today 2 billion people are online[1] – almost a third of the world's population. Billions more are set to join them over the next decade. There are over 5 billion internet-connected devices.[2] $8 trillion changed hands last year in online commerce.[3]

1.2 The internet is already having a profound impact on the way we live our lives. This social change will only grow and gather pace as the number of users increases. Already it looks like it will be on the scale of the very biggest shifts in human history, such as the coming of the railways, or even learning to smelt metals.

Real GDP per capita has risen by $500 over the last 15 years in mature countries enabled by the internet. By comparison, it took 50 years for the industrial revolution to have the same effect.

McKinsey Global Institute, Internet Matters, 2011

...which feeds growth....

1.3 It is easy to see why the growth of the internet has been so dramatic. Cyberspace is transforming business, making it more efficient and effective. It is opening up markets, allowing commerce to take place at lower cost and enabling people to do business on the move. It has promoted fresh thinking, innovative business models and new sources of growth. It enables companies to provide better, cheaper and more convenient service to customers. And it helps individuals to shop around, compare prices and find what they want.

Cyberspace is an interactive domain made up of digital networks that is used to store, modify and communicate information. It includes the internet, but also the other information systems that support our businesses, infrastructure and services. Digital networks already underpin the supply of electricity and water to our homes, help organise the delivery of food and other goods to shops, and act as an essential tool for businesses across the UK. And their reach is increasing as we connect our TVs, games consoles, and even domestic appliances.

1.4 Developing countries in particular stand to benefit as increasing interconnectivity makes commerce easier and allows access to information, knowledge and education, enabling people to innovate, collaborate and compete in global marketplaces.

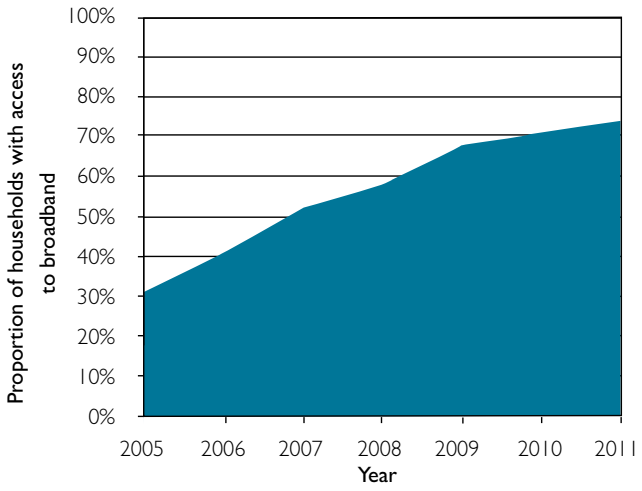
Some 52% of UK consumers with access to broadband use online shopping as an opportunity to save money.

Ofcom, *Communications Market Report*, 2010

1.5 The UK has positively adopted cyberspace as a means of doing business. In 2009, 608 million card payments were made online, with a total spend of £47.2 billion,[4] and in 2011 around 74% of UK

homes had access to broadband, as shown in the graph below (this compares to an EU average of 60.8% in 2010[5]).

Take-up of broadband in the UK, 2005–11



Source: Ofcom

1.6 Recent research suggests that the internet contributes an average of 3.4% of GDP in a range of developed countries[6]. In the UK, the internet accounts for around 6% of GDP: if it were a sector in itself it would be larger than either utilities or agriculture.

1.7 The same research shows that the internet has also played a vital role in driving prosperity, accounting for 21% of GDP *growth* in the last five years in 'mature' countries. Often, small businesses and traditional industries draw the biggest benefits. This study also shows that overall moving trade online has resulted in gains: for every job lost, 2.6 jobs have been created.

1.8 As it has developed, cyberspace has enabled the automation and optimisation of the infrastructure that supports many businesses; for example, the SCADA[7] systems that automatically control and regulate industrial processes such as manufacturing, water distribution, refining and power generation.

1.9 Cost savings for governments resulting from using online services instead of telephone or face-to-face services are substantial.

The creation of a common ICT infrastructure for Government will save £460 million in 2014/15.

Government ICT strategic implementation plan 2011

Universal Credit will provide support to around 19 million citizens across 8.5 million households, and will include provision of online access to benefit-related services and information. Online delivery and greater automation of processes will contribute towards £500 million savings in costs, per year, once Universal Credit is fully operational.

Department for Work and Pensions

... supports open, strong societies...

1.10 Cyberspace also strengthens open societies. It acts as a vast repository for many forms of knowledge. It allows individuals to connect with one another, share ideas and express views, and take new approaches to shared problems. It provides new and more effective ways to participate, allowing larger numbers of people to solve problems, support each other and get involved in the issues they care about. As more people connect to the internet the flow of new and innovative ideas increases. With a reach that continues to expand, cyberspace is becoming 'democratised' and can now enable social change. It is now being used to empower people by making governments more transparent, accountable[8] and efficient in the way they provide public services.[9]

93% of children aged 12-15 now use the internet at home. This group are more likely to say they would miss the internet than television.

Ofcom, *Children and Parents: Media use report 2011*

...and which will continue to grow

1.11 Since the 1970s, we have witnessed remarkable transformational change that has helped drive the growth of cyberspace. The amount of information created or replicated using

digital technology continues to grow. In 2010 it was estimated to be 1.2 zetabytes and by 2011 it is predicted to grow to 1.8 zetabytes[10] (enough information to fill 380 billion DVDs). A zetabyte is a staggeringly large number – a *billion* terabytes – where a terabyte is typically the largest hard disk available for home computers in 2011.

1.12 But in many ways the most exciting developments in cyberspace are still to come. As more people and organisations around the world connect, it becomes more and more useful in a variety of new and often unexpected ways. The introduction of cloud computing and smart-grids, the continued growth of mobile working and the growth in the number of users of cyberspace each demonstrate that the pace of change will not let up: cyberspace will become increasingly valuable and important to the UK, and to countries across the world.

2. Changing threats

2.1 The internet will become increasingly central to our economy and our society. But the growing role of cyberspace has also opened up new threats as well as new opportunities – we have no choice but to find ways to confront and overcome these threats if the UK is to flourish in an increasingly competitive and globalised world.

2.2 The digital architecture on which we now rely was built to be efficient and interoperable. When the internet first started to grow, security was less of a consideration. However, as we put more of our lives online, this matters more and more. People want to be confident that the networks that support our national security, our economic prosperity, and our own private lives as individuals are safe and resilient.

2.3 Unfortunately a growing number of adversaries are looking to use cyberspace to steal, compromise or destroy critical data. The scale of our dependence means that our prosperity, our key infrastructure, our places of work and our homes can all be affected. For this reason the Government's 2010 National Security Strategy identified cyber attacks on the UK as a 'Tier 1' threat – that is, as one of our highest priorities for action.

What are the threats?

2.4 **Criminals** from all corners of the globe are already exploiting the internet to target the UK in a variety of ways. There are crimes that only exist in the digital world, in particular those that target the integrity of computer networks and online services. But cyberspace is also being used as a platform for committing crimes such as fraud, and on an industrial scale. Identity theft and fraud online now dwarf their offline equivalents. The internet has provided new opportunities for those who seek to exploit children and the vulnerable. Cyberspace allows criminals to target the UK from other jurisdictions across the world, making it harder to enforce the law. As businesses and government services move more of their operations online, the scope of potential targets will continue to grow.

2.5 Some of the most sophisticated threats to the UK in cyberspace come from other **states** which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial and economic assets, as well as monitoring opponents of their own regimes. 'Patriotic' hackers can act upon states' behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home.

2.6 Cyberspace is already used by **terrorists** to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While terrorists can be expected to continue to favour high-profile physical attacks, the threat that they might also use cyberspace to facilitate or to mount attacks against the UK is growing. We judge that it will continue to do so, especially if terrorists believe that our national infrastructure may be vulnerable (the recently published CONTEST[11] strategy sets out our approach to terrorism).

2.7 The threat to the UK from politically-motivated activist groups operating in cyberspace is real. Attacks on public and private sector websites and online services in the UK orchestrated by **'hacktivists'** are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity.

2.8 All these different groups – criminals, terrorists, foreign intelligence services and militaries – are active today against the UK's interests in cyberspace. But with the borderless and anonymous nature of the internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred.

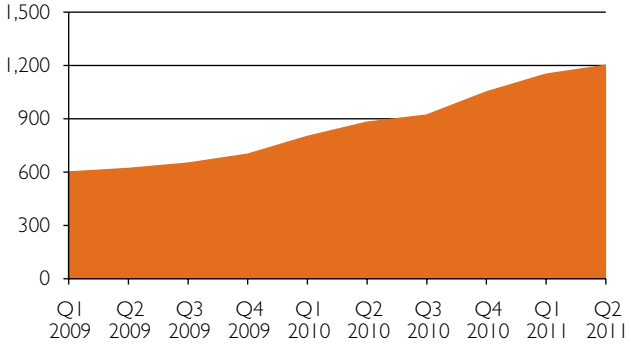
Affecting businesses

2.9 Organisations are not always aware of the new vulnerabilities that dependence on cyberspace can bring. Intellectual property and other commercially sensitive information (for example, business strategies) can be attractive targets. This risks undermining the strengths of the UK's research base and intellectual property as important drivers of growth. Services relying on, or delivered via, cyberspace can be taken offline by criminals or others, damaging revenue and reputations.

In the spring of 2011, Sony announced that criminals had successfully targeted the PlayStation network, compromising the personal details of up to 100 million customers and resulting in the network shutting down for several weeks. The costs to Sony are expected to total $171 million.

2.10 As the digital connections between organisations and individuals proliferate (for example through shared or sub-contracted services), incidents can affect larger numbers of individuals and organisations. Recent research suggests that the costs to the UK of cyber crime could be in the order of £27 billion per year[12]. A truly robust estimate will probably never be established, but it is clear the costs are high and rising. Cyber criminals have demonstrated their ability to adjust quickly to new developments like smart-phones (see graph above). The collective impact of this threat now has the potential to cause significant damage to online economies.

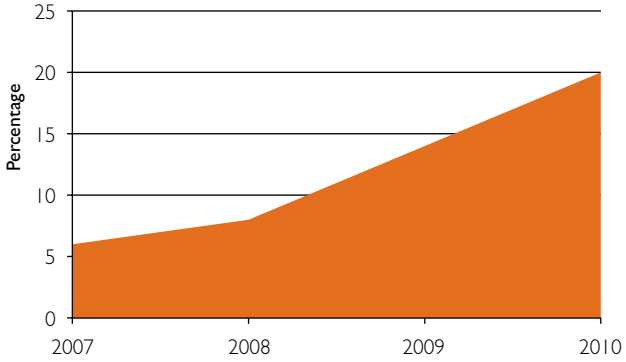
Total number of malware variants targeting smart phones



Source: data from McAfee, as cited in *The Economist, October 2011.*

2.11 The chart below demonstrates the growing impact of information security incidents on businesses worldwide. Maintaining confidence in e-commerce as a viable way of doing business is crucial. Investors, businesses, government and particularly customers each need to be confident that networks are safe to use if the UK is to realise its full potential for growth.

Proportion of companies reporting security incidents with financial impact



Source: *Pricewaterhouse Coopers. Global state of information security survey, 2011*

2.12 But staying secure in cyberspace can seem complex, difficult and expensive. Without a clear and shared understanding of the nature and scale of threats and vulnerabilities, the case for investing in protection and prevention can be undermined.

Affecting our security

2.13 Cyberspace has now grown to become a domain where strategic advantage – industrial or military – can be won or lost. It underpins the complex systems used by commerce (for example, banking, the delivery of food and the provision of utilities such as power and water) and the military. The growing use of cyberspace means that its disruption can affect nations' ability to function effectively in a crisis.

Nearly two-thirds of critical infrastructure companies report regularly finding malware designed to sabotage their systems.

McAfee, Critical infrastructure protection report, March 2011

2.14 Some states regard cyberspace as providing a way to commit hostile acts 'deniably'. Alongside our existing defence and security capabilities, the UK must be capable of protecting our national interests in cyberspace.

"There are over 20,000 malicious emails on government networks each month, 1,000 of which are deliberately targeting them."

Iain Lobban, Director of Government Communications Headquarters, 2010

These kinds of attack are increasing; the number of emails with malicious content detected by government networks in the whole of 2010 was double the number seen in 2009.

Cabinet Office, 2011

Affecting individuals and societies

2.15 In order to get the most from the internet, it is important that people feel confident that it can be used safely. As all of us make more use of the internet in our work and private lives it makes for a more attractive target for criminals or others. Any reduction in trust towards online communications can now cause serious economic and social harm to the UK.

2.16 Beyond the impact on individuals, the scale of the use of cyberspace means that it can now also affect society more broadly. We have a strong tradition in the UK of protecting our citizens in ways that are guided by core values of liberty, fairness, transparency and the rule of law. These values help define who we are, what we do and what it means to be British. The interconnected nature of cyberspace and its expansion mean that it has developed to promote many of these values.

2.17 The conventions and norms covering conduct within the cyber domain are still developing. While this helps make it the vibrant domain that it is today, it can also cause instability and uncertainty about accountability. The blurring of boundaries in cyberspace increases the risk of actions affecting larger numbers of people and organisations unintentionally. At its most serious, this leads to the potential for unpredictable and large-scale shocks.

2.18 Actions to strengthen our national security must also be consistent with our obligations, such as those concerning freedom of expression; the right to seek, receive and impart ideas; and the right to privacy. Defending security should be consistent with our commitment to uphold civil liberties. Of course, these are well-established and ongoing debates, but cyberspace can bring them into focus in new ways, and more quickly than in other areas.

2.19 These changes do not affect the UK alone. We believe that the global reach of the internet and digital technologies can provide an important means for the spread of ideas, with profound implications for societies. But like any communications medium, cyberspace can also potentially be used to restrict liberty and undermine freedoms. Some states and organisations are already seeking to control and restrict the future development of the cyber domain. These attempts are ultimately doomed to fail. But for as long as they last they are holding back progress and reducing social benefit. The UK will continue to work with like-minded states around the world to maximise the extent to which the world can fully realise and enjoy the benefits that cyberspace will offer.

A complex problem

2.20 The growing adoption of the internet and new uses of digitally connected technologies make for a fast moving and complex environment, which brings its own challenges:

- Cyberspace is largely commercially owned and driven, and global in nature.
- The systems that form cyberspace contain a vast array of components, sourced from a global and diverse range of suppliers. Multiple sub-contractors produce, test, package and assemble these components.
- Predicting and understanding how cyberspace will be used in future is difficult given the rate of innovation and change.
- New vulnerabilities and risks will emerge suddenly.
- The pace of events can make existing defences and responses look slow and inadequate. Along with the complexity of cyberspace, this makes attributing hostile actions difficult.
- The covert nature of the threat means that the public and businesses can underestimate the risks.

Existing capacity to meet the challenge

2.21 In tackling these problems we are not starting from scratch. The UK is well placed to respond to many of the challenges that cyberspace presents. Our private sector, key government agencies, and academia all have world-leading strengths in cyberspace; we must bring these together to capitalise on the opportunities and get the most for the UK:

- The UK has strong international alliances based on shared values and common interests.
- Our sound domestic legal framework and regulatory environment mean that the UK has the basis to respond to cyber crime and similar threats to the UK. We need to promote a similar environment internationally.
- The UK already has ways to exchange information with the private sector on the risks emerging from cyberspace, and to tackle cyber crime.
- Some of the specific technical and specialist expertise needed to help us achieve our cyber security objectives already exists in the UK.
- In particular GCHQ, the Government's signals intelligence agency, has some world-class skills at its disposal.
- We already have some businesses with strengths in cyber security.
- Information assurance already plays an important role in reducing our vulnerabilities in cyberspace.

2.22 But *government* capacity, though it includes these real strengths, is not sufficient or sufficiently scaled to meet the growing security challenges of the digital age. Although government already provides advice to organisations that run our infrastructure on how to manage the risks in cyberspace, the adoption of this approach needs to be broader. Our current capacity to enforce the law is too distributed, meaning that criminals still regard exploiting cyberspace as a profitable and low-risk option.

2.23 As for *business*, some firms recognise the growing scale and impact of the risks. However, some sectors of the economy, particularly small and medium sized businesses, do not have access to the skills and knowledge to protect themselves online. We need to improve our understanding of the threat across the board and manage it more effectively. This can mean relying upon skills and knowledge, not often found in the same place.

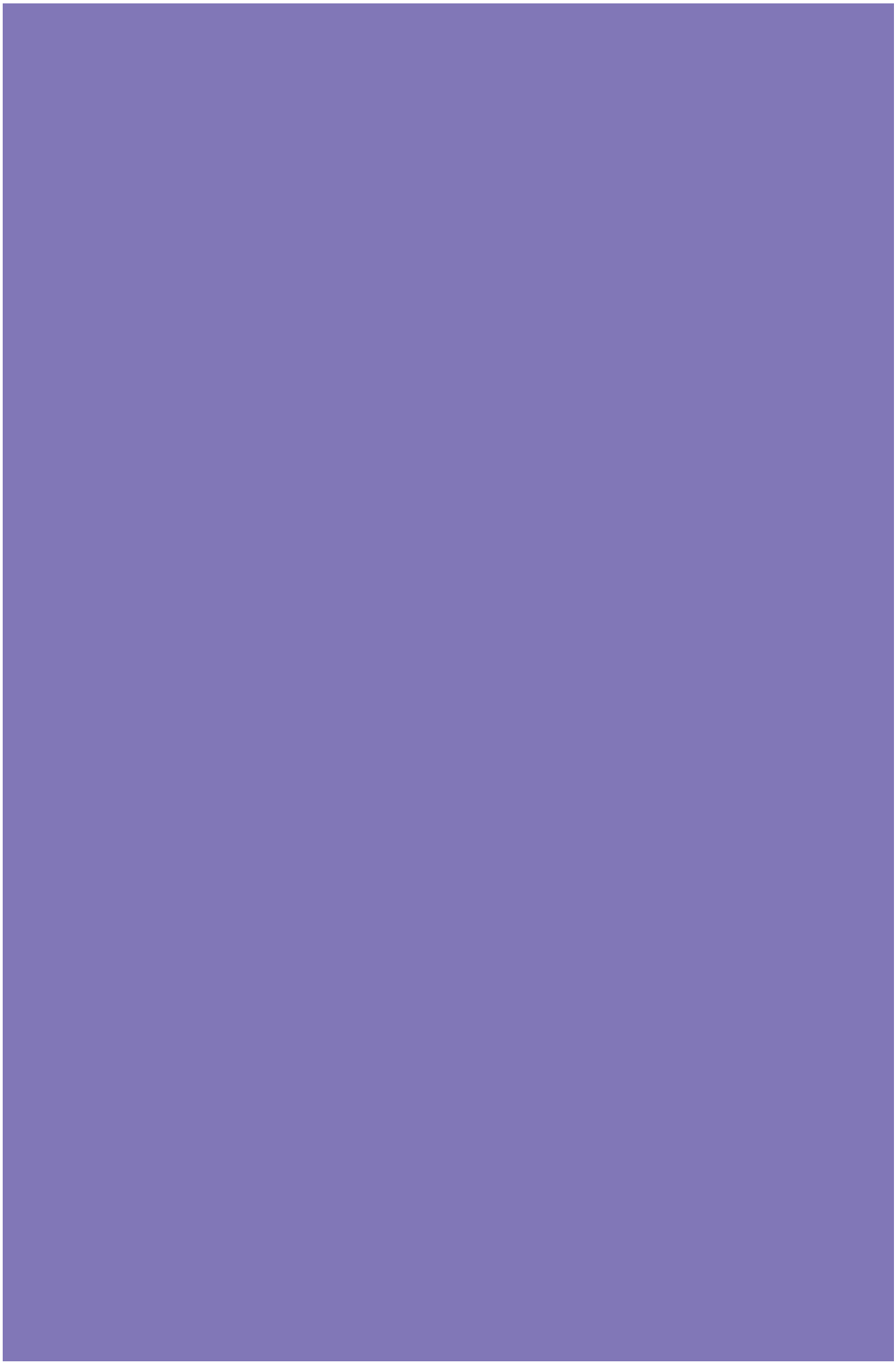
2.24 We also recognise that there are challenges in ensuring that the *public* has access to the information and skills they require in order to understand the threat and take actions to operate safely online. More needs to be done to ensure that the current provision of information is coordinated across Government, and with the private sector.

2.25 We do have a body of internationally agreed principles, behaviour and law which applies to cyberspace. The International Covenant on Civil and Political Rights sets out some of the key obligations. But there remains more to be done

with *other countries* to establish the practical implications of applying existing principles to cyberspace. At a practical level, not all countries have appropriate legislation to allow them to work together to tackle threats from crime in cyberspace.

2.26 The technical capabilities that enable a wide range of actions to protect the UK need strengthening. But it is clear that our approach to the risks in cyberspace must not rely on technical measures alone. Changes in attitudes and behaviours will also be crucial to operating safely in cyberspace.

2.27 It is clear that cyberspace is changing the world. The huge benefit that this brings also means new vulnerabilities. This dynamic and changing profile of risk demands a new approach.



3. A vision for UK cyber security in 2015

3.1 In order to secure the vast economic and social benefits that cyberspace will offer the UK we will transform our approach to cyber security. This section sets out our vision for the UK in 2015 and identifies the principles that will shape our work. The next chapter shows how we will use our existing strengths and the new National Cyber Security Programme to achieve our goals.

Our vision

Our vision is for the UK in 2015 to derive huge economic and social value from a vibrant, resilient and secure cyberspace, where our actions, guided by our core values of liberty, fairness, transparency and the rule of law, enhance prosperity, national security and a strong society.

Our objectives

Our objectives are for:

Objective 1:

The UK to tackle cyber crime and be one of the most secure places in the world to do business in cyberspace

Objective 2:

The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace

Objective 3:

The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies

Objective 4:

The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber security objectives

Our principles:

A risk-based approach....

3.2 In a globalised world where all networked systems are potentially vulnerable and where cyber attacks are difficult to detect, there can be no such thing as absolute security. We will therefore apply a risk-based approach to prioritising our response.

....working in partnership...

3.3 Though the scale of the challenge requires strong national leadership, Government cannot act alone. It must recognise the limits of its competence in cyberspace. Much of the infrastructure we need to protect is owned and operated by the private sector. The expertise and innovation required to keep pace with the threat will be business-driven.

3.4 Similarly, though we can improve our defences domestically, the internet is fundamentally transnational. Threats are cross-border. Not all the infrastructure on which we rely is UK-based. So the UK cannot make all the progress it needs to on its own. We will seek partnership with other countries that share our views, and reach out where we can to those who do not.

... balancing security with freedom and privacy

3.5 At home we will pursue cyber security policies that enhance individual and collective security while preserving UK citizens' right to privacy and other fundamental values and freedoms.

3.6 Internationally the UK will continue to pursue the development of norms of acceptable behaviour in cyberspace. We start from the belief that behaviour which is unacceptable offline should also be unacceptable online. Our position will be guided by the principles proposed by the Foreign Secretary in February 2011 and reiterated at the London Conference on Cyberspace this November:

- The need for governments to act proportionately in cyberspace and in accordance with national and international law.
- The need for everyone to have the ability – in terms of skills, technology, confidence and opportunity – to access cyberspace.
- The need for users of cyberspace to show tolerance and respect for diversity of language, culture and ideas.
- The need to ensure that cyberspace remains open to innovation and the free flow of ideas, information and expression.
- The need to respect individual rights of privacy and to provide proper protection to intellectual property.
- The need for us all to work collectively to tackle the threat from criminals acting online.
- The promotion of a competitive environment which ensures a fair return on investment in network, services and content.

Roles and responsibilities

3.7 Achieving this vision will require everybody, the private sector, individuals and government to work together. Just as we all benefit from the use of cyberspace, so we all have a responsibility to help protect it.

Individuals

3.8 Ordinary people have an important role to play in keeping cyberspace as a safe place to do business and live our lives. By 2015 we want a UK where:

- People know how to get themselves a basic level of protection against threats online. They have access to accurate and up to date information on the online threats that they face, and the techniques and practices they can employ to guard against them.
- Individuals are careful about putting personal or sensitive information on the internet; are wary of email attachments or links from unrecognised senders; and are cautious about downloading files from websites they know little about.
- Everyone, at home and at work, can help identify threats in cyberspace and report them – for example, identifying fraudulent websites.
- Individuals play their part in transacting safely with businesses and Government, protecting passwords, understanding the importance

of updating software and operating systems regularly and running anti-malware programs to help prevent their computers being used by others to increase the threat.

- People are clear that, as in the offline world, we are each responsible for our behaviour in cyberspace (including those who harass others, commit crime or 'hack' into systems for publicity or to cause disruption).

The private sector

3.9 The private sector has a crucial role to play in the UK's cyber security. Much of cyberspace is owned and used by private companies. It is businesses that will drive the innovation required to keep pace with security challenges. By 2015 we want a UK where:

- Companies are aware of the threat and use cyberspace in a way that protects commercially sensitive information, intellectual property and customer data.
- Private organisations work in partnerships with each other, Government and law enforcement agencies, sharing information and resources, to transform the response to a common challenge, and actively deter the threats we face in cyberspace (the work of the UK Council for Child Internet Safety offers a good example of what can be achieved).
- Companies capitalise on the growth in demand in the UK and globally for vibrant and innovative cyber security services.
- The private sector has built upon the strengths of the UK's skills base in cyber security to invest and create centres of excellence to provide the cyber security skills we will need in future.

Government

3.10 Government will play its part in achieving these aims. By 2015 we want a UK where we have:

- Built up our capacity to detect and defeat high-end threats.
- Helped shape an international consensus on 'norms of behaviour' in cyberspace.
- Reduced vulnerabilities in government systems and our critical national infrastructure.
- Grown the cadre of cyber security professionals.
- Strengthened law enforcement and tackled cyber crime.
- Improved prevention and public awareness.
- Raised business awareness.
- Seized the business opportunities – working with industry and academia to boost our share of the cyber security market and cemented the UK's status as a safe place to do business online.

3.11 The next section sets out how we will work with partners to achieve this vision.

4. Action: Meeting threats, taking opportunities

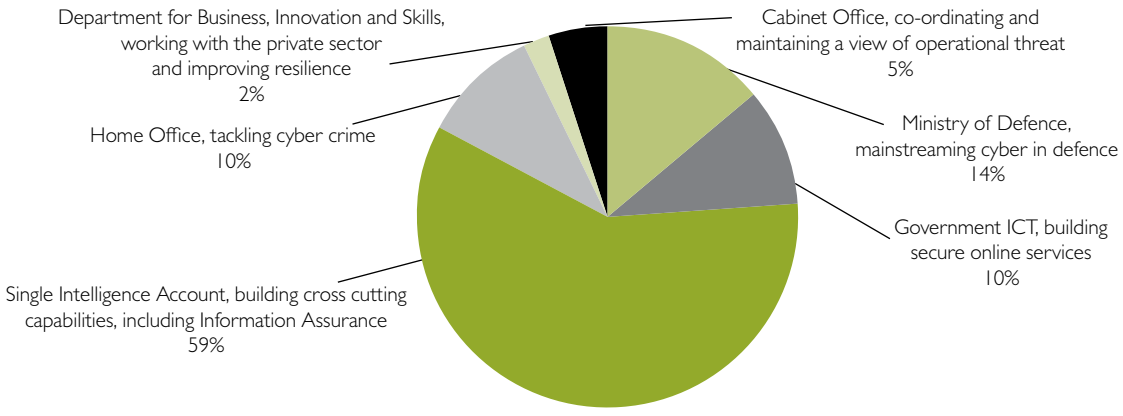
4.1 As one of the outcomes of its Strategic Defence and Security Review[13] in 2010 the Government put in place a £650 million, four-year National Cyber Security Programme (NCSP). This funding is intended to transform the Government's response to cyber threats, and has been allocated to those departments and agencies that have key roles to play.

4.2 The intelligence agencies and Ministry of Defence have a strong role in improving our understanding of – and reducing – the vulnerabilities and threats that the UK faces in cyberspace. GCHQ in particular is central to this effort. But the Home Office, the Cabinet Office and BIS are also receiving funding to bolster their specific individual capabilities. As set out in Chapter 3, outreach to business and the public is crucial. With the rise of cyber crime what was a concern primarily for the defence and intelligence elements of government is now something that concerns us all.

4.3 The NCSP is managed and co-ordinated on behalf of Government by the Office of Cyber Security and Information Assurance in the Cabinet Office, under the oversight of the Minister for the Cabinet Office. Allocations to departments for later years are provisional and can be adjusted if experience suggests that a different mix of inputs will produce better results.

4.4 Working through departments and their partners in business, civil society and internationally the NCSP will deliver on the following priorities. We will report on progress in a year's time.

National Cyber Security Programme investment (2011-2015)



Priorities for action

4.5 We will build on the UK's existing strengths as follows:

- We will continue to improve our detection and analysis of sophisticated cyber threats, with a focus on the UK's critical national infrastructure, and other systems of national interest.
- As part of this we will pool knowledge and situational awareness as appropriate with partners across business to build a genuinely national response.
- We will enhance our capability to defend against and deter high-end, state-sponsored threats, and to prevent these techniques becoming available to non-state actors.
- We will work internationally to develop international principles or 'rules of the road' for behaviour in cyberspace. We will work with other countries on practical confidence-building measures to reduce the risk of escalation and avoid misunderstandings.
- The UK has ratified the Budapest Convention on cyber crime and will work to persuade other countries to develop compatible laws, so that cyber crimes can be prosecuted across borders and cyber criminals are denied safe havens.
- At home we will maintain an effective legal framework and enforcement capabilities to disrupt and prosecute cyber crime. We will make it easier to report cyber crime and ensure that the intelligence from reporting is fed back into effective action and advice to the public. Where appropriate we will use cyber-relevant sanctions to tackle cyber crimes like online bullying or internet scams.
- We will model best practice on cyber security in the Government's own systems, setting strong standards for suppliers to government to ensure we raise the bar.
- We will promote the development of a cadre of skilled cyber security professionals so that the UK continues to retain an edge in this area, together with the underlying research and development to keep producing innovative solutions.
- Because prevention is key, we will work to raise awareness and to educate and empower people and firms to protect themselves online. 80% or more of currently successful attacks exploit weakness that can be avoided by following simple best practice, such as updating anti-malware software regularly.
- We will create a thriving market in cyber security products and services that can win the UK business abroad and contribute to growth. It will also enable us to promote the UK as a good place to do business in cyberspace.

Building capacity to deter and defend against high-end threats

4.6 The 2010 NATO Lisbon Summit highlighted the cyber domain as an area of significant new risk and opportunity for the Alliance. The new Strategic Concept committed the Alliance to:

> *"develop further our ability to prevent, detect, defend against and recover from cyber-attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations".*

4.7 In keeping with the NATO Strategic Concept, and with the agreement of the National Security Council, the NCSP is investing to ensure we take a more proactive approach to tackling cyber threats and exploiting the cyber environment for our own national security needs.

4.8 In the Ministry of Defence, investment in ensuring military networks and equipment are protected against cyber attack is already underway. The new Joint Forces Command will take the lead in the development and integration of defence cyber capabilities from April 2012.

4.9 As part of this we are creating a new Defence Cyber Operations Group to bring together cyber capabilities from across defence. The group will include a Joint Cyber Unit hosted by GCHQ at Cheltenham whose role will be to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through

operations in cyberspace. We will also consider the future contribution of reservists in bringing in specialist cyber knowledge and skills.

4.10 The Ministry of Defence has recently opened a new Global Operations and Security Control Centre, located at Corsham, to act as a focus for cyber defence for the armed forces. A second Joint Cyber Unit embedded within the centre at Corsham will develop and use a range of new techniques, including proactive measures, to disrupt threats to our information security.

4.11 The Ministry of Defence is also strengthening relations with key allies and with industry to improve our collective awareness of and response to cyber threats, vulnerabilities and incidents.

4.12 Around half of the £650 million funding will go towards enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks. The details of this work are necessarily classified, but it will strengthen and upgrade the sovereign capability the UK needs to confront the high-end threat.

Working to build international consensus on proportionality in cyberspace

4.13 At the same time we will work internationally to develop international principles or 'rules of the road' for behaviour in cyberspace.

4.14 As a start, the UK believes that all governments must act proportionately in cyberspace and in accordance with national and international law. This includes respect for intellectual property and for fundamental human rights to freedom of expression and association.

4.15 The UK has already set a lead in this area with the London Conference on Cyberspace in November 2011. It will continue to work in the UN and other international fora on the agenda set out in London, to develop norms of acceptable behaviour. We are clear that the debate must involve all those with a stake in an open, trusted and stable cyberspace, including industry, business and representatives of civil society.

4.16 Meanwhile the UK will work actively in the UN and with organisations such as the Organisation for Security and Cooperation in Europe (OSCE) to develop practical confidence-building measures to reduce the risk of escalation and avoid misunderstandings between states arising from unexpected incidents in cyberspace.

In February 2011 the Foreign Secretary called for 'rules of the road' for behaviour in cyberspace, and for a more focussed and inclusive dialogue between all those with a stake in the internet – civil society and industry as well as governments – on how we might implement them.

On 1-2 November that more focussed debate was begun at the London Conference on Cyberspace. This brought together Ministers, senior government officials, industry leaders, and representatives of the internet technical community and civil society. In all, more than 700 participants from 60 countries took part. There was also a lively online debate around the Conference, with citizens from across the world following the debate in real time through livestreaming, and feeding in questions and issues through the Web. The agenda set out in London will now go forward over the next 24 months with conferences in 2012 and 2013, hosted by Hungary and South Korea respectively, to take stock.

Reducing vulnerabilities in government systems and our critical infrastructure

4.17 The Government ICT Strategy sets out how Government is working to make its own **critical data and systems secure and resilient**. We will work with industry to develop **rigorous cyber security and IA standards** for ICT products and services supplied to Government and its Public Services Network. In particular we will raise the standard of cyber security we expect from suppliers for sensitive **defence equipment**. Just as we already place certain requirements on contractors' physical security, it now also makes sense to look again at our requirements on cyber security, as the means through which attempts to steal data are now most likely to come. The Ministry of Defence is leading on the approach to managing risks to Government information through the ICT Strategy, strengthening risk

management governance and building on the progress Government has already made in the oversight of Information Assurance.

4.18 The UK is about to see a big expansion of public services online as the Government rolls out its **'digital by default'** agenda. Many of these services will migrate to cloud computing in due course, and Government recently published a Cloud Computing Strategy[14] setting out how this shift will be effected without compromising security. This is the right thing to do to improve efficiency and service delivery to customers. But we need to make sure that these services are safe and resilient against fraud and cyber attack. Government is rationalising the numerous technology platforms used to deliver Government services. This will also enable increased protection and improve protective monitoring. We will set targets for the speed with which systems apply security patches to all of their supported software and machines. To ensure that service users can be identified and fraud prevented, the NCSP is funding work on a trusted and resilient approach to **identity assurance** and other supporting measures.

4.19 Of course much of the UK's **critical infrastructure** is not in Government hands but is owned and managed by the private sector. CPNI (see box) is already working with a network of critical national infrastructure companies to ensure that they take the necessary steps to protect key systems and data.

The Centre for the Protection of National Infrastructure delivers advice that aims to reduce the vulnerability of organisations in the national infrastructure to terrorism and other threats such as espionage, including those from cyberspace. It has built up strong partnerships with private sector organisations across the national infrastructure, creating a trusted environment where information can be shared for mutual benefit. Direct relationships are augmented by an extended network, which includes other Government departments and professional service organisations.

4.20 Government will now work to scale up this approach to reach a wider group of companies not currently deemed part of the critical infrastructure, but where the threat to revenues and intellectual property is capable of causing significant economic damage to the UK. CPNI will be critical to this effort through the NCSP-funded Cyber Protection Priorities outreach work.

4.21 **A cyber security 'hub'** (see below) is being established to make sure this wider group can draw on actionable information on threats and what can be done to counter them.

Responding in partnership: the cyber security 'hub'

In February 2011 the Prime Minister met the heads of some of the largest companies from all sectors of the UK economy to discuss the cyber threat and our shared interest in getting the response right.

In the months since, the private sector and Government have come together to design and build an innovative new approach focused on:

- exchanging actionable information on cyber threats and strengthening our response to incidents
- analysing new trends and identifying new and emerging threats and opportunities
- working to strengthen and link up our collective cyber security capabilities.

A joint public/private sector 'hub' will pool government and private threat information and pass that out to 'nodes' in key business sectors, helping them identify what needs to be done and providing a framework for sharing best practice. A pilot will commence in December involving five business sectors: defence, finance, telecommunication, pharmaceuticals, and energy. Lessons from this will be used to inform roll-out of the initiative to other sectors from March 2012. We will also establish the best way to make sure that SMEs are also aware of the threats and benefit from the cyber security 'hub'.

Encouraging a cadre of cyber security professionals

4.22 The pace of technological change is relentless. Keeping pace will require people who have a deep understanding of cyberspace and how it is developing. But these people are currently a scarce resource across Government and in business. There are clear and authoritative voices warning that cyber security skills and expertise in the private sector will be increasingly sought after, and that business and providers of education and training need to respond. To help boost and maintain the pool of experts in the UK and encourage the development of a community of 'ethical' hackers in the UK who can help ensure our networks are well protected, the National Cyber Security Programme will:

- Drive up the skill levels of information assurance and cyber security professionals by establishing programmes of certified specialist training by March 2012.
- Continue to support the Cyber Security Challenge (see below) as a way of bringing new talent into the profession.
- Strengthen postgraduate education to expand the pool of experts with in-depth knowledge of cyber.
- Strengthen the UK's academic base by developing a coherent cross-sector research agenda on cyber, building on work done by the Government Office for Science.
- Establish, with GCHQ's help, a research institute in cyber security, with an indicative budget of £2 million over 3.5 years.
- Commissioning research clarifying the extent, pattern and nature of the demand for cyber security skills across the private sector.

From postman to cyber expert

The UK will need cyber security experts with technical skills and an aptitude for problem solving and investigation. Cyber Security Challenge runs challenging competitions with a diverse range of entrants to help identify talented individuals. A recent winner was working as a postman, but now works as an information security professional for the Royal Mail.

Cyber crime and law enforcement

4.23 What is illegal offline is illegal online. We will ensure the UK has a robust legal framework that enables law enforcement agencies to tackle cyber crime.

4.24 Because cyberspace allows criminals to operate from around the world, we are working to encourage wider adoption of the Budapest Convention on cyber crime, putting in place compatible frameworks of law that enable effective **cross-border law enforcement and deny safe havens to cyber criminals**. We will make progress on this a key element of the UK's chairmanship of the Council of Europe over the next 12 months.

4.25 While having the right legislation in place is essential, this must also be supported by a willingness to act when called upon. We need practical collaboration and **capacity development on cross-border law enforcement**, to take place at a rapid pace that reflects the reality of the networked world. The UK is a strong supporter of the network of law enforcement contact points known as the '24/7 Network' as the best means to make sure that when urgent assistance is required, partner countries are able to obtain it. The UK will work with other countries to encourage them to join the 24/7 Network and to put in the commitment to make it a success. The Serious Organised Crime Agency (SOCA) already has liaison officers around the world.

4.26 We also need to make sure that we are able to respond robustly here in the UK. At home we are reviewing the UK's own **Computer Misuse Act** to ensure it is fit for purpose in an area of

fast-moving technological change. If amendments are needed, proposals for these will be brought forward as soon as possible.

4.27 The Government will also work to ensure that law enforcement agencies and the judiciary are aware of the additional powers the courts already have to protect the public when there is strong reason to believe someone is likely to commit further serious cyber crime offences. Computer use may be monitored or restricted under licence conditions when an offender is released, or through a Serious Crime Prevention Order (under the Serious Crime Act 2007). For example an internet fraudster can be prevented from offering goods for sale online. Other orders which may include restrictions on internet use are used to protect the public or victims in cases of sexual offences, harassment and anti-social behaviour. Through guidance we will encourage the judicial system to consider these **cyber-relevant sanctions for cyber offences** wherever appropriate.

4.28 In addition, the Ministry of Justice and the Home Office will consider and scope the development of a new way of enforcing these orders, using 'cyber-tags' which are triggered by the offender breaching the conditions that have been put on their internet use, and which will automatically inform the police or probation service. If the approach shows promise we will look at expanding cyber-sanctions to a wider group of offenders.

4.29 As well as broadening the powers at their disposal, we are also helping law enforcement agencies tighten up its operational response. As part of the creation of the National Crime Agency (NCA), we will create a **new national cyber crime capability**, drawing together the work currently carried out by the e-crime unit in SOCA and the Metropolitan Police's Central E-Crime Unit. The new unit will underpin the work of all four operational commands of the NCA (borders, organised crime, economic crime and Child Exploitation and Online Protection – CEOP) by providing specialist support, intelligence and guidance.

4.30 The unit will act as the national capability to deal with the most serious national-level cyber crime, and to be part of the response to major national incidents. The NCA will continue the good work of SOCA and the Metropolitan Police in finding ways to disrupt criminal activity even where – because of cross-border jurisdictional issues – convictions are unlikely. We will also use cyber techniques to disrupt other types of organised crime.

4.31 The NCA will also **support police forces** across England and Wales to drive up wider national capability on cyber crime, including through shaping the training for mainstream law enforcement on cyber issues, and making sure the links to related issues such as bullying or child exploitation are made. A key area will be ensuring the best possible flow of information between police forces and the NCA. The Government will look closely at the way intelligence (for example, on threats to children provided by CEOP) is used by forces and how the outcome of action by forces and the courts is fed back to develop the best possible picture on threats. As part of our work to build strong relationships between the police, business and communities, we will encourage the transfer of skills between these sectors. The Metropolitan Police's Police Central E-crime Unit has made groundbreaking use of Police Specials with relevant specialist skills to help tackle cyber crime: we will encourage all police forces to make use of such **'cyber-specials'**. We will involve people from outside law enforcement to help tackle cyber crime as part of the NCA cyber crime unit.

4.32 The increase in e-commerce, and use of networked technologies to underpin all elements of business make it an increasingly attractive target for criminals. Businesses have a key role in combating this kind of crime. We will learn from the success we have had in tackling online threats to children by bringing industry, law enforcement and government in the UK Council for Child Internet Safety (UKCCIS). We will introduce a similar forum, led by Ministers, to bring together a wide range of groups to develop **cross-sector working** on cyber crime. This forum will help drive forward work on designing out crime online, developing best practice for security, and effective crime prevention advice for all levels of business.

4.33 In parallel we are taking action to make sure that it is simple and straightforward for members of the public to **report cyber crimes**. Of course this should include being able to do so online.

4.34 Over half of all police forces already provide a facility for the public to report crime online, though these range from basic systems for certain crime types to fully integrated crime reporting tools. We will support forces to move to full online crime reporting by helping them identify good practice.

4.35 People are already encouraged to report fraud, including cyber fraud, through the internet, using the **Action Fraud** tool. We will make it easier for people to do this by improving its accessibility and functionality. Crime reports can currently take up to 30 minutes to complete online. We will aim to reduce that time by a half.

4.36 As well as allowing the police to follow up directly on individual crimes, better reporting will help build our intelligence picture through the National Fraud Intelligence Bureau, improving the targeting of enforcement resources and feeding into crime prevention advice.

Prevention and public awareness

4.37 Prevention is key. Most common cyber incidents could be prevented by quite simple 'cyber hygiene'. GCHQ estimates that 80% or more of currently successful attacks are defeatable by simple best practice, such as updating anti-virus software regularly.

4.38 In order to help people protect themselves we will:

- Help consumers respond to the cyber threats that will be the 'new normal' by using **social media** to provide warnings about scams or other online threats.
- Look at the best ways to improve cyber security **education at all levels** so that people are better equipped to use cyberspace safely.
- Work with internet companies to explore the potential for **online sanctions** for online offences.
- Work with **Internet Service Providers (ISPs)** to help individuals identify whether their computers have been compromised and what they can do to resolve the compromise and protect themselves from future attacks.
- Provide clear **cyber security advice** for use by anyone using the internet so that people can decide how they want to use cyberspace, informed of the risks.
- Improve the information available to people buying security products by encouraging the development of **security 'kitemarks'**. BIS will work with domestic, European and global and commercial standards organisations to stimulate the development of industry-led standards and guidance that help customers to navigate the market and differentiate companies with appropriate levels of protection and good cyber security products.

4.39 **Get Safe Online** (see below) already exists as a platform around which this effort will be built. We are talking to funding partners, internet companies, retailers and ISPs about how we improve it and make it more interactive; develop more sustained awareness activity; signpost the public to further sources of support; and through 'kitemarks' help consumers distinguish between genuinely helpful products and advice and the purveyors of 'scareware'. A joint action plan will be launched in the New Year.

Get Safe Online is a joint public/private sector campaign to raise awareness of online security, aimed at the general public and small businesses. It is sponsored by Government, Microsoft, HSBC, Cable and Wireless, Ofcom, Trend Micro, Gumtree, Verisign, Symantec and Paypal. It works with a range of community groups and aims to give people the confidence and know-how to use the internet securely. It combines marketing and PR activities with a comprehensive website (www.getsafeonline.org) giving up-to-date advice, tools and guidance on cyber good practice. It includes advice on topics such as online shopping, social networking sites, data theft and identity fraud.

Raising business awareness

4.40 As well as working with consumers, we need to raise awareness in **business** of the potential threat to reputation, revenues and intellectual property from cyber attack.

4.41 Business is the largest victim of crime and economic espionage perpetrated through cyberspace. Responsibility for the issue must be shared by Government and the private sector. Ultimately it is the private sector that owns the assets and makes the business decisions about investing in improved cyber security. We have already begun to do more to raise awareness of the threat and what businesses can do to protect their assets. However, raising awareness will only take us so far and we need to do more to bring about behavioural change.

4.42 The joint public/private sector **cyber security 'hub'** (see page 28) has a key role to play in helping to identify and manage threats by sharing information.

4.43 **Get Safe Online increases awareness and provides advice for consumers and small and medium sized companies.** But we need other measures to reach these businesses that are not already acting – and have lots of other competing demands on their time. We will use digital channels and online media to raise awareness of threats to information assets and reputation, and encourage more cyber-aware behaviour by SMEs, including using online tutorials.

4.44 In order to improve the protection of business critical information and assets the Government believes it is important to find ways to improve the profile and transparency of information about breaches of cyber security. BIS will publish in 2013 **comprehensive research into cyber security breaches including research into security breach disclosure** in UK business. In the meantime BIS will work through existing and ongoing research in this area (the 2012 Information Security Breaches Survey produced by PricewaterhouseCoopers and Reed Exhibitions) to improve understanding of the risks.

4.45 The market for security products can be hard to navigate for small businesses, just as it is for individual consumers. So BIS will work to stimulate the development of **industry-led standards** and guidance that help customers to differentiate good cyber security products and services. BIS is also exploring ways in which **industry-led standards for firms' performance on cyber security** might be used as a market differentiator more generally. BIS will work with users, industry and appropriate standards organisations (domestic, and European and international) to stimulate the development of appropriate standards.

4.46 The **suppliers of business services** have an important role to play in raising awareness. As well as mainstreaming cyber security messages in its own outreach to business, BIS will work with professional business services and the insurance market on how we can together ensure that cyber security is effectively managed as a business risk. BIS will hold a strategic summit with professional business services providers (including insurers, lawyers and auditors) to discuss how they can develop the services they offer to businesses to help them manage and reduce the risks.

4.47 Government will work specifically with the **retail industry** to address challenges there. The UK has one of the largest online retail economies in the world, with transactions estimated to be worth more than £100 billion in 2009; UK shoppers spend more on average online than in any other major economy. In order to protect this thriving online retail sector, the Government is establishing a Retail Cyber Security Forum to address the specific key issues for this sector, including effective reporting and information sharing. Government will work with the British Retail Consortium and its members to help consumers stay safe online.

4.48 Through their relationship with their customers, ISPs can make an important contribution to identifying and preventing cyber attacks on UK networks. Building on the existing relationships between Government and ISPs, we will work together to co-design a set of guiding principles that could be adopted on a voluntary basis. These principles might include agreement for ISPs to offer support to internet users to deal with malicious activity on their systems, agreement to establish a collaborative means of identifying and sharing threat information between Government and ISPs, or for ISPs to offer customers the means

to address compromises to their computers or to protect themselves from cyber attacks in future.

Fostering business opportunity

4.49 In order to support the private sector in taking the opportunities that cyberspace offers we will aim to foster a vibrant and innovative cyber security sector in the UK, with global reach.

4.50 GCHQ is home to world-class expertise in cyber security. Government will explore ways in which that expertise can more directly benefit economic growth and support the development of the UK cyber security sector without compromising the agency's core security and intelligence mission. For example, options examined might include:

- Working with private sector partners to explore the potential commercial applications for GCHQ's unique expertise.
- GCHQ working with BIS, the Technology Strategy Board and the Engineering and Physical Sciences Research Council to explore strategic vehicles for bringing together industry, academia and Government to develop and exploit innovations in cyber security.
- A government-sponsored venture capital model to unlock innovation on cyber security in SMEs.

4.51 As we have said, we plan to require higher cyber security standards for ICT products supplied into the Public Services Network. To ensure smaller companies can play their part as drivers of new ideas and innovation we will bring forward proposals as part of the Growth Review to help **small and medium sized enterprises** fully access the value of public procurement. For cyber security, Government is setting an expectation that at least 25% of the value of Government cyber security contracts go to SMEs, either by breaking contracts into lots or by including SME sub-contracting arrangements in contracts awarded to larger suppliers (providing these arrangements are proportionate to the market conditions for the particular requirements of the contract). The Cabinet Office will work with departments to ensure the transparency of SME arrangements in all new contracts, in line with the Prime Minster's commitments on transparency in procurement and contracting.

4.52 We are also raising the standard of cyber security we expect from **suppliers of sensitive defence equipment**. We are doing this on national security grounds: for example to prevent key data on equipment performance being compromised by a foreign intelligence service before the kit even enters service. But the Government hopes these rising standards for public procurement will also help drive forward the wider market in cyber security in the UK.

4.53 Better data on the extent of the problem, a developing insurance market and clearer signposts on what good cyber security looks like should between them help remove factors dampening demand within the UK. **UK Trade and Investment (UKTI)** will work with the security sector's trade associations to make sure that this increasing domestic strength is leveraged to help UK firms sell abroad. We will turn the threat into opportunity and make strong cyber security a positive for all UK businesses and part of the UK's competitive advantage.

4.54 Further information on the National Cyber Security Programme and the Government's approach can be found in Annex A.

Annex A: Implementation

Below is more detail on the Government's approach and the specific actions we will take to deliver against our cyber security objectives.

Objective 1: Tackling cyber crime and making the UK one of the most secure places in the world to do business

Cyberspace is an important and expanding part of our economy. Our objective is to tackle cyber crime and make the UK one of the most secure places in the world to do business.

Objective	Approach	Actions to include
Tackling cyber crime and making the UK one of the most secure places in the world to do business	**Tackling cyber crime** • Reducing online vulnerability • Restricting criminal activity online • Promoting more effective partnerships *Government lead: Home Office* **Making it safer to do business in cyberspace** • Increasing awareness and visibility of threats • Improving incident response • Protecting information and services • Fostering a culture that manages the risks • Promoting confidence in cyberspace *Government lead: BIS*	1. Encourage the courts in the UK to use existing powers to impose appropriate online sanctions for online offences. 2. Create a new national cyber crime capability as part of the new National Crime Agency by 2013. 3. Encourage the use of 'cyber-specials' to bring in those with specialist skills to help the police. 4. Significantly increase the law enforcement agency capability on cyber crime by March 2012, and develop new training, giving more capability to understand, investigate and disrupt cyber crime. 5. More resources will go into working with the private sector and our international partners in 2012, and from now SOCA will increase the focus of cyber crime in its international network. 6. Promote greater levels of international cooperation and shared understanding on cyber crime as part of the process begun by the London Conference on Cyberspace, in addition to promoting the Council of Europe's Convention on Cyber crime (the Budapest Convention) and building on the new EU Directive on attacks on information systems. Contribute to the review of security provisions of the EU Data Protection Directive and the proposed EU Strategy on Information Security. 7. Review existing legislation, for example the Computer Misuse Act 1990, to ensure that it remains relevant and effective. 8. By the end of 2011, build a single reporting system for citizens and small businesses to report cyber crime so that action can be taken and law enforcement agencies can establish the extent of cyber crime (including how it affects individuals and the economy).

Continued on next page

Objective 1: Tackling cyber crime and making the UK one of the most secure places in the world to do business *(continued)*

Cyberspace is an important and expanding part of our economy. Our objective is to tackle cyber crime and make the UK one of the most secure places in the world to do business.		
Objective	**Approach**	**Actions to include**
		9. Commencing this year, the police will mainstream cyber awareness, capacity and capabilities throughout their service. 10. Take action to tackle hate crime on the internet with a plan to be published in Spring 2012. 11. Exploring the ways in which GCHQ's expertise could more directly benefit economic growth and support the development of the UK cyber security sector without compromising the agency's core security and intelligence mission. 12. Starting in January 2012, harnessing the wider private sector joint working initiative on cyber security to ensure that law enforcement fully engages with business in information sharing and minimising the risks from cyber crime. 13. Working with domestic, European, global and commercial standards organisations to stimulate the development of industry-led standards and guidance that help customers to navigate the market and differentiate good cyber security products. 14. Work with business services providers (including insurers, lawyers and auditors) to discuss how they can develop the services they offer to businesses to help them manage and reduce the risks. 15. Work with other countries to make sure that we can co-operate on cross-border law enforcement and deny safe havens to cyber criminals. 16. Ensure that new national procedures (adopted in May 2011) for responding to cyber incidents, and the developing partnership between government and the private sector, facilitate agile information sharing on threats to business, with mitigating advice aimed at reducing impacts. 17. Bolstering (and, where necessary, building at pace) new operational partnerships between the public and private sectors to share information on threats, manage cyber incidents, develop trend analysis and build cyber security capability and capacity. Led by the Prime Minister and representatives of industry, an initial operating capability will be in place by March 2012.

Objective 1: Tackling cyber crime and making the UK one of the most secure places in the world to do business *(continued)*

Cyberspace is an important and expanding part of our economy. Our objective is to tackle cyber crime and make the UK one of the most secure places in the world to do business.		
Objective	**Approach**	**Actions to include**
		18. Support GetSafeOnline.org to become the single authoritative point of advice on responding to cyber threats (for example, the recent publication of an internet safety guide). 19. Promote robust levels of cyber security in online public services, allowing people to transact online with government with confidence. 20. Enable the UK cyber security industry to thrive and expand, supporting it in accessing overseas markets. 21. Develop a better understanding of the cyber security industry's strengths, growth potential and barriers to success. 22. Develop a marketing strategy to promote internationally the capabilities of the UK cyber security industry, by March 2012. 23. Raise awareness amongst businesses of the threat and actions that they can take to protect themselves including working through strategically important sectors to raise cyber security issues throughout their supply chains. 24. Encourage industry-led standards and guidance that are readily used and understood, and that help companies who are good at security make that a selling point.

Objective 2: Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace

Making the UK more resilient and better able to protect our interests in cyberspace will mean reorganising and refocusing our existing resources to find new ways to strengthen our national security.

Objective	Approach	Actions to include
Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace	**Defending our national infrastructure from cyber attacks** • Strengthening defences in cyberspace • Improving resilience and diminishing the impact of cyber attacks • Countering terrorist use of the internet *Government lead: Cabinet Office* **Ensuring that the UK has the capability to protect our interests in cyberspace** • Improving our ability to detect threats in cyberspace • Expanding our capability to deter and disrupt attacks on the UK *Government lead: MOD*	1. Work with the companies that own and manage our Critical National Infrastructure (CNI) to ensure key data and systems continue to be safe and resilient 2. Expand the government advice to include a wider range of organisations whose resilience is a priority for the UK economy. 3. Ensure that new national procedures for responding to cyber incidents (ensuring that key services can be maintained or restored quickly) are fully tested, both within the UK and in exercises with international partners. This will include a programme of exercises and plans for an EU-wide event in 2012. This builds on a minister-led incident management/response exercise (July 2011) and government's ongoing exercise programme. 4. Work with allies to ensure implementation of NATO's cyber defence policy (agreed in June 2011). 5. Through the Government ICT strategy, ensure that we build and maintain appropriately secure government ICT networks. 6. Supporting Olympic cyber security by joining up the relevant government departments and conducting exercises to ensure preparations for cyber incidents are robust. 7. Through the CONTEST strategy, increase our disruption of online radicalisation and recruitment, and safeguarding against cyber attack. 8. Sharpen our ability to identify the nature and attribution of cyber attacks. 9. Create and build a dedicated and integrated civilian and military capability within the MoD. Mainstreaming cyber within the organisation and setting up a Defence Cyber Operations Group (DCOG). An interim DCOG will be in place by April 2012 and will achieve full operational capability by April 2014. 10. Maintain and strengthen our ability to anticipate, prepare for and disrupt hostile acts in cyberspace (including improving information sharing across government and industry partners, enhancing defence against hostile acts and increasing law enforcement capability to investigate and prosecute those carrying out hostile acts). 11. Maintain capabilities that enable the UK's freedom of action and cyber advantage and preserve our sovereign capabilities in niche areas.

Objective 3: Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies

We will work in partnership with other nations and organisations to help shape the development of cyberspace to support its role as a driver of open societies, whilst promoting stability and reliability.

Objective	Approach	Actions to include
Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies	**Helping to shape the development of cyberspace** • Promoting an open and interoperable cyberspace • Promoting the fundamental freedoms and rights that we enjoy *Government lead: Department for Culture, Media and Sport (DCMS)* **Protecting our way of life** • Ensuring our security without compromising our values *Government lead: FCO*	1. Continue the process started by the London Conference on Cyberspace to establish international norms of acceptable behaviour in cyberspace. 2. Undertake a review of policy and regulation of the UK communication sector, with a view to publishing a Green Paper early in 2012 followed by a White Paper and a draft Bill by 2013. 3. Support the open internet, working with the Broadband Stakeholder Group to develop industry-wide principles on traffic management and non-discrimination and reviewing its transparency code of practice in early 2012. 4. Implement bilateral commitments set out in high-level communiqués (agreed in 2010 and 2011) with the US, Australia and France.[15] 5. Develop new bilateral relationships on cyber with those emerging powers that are active in cyberspace. 6. Encourage international and regional organisations to support capacity building, for example working with the Commonwealth to promote model legislation on cyber crime, with the International Telecommunications Union (ITU) to support training on technical standards, with the Council of Europe (during our chairmanship starting in November 2011) and with the Organization for Security and Co-operation in Europe (OSCE) to promote freedom of expression online. 7. Use multilateral and bilateral channels to discuss how to apply the framework of international human rights law in cyberspace and new challenges in guaranteeing such rights. 8. Strengthen international systems to build confidence among states in cyberspace, including through engagement within the OSCE on confidence-building measures.

Objective 3: Helping to shape an open, vibrant and stable cyberspace which the UK public can use safely and that supports open societies *(continued)*

We will work in partnership with other nations and organisations to help shape the development of cyberspace to support its role as a driver of open societies, whilst promoting stability and reliability.		
Objective	**Approach**	**Actions to include**
		9. Actively engage in the UN Group of Governmental Experts, which will reconvene in 2012, to ensure that a constructive report is made to the Secretary-General in 2014 in line with UN General Assembly Resolution 65/141. 10. Work closely with the European Commission and the External Action Service to encourage greater coherence within the EU on cyber issues. 11. Seek agreement with ISPs on the support they might offer to internet users to help them identify, address, and protect themselves from with malicious activity on their systems.

Objective 4: Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives

We will build a foundation of flexible knowledge, skills and capability in the UK, supporting all of our objectives.

Objective	Approach	Actions to include
Building the UK's cross-cutting knowledge, skills and capability to underpin all cyber security objectives	**Extending knowledge** • Building a coherent cross-sector research agenda • Deepening understanding of the threats, vulnerabilities and risks *Government lead: BIS* **Enhancing skills** • Building a culture that understands the risks and enables people to use cyberspace and improving cyber security skills at all levels *Government lead: BIS* **Expanding capability** • Building technical capabilities • Increasing ability to respond to incidents *Government lead: Cabinet Office*	1. Improve our ability to anticipate the technological, procedural and societal behaviour developments that affect our use of cyberspace. 2. Expand our understanding of the threats and vulnerabilities in cyberspace that affect the UK. 3. By March 2012, conduct research on how to improve educational involvement with cyber security significantly at all levels – including higher education and postgraduate level. 4. During 2012, establish a programme of exercises to improve our capability to respond to incidents in cyberspace, building on the experience gained exercising response mechanisms for the Olympics. 5. Improve levels of professionalism in information assurance and cyber defence across the public and private sector. Establishing a scheme for certifying the competence of information assurance and cyber security professionals by March 2012, and a scheme for certifying specialist training in 2012. Continuing to support the Cyber Security Challenge as a way of bringing new talent into the profession. 6. Put in place clear leadership of cyber across Government, with a dedicated minister and oversight at the highest levels of Government. 7. Support the application of research, working with the Government Office for Science and others to build innovative cyber security solutions, building on our world-leading technical capabilities in support of our national security interests and wider economic prosperity. 8. Manage crucial skills and helping to develop a community of 'ethical hackers' in the UK to ensure that our networks are robustly protected. 9. Enhance the world-class technical skills of GCHQ. 10. Identify Centres of Excellence in cyber research to locate existing strengths and providing focused investment to address gaps. First focused investment by March 2012. 11. Raise awareness amongst the public and businesses of the threat and the actions they can take to protect themselves.

References

1. www.internetworldstats.com/emarketing.htm
2. http://imsresearch.com/news-events/press-template.php?pr_id=1532
3. www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf
4. www.theukcardsassociation.org.uk/view_point_and_publications/facts_and_figures/internet_card_use_(2009)/
5. European Commission
6. www.mckinsey.com/mgi/publications/internet_matters/pdfs/MGI_internet_matters_full_report.pdf
7. Supervisory Control and Data Acquisition
8. www.cabinetoffice.gov.uk/content/transparency-overview
9. www.cabinetoffice.gov.uk/sites/default/files/resources/uk-government-government-ict-strategy_0.pdf
10. www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf
11. http://www.homeoffice.gov.uk/publications/counter-terrorism/counter-terrorism-strategy/
12. www.detica.com/uploads/press_releases/THE_COST_OF_CYBER_CRIME_SUMMARY_FINAL_14_February_2011.pdf
13. www.cabinetoffice.gov.uk/sites/default/files/resources/strategic-defence-security-review.pdf
14. http://www.cabinetoffice.gov.uk/sites/default/files/resources/government-cloud-strategy_0.pdf
15. http://www.number10.gov.uk/news/uk-us-co-operation-on-cyberspace/, http://www.number10.gov.uk/news/uk%e2%80%93france-summit-2010-declaration-on-defence-and-security-co-operation/

Cabinet Office
22 Whitehall
London SW1A 2WH

Publication date: November 2011

© Crown copyright 2011

You may re-use this information (not including logos) free of charge in any format or medium, under the terms of the Open Government Licence.

To view this licence, visit www.nationalarchives.gov.uk/doc/open-government-licence/
or write to the Information Policy Team,
The National Archives, Kew, London TW9 4DU,
or e-mail: psi@nationalarchives.gsi.gov.uk.

This publication is available for download at:
www.cabinetoffice.gov.uk

The material used in this publication is constituted from 75% post consumer waste and 25% virgin fibre.

Ref: 407494/1111