Cabinet Office

Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space

June 2009

Cyber Security Strategy of the United Kingdom

safety, security and resilience in cyber space

Presented to Parliament by the Prime Minister, by Command of Her Majesty

June 2009

Cm 7642

£14.35

ISBN: 9780101764223

Contents

Executive Summary

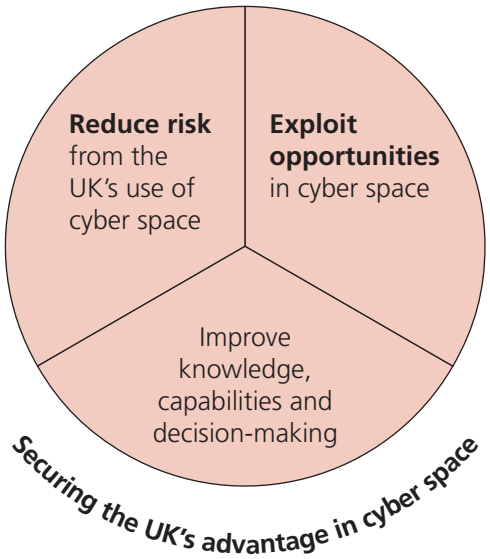
Every day, millions of people across the United Kingdom rely on the services and information that make up cyber space: that is, all forms of networked, digital activities. They may be aware of this if surfing the web, shopping or social networking online, or they may be unaware of the networked activity underpinning the services they rely on, and of just how critically dependent the work of government, business and national infrastructure is on this new domain of human activity. Either way, the effective functioning of cyber space is of vital importance. As the Government's *Digital Britain*[1] report says: "The Digital World is a reality in all of our lives". This document explains what the Government will be doing to ensure its safety, security and resilience and to exploit the opportunities it presents.

As the UK's dependence on cyber space grows, so the security of cyber space becomes ever more critical to the health of the nation. Cyber space cuts across almost all of the threats and drivers outlined in the National Security Strategy[2]: it affects us all, it reaches across international borders, it is largely anonymous, and the technology that underpins it continues to develop at a rapid pace.

The threats to those who use cyber space range from phishing to enable credit-card fraud through to corporate espionage. These activities can affect organisations, individuals, critical infrastructure, and the business of government.

This Cyber Security Strategy recognises the challenges of cyber security and the need to address them. It stresses that the UK needs a coherent approach to cyber security, and one in which the Government, organisations across all sectors, the public, and international partners all have a part to play. The Strategy outlines the Government's approach and puts in place the structures that the UK needs in order to weave together new and existing work to move towards our **vision**:

Citizens, business and government can enjoy the full benefits of a safe, secure and resilient cyber space: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience.



1 Digital Britain: The Final Report 2009 (Cm 7650)

2 The National Security Strategy: Security for the Next Generation 2009 (Cm 7590)

The Strategy highlights the need for Government, organisations across all sectors, international partners and the public to work together to meet our strategic objectives of **reducing risk and exploiting opportunities** by **improving knowledge, capabilities and decision-making** in order to **secure the UK's advantage in cyber space.**

The Government will…

Secure the UK's advantage in cyber space …

…by **reducing risk from the UK's use of cyber space…**

- Reduce the threat of cyber operations by reducing an adversary's motivation and capability;
- Reduce the vulnerability of UK interests to cyber operations;
- Reduce the impact of cyber operations on UK interests;

…and **exploiting opportunities in cyber space…**

- Gather intelligence on threat actors;
- Promote support for UK policies; and
- Intervene against adversaries;

…through **improving knowledge, capabilities and decision-making.**

- Improve knowledge and awareness;
- Develop doctrine and policy;
- Develop governance and decision making;
- Enhance technical and human capabilities.

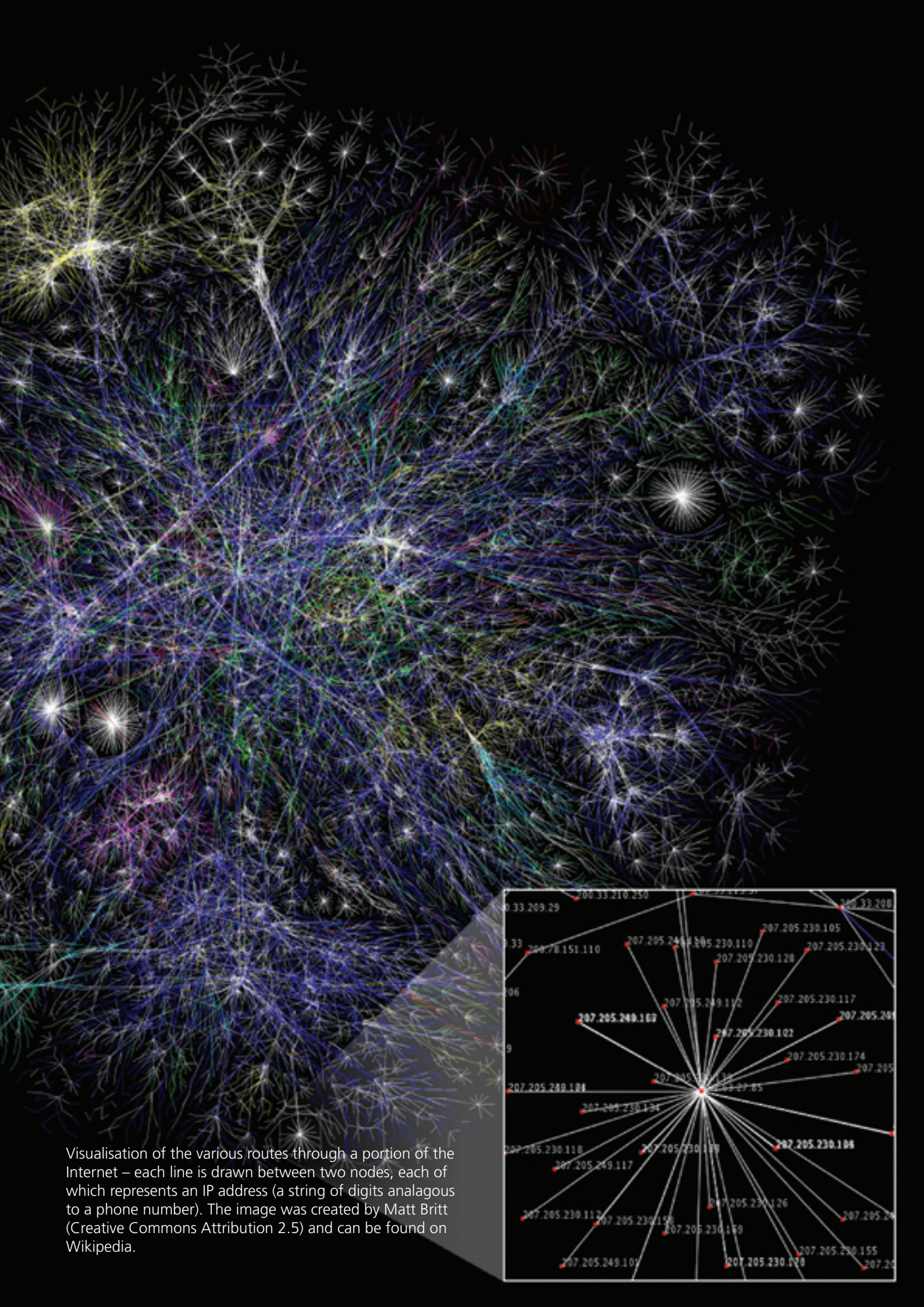
The Government, in conjunction with industry, already undertakes a range of high quality activity in the field of cyber security. However, the challenges are such – and cyber security is so important – that this needs to be developed further. One of the principal aims of this Strategy is to bring greater coherence to our cyber security work, by setting up two new organisations that will bring together the expertise and advice to meet this objective.

Our approach will be proportionate to the risks and we will put the protection and promotion of our fundamental rights and values at the heart of our work.

To address the UK's cyber security challenges, the Government will:

- ***Establish a cross-government programme*** to address priority areas in pursuit of the UK's strategic cyber security objectives, including:
  - Providing additional funding for the development of innovative future technologies to protect UK networks;
  - Developing and promoting the growth of critical skills;
- ***Work closely with*** the wider public sector, industry, civil liberties groups, the public and with international partners;
- ***Set up an Office of Cyber Security (OCS)*** to provide strategic leadership for and coherence across Government;
- ***Create a Cyber Security Operations Centre (CSOC)*** *to*:
  - actively monitor the health of cyber space and co-ordinate incident response;
  - enable better understanding of attacks against UK networks and users;
  - provide better advice and information about the risks to business and the public.

Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our advantage in cyber space. This Strategy – our first national Strategy for cyber security – is an important step towards that goal.



Visualisation of the various routes through a portion of the Internet – each line is drawn between two nodes, each of which represents an IP address (a string of digits analagous to a phone number). The image was created by Matt Britt (Creative Commons Attribution 2.5) and can be found on Wikipedia.

Chapter 1

Introduction

What is the vision for cyber security in the United Kingdom?

1.1 Citizens, business and government can enjoy the full benefits of a **safe, secure and resilient cyber space**: working together, at home and overseas, to understand and address the risks, to reduce the benefits to criminals and terrorists, and to seize opportunities in cyber space to enhance the UK's overall security and resilience.

Who is this for?

1.2 This document is aimed at all those people who work, communicate or interact using cyber space, and therefore have a responsibility for maintaining and improving its security; this includes individual members of the public, organisations across all sectors, and the Government. It will guide the Government's partnership approach domestically and internationally.

1.3 Many UK Government departments and agencies already have policies and projects relating to the security of cyber space, and some of the areas covered in this Strategy are the responsibility of the Devolved Administrations. This Cyber Security Strategy does not intend to duplicate existing work. Instead it intends to provide a strategic enabling framework through which to examine the challenges and the opportunities we face, and ultimately identify where we as a nation should be focusing our efforts in cyber security.

1.4 There is obviously a degree to which the disclosure of information regarding the UK's cyber security capabilities could be exploited by potential adversaries. Balanced against this risk, however, is the Government's strong belief in making public as much information as possible. In this document we have made every effort to withhold only information which would compromise our national security aims were it to be released.

Context

What is cyber space?

Cyber space encompasses all forms of networked, digital activities; this includes the content of and actions conducted through digital networks.

1.5 Computer and communications technology has developed enormously in speed and capability over the past fifty years, dramatically altering the way people interact with each other and their environment. Arguably the most significant development that these advances have led to is the emergence, over the past two decades, of cyber space – the new domain of computer-facilitated communication that is essential for the economic, social and political health of advanced nations. The physical building blocks of cyber space are individual computers and communications systems. These discrete technical elements underpin many of our daily activities, both at work and in our personal lives, and also fundamentally support much of our national infrastructure and information.

Why is cyber space important?

As consumers, some 90 per cent of our high street purchases are transacted by plastic which depends on wired and wireless communication to work. That is in addition to £50 billion of consumer purchases and sales through e-commerce that takes place wholly online.[3]

1.6 The home computer is a part of cyber space and the use of emails, social websites and Internet-shopping, for example, all take place within the cyber domain. Moreover, the global and real-time nature of cyber space means that businesses are able to co-ordinate complex, "just-in-time"[4] supply chains stretching around the world and operate 24-hour "follow the sun"[5] development and maintenance operations. The Government itself is reliant on cyber space and, through programmes such as the *Transformational Government Strategy*[6], provides efficient services to the public whenever and wherever they want them. All of these activities rely on the Internet and exploit the benefits of cyber space – and more will follow.

By mid 2008 around 16.5 million, or 65 per cent, of UK households had access to the Internet (an increase of 8 per cent since 2007).

Office for National Statistics, 2008

Trading online – Case Study

eBay Incorporated provides one of the largest online trading places in the world. The eBay website makes it possible for small businesses as well as individuals to trade with others through a platform which includes several advanced features such as secure transactions, ratings, image loading, and product descriptions. eBay's success is founded on empowering the end user - enabling consumers and businesses to compete in a universal online market. The impact of increased internet accessibility and in particular broadband has provided eBay users with an even greater opportunity to trade to greater numbers in a global audience.

Launched in September 1995, eBay has continued to grow rapidly. In 2008 the company posted pre-tax profits of $2.9 billion – an increase of 112 per cent on the previous year. At the end of March 2009 eBay had 88.2 million registered users.

1.7 Developments in cyber space are gathering pace and so is the degree to which we utilise them. This offers great opportunities for our economy and hence our prosperity. Businesses are increasingly interconnecting their own information systems in order to deliver more effective services to each other. Multi-national companies, such as telecommunications companies themselves, are consolidating

3 Digital Britain: The Final Report 2009 (Cm 7650)

4 Production and inventory systems that aim to minimise storage and stock management overheads by having supplies arrive at the moment they are needed.

5 Method of distributing tasks between sites in different time-zones around the world to provide, for example, continuous services around the clock.

6 Transformational government – enabled by technology 2005 (Cm 6683)

critical parts of their organisations into countries where costs are low, relying on networks to connect back to the UK. Our critical national infrastructure[7] – all the systems we rely on like utilities, food distribution, transport, the health service and the financial system – depends more and more on the Internet. UK interests are becoming ever more reliant on all the components of cyber space and this dependence is one that is far-reaching, affecting the individual citizen, almost all aspects of government, industry, our national infrastructure, transportation and the way our economy operates.

What do we mean by cyber security?

1.8 Cyber security embraces both the protection of UK interests in cyber space and also the pursuit of wider UK security policy through exploitation of the many opportunities that cyber space offers.

1.9 It is important to remember that cyber security is not an end in itself. It should not discourage the use of new technologies. The Government's *Digital Britain* Strategy aims to make the UK the leading major economy for innovation, investment and quality in the digital and communications industries. The Government's ultimate goal is to enable the full benefits of cyber space for the UK.

Why does the UK need a Cyber Security Strategy?

1.10 The UK is increasingly dependent on cyber space. As cyber space continues to evolve, we will pursue the increasing number and variety of benefits that it can offer; however, with growing dependence also comes a greater exposure to the rapidly evolving threats and risks. Government must lead a coherent UK response to the security challenges that arise from these threats and risks and a strategic approach is fundamental to achieving this aim.

Living and working online with confidence – Digital Britain

The UK's *Digital Britain* report sets out the Government's ambition to ensure that everyone can live and work online with confidence and safety. A world class approach to digital security, built on a safe, secure and resilient cyber space, will bring significant benefits:

- UK networks will be seen as safe and reputable (where perhaps others are unreliable or more vulnerable to criminal exploitation);
- The intellectual property of businesses, universities and other institutions, which underpins a knowledge economy, will be better protected;
- Businesses using UK networks will gain a competitive edge in the global marketplace;
- UK citizens and business will prosper as the volume of business transacted securely online continues to increase;
- UK citizens will have greater confidence in public service transactions, thus yielding efficiencies and cost savings;
- The businesses that have delivered secure functionality will have opportunities to sell their services globally on the back of UK success.

7 There are nine sectors (as defined by CPNI) which deliver essential services: energy, food, water, transport, communications, government & public services, emergency services, health and finance. Within these sectors there are key elements that comprise the critical national infrastructure. These are the components or assets without which the essential services cannot be delivered.

Guiding Principles

What are the principles that should guide our approach to security in cyber space?

1.11 The Government's approach to cyber security must be consistent with the overarching principles of the *National Security Strategy*:

- Our approach to national security is clearly grounded in a set of core values, including: human rights, the rule of law, legitimate and accountable government, justice, freedom, tolerance and opportunity for all;
- We will be hard-headed about the risks, our aims, and our capabilities;
- Wherever possible, we will tackle security challenges early;
- Overseas, we will favour a multilateral approach;
- At home, we will favour a partnership approach;
- Inside government, we will develop a more integrated approach;
- We will retain strong, balanced and flexible capabilities;
- We will continue to invest, learn and improve to strengthen our security.

Security and Liberty

1.12 The Government believes that the continuing openness of the Internet and cyber space is fundamental to our way of life, promoting the free flow of ideas to strengthen democratic ideals and deliver the economic benefits of globalisation. Our approach seeks to preserve and protect the rights to which we are accustomed (including privacy and civil liberties) because it is on these rights that our freedoms depend. A fundamental challenge for any government is to balance measures intended to protect security and the right to life with the impact they may have on the other rights that we cherish and which form the basis of our society.

1.13 Cyber security poses particular challenges in meeting the tests of necessity and proportionality, as the distributed, de-centralised form of cyber space means that a wide range of tools must be deployed to tackle those who wish to use it to harm the UK's interests. A clear ethical foundation and appropriate safeguards on use are essential to ensure that the power of these tools is not abused.

1.14 The programme of work outlined in this Strategy cannot and should not be progressed in isolation from these issues, and will require ongoing consultation with a variety of groups and organisations that work to safeguard our civil liberties and protect the privacy of the individual.

Partnerships and Stakeholders

1.15 The UK is by no means alone in facing the security challenges that cyber space presents, and no one player can address them in isolation. The interdependent nature of the national security threats and drivers in the cyber domain means that it is vital for the Government, organisations across all sectors, and the public to work together if we are to achieve our collective cyber security aspirations. Close engagement to strengthen existing cross-cutting private sector partnerships, and form new ones where required, will be fundamental to the current and longer term success of this Strategy. As Chapter 3 outlines, industry and other stakeholders will have a key role to play in the work required to realise the UK's vision for cyber security.

Industry Partnerships – Case Study

The Centre for the Protection of National Infrastructure (CPNI) 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 cyber space. It has built up strong partnerships with private sector organisations across the national infrastructure, creating a trusted environment where confidential information can be shared for mutual benefit. Direct relationships are augmented by an extended network, which includes other government departments and professional service organisations. This enables innovation to flourish and results in the sharing of best practice.
www.cpni.gov.uk

1.16 Additionally, the transnational span of cyber space requires that we work closely with international partners to ensure that its benefits continue to be delivered in a global, rules-based environment[8]. The UK can learn from the approaches taken by other nations and, as the Strategy explains, some of the issues can only be effectively tackled through international fora.

What is the Government already doing to secure cyber space?

1.17 The Government has been taking action to secure cyber space for several years. For example, the *National Information Assurance Strategy*[9] outlined the first steps for the UK in assuring the integrity, availability and confidentiality of Information and Communications Technology systems and the information they handle.

1.18 A number of organisations already work to protect the UK from cyber threats. For example, CESG (a part of GCHQ) provides the National Technical Authority for Information Assurance and runs the Computer Emergency Response Team (GovCertUK), which provides warnings, alerts and assistance in resolving serious IT incidents for the public sector; CPNI plays a similar role with the businesses and organisations that provide the UK's critical national infrastructure (see box); while the Home Office, the Serious Organised Crime Agency (SOCA) and the Police work to combat the activities of criminals in cyber space through initiatives such as the forthcoming ACPO e-crime strategy.

8 The UK is committed to working multi-laterally to develop a strong rules-based international system to promote economic growth and development, as well as mitigate the risk of another state acting to damage our economic well-being in a way that poses a threat to our national security.

9 National Information Assurance Strategy 2003, 2007

Chapter 2

Threats, Vulnerabilities, Impacts and Opportunities

Links to the National Security Strategy

2.1 The 2009 update to the *National Security Strategy: Security for the Next Generation* builds on the broad interpretation of the phrase "National Security" used in the inaugural 2008 version; it identifies the main threats to our national security, the drivers that may motivate those threats, and the interconnectedness between them. In addition, *Security for the Next Generation* recognises the existence of a number of physical and technological environments, such as land, maritime and space, which we can characterise as domains, in which national security threat actors can act to harm the interests of the UK and its people.

2.2 Cyber space is one such domain, where it is now possible to undertake actions that would previously have been impossible in the purely physical world. Cyber space is linked to almost all of the security challenges in the *National Security Strategy*, it transcends international boundaries, and it renders distance far less effective as a buffer against potential threats.

Increasing dependence…

2.3 The UK's use of cyber space is characterised by increasing levels of reliance as government, business and individuals continue to benefit from the significant advantages of our increasingly networked society. With this growing dependence, however, comes an increased level of exposure and vulnerability to some of the national security threats that interact with and through cyber space. For example, power supply, food distribution, water supply and sewerage, financial services, broadcasting, transportation, health, emergency, defence and government services would all suffer if the national information infrastructure were to be disrupted.

The average cost of an information security incident to a small company is £10,000–£20,000. For a large company, with more than 500 employees, it can be £1–2 million.[10]

…evolving threats…

2.4 The low cost and largely anonymous nature of cyber space makes it an attractive domain for use by those who seek to use cyber space for malicious purposes. These include criminals, terrorists, and states, whether for reasons of espionage, influence or even warfare.

Actors

Criminals

2.5 Organised cyber crime has grown exponentially over the past five to ten years as criminals continue to exploit

10 BIS Information Security Breaches Survey 2008

vulnerabilities in government, corporate and personal IT systems. Methods range from "phishing" and other techniques for influencing behaviour (i.e. by manipulating individual users) to more sophisticated "infections" capable, for example, of defeating anti-virus software. They employ automation for criminal endeavours, such as credit card fraud, and benefit from cyber space both to organise their activities (for example, online markets have arisen in stolen credit card details), and to launder proceeds of crimes including through use of online games. E-crime is estimated to cost the UK economy many billions of pounds every year. These attacks can affect individuals carrying out financial business from their home computer, and major enterprises controlling major transactions across complex networks.

Online fraud generated £52 billion worldwide in 2007.[11]

States

2.6 The most sophisticated threat in the cyber domain is from established, capable states seeking to exploit computers and communications networks to gather intelligence on government, military, industrial and economic targets, and opponents of their regimes. The techniques used by these state actors go beyond "traditional" intelligence gathering and can also be used for spreading disinformation and disrupting critical services. Undetected malicious software installed on a system can be adapted to suit an attacker's changing objectives, lying hidden within the system in readiness for exploitation during times of increased tension or conflict. Some states also encourage, and benefit from, the expertise of "patriotic hackers" – enthusiastic individuals or groups of skilled hackers, carrying out attacks safe from prosecution in their own countries. The use of proxies provides state actors with an extra level of deniability.

Terrorists

2.7 Terrorists and violent extremists use cyber space for communication, co-ordination, propaganda, fund-raising, radicalisation, and recruitment, providing them with an unprecedented opportunity to access a wider global community. Whilst we expect terrorist groups to continue to favour high-profile conventional operations over cyber attacks, we must be vigilant against any future increase in capability that might be directed against UK interests at home and overseas.

Methods of Attack

2.8 Cyber attack can be carried out in a number of ways:

- **electronic attacks**, launched over a network, whereby criminals and others attempt to gain access, either directly or by misleading the user, to devices such as mobile phones, computers or web-servers, and thereby obtain information on those systems, interfere with their services or use them as a launchpads for further attacks;
- **subversion of the supply chain**, where the technology supplied to an organisation or individual is subtly altered (for example by implanting malicious programs) in order to make network attacks easier, or to interfere with services;
- some systems can be attacked through manipulation of the **radio**

11 ACPO Strategic Assessment 2008.

signals upon which they are dependent (e.g. wireless networks and Global Positioning Systems); and
- given sufficiently **high power,** radio frequency transmissions can damage or disrupt all unprotected electronics in a given geographical area.

2.9 The effectiveness of these methods will vary according to the target and the wider context. The first two are more likely to be used covertly in times of peace, whereas the latter two are more overtly hostile, in some cases more easily attributed, and hence more suited to military activity, though not uniquely so.

2.10 Computer systems, networks and applications all rely upon people for their development, delivery, operation and protection. The likely success of an attack employing one or more of the methods outlined above is therefore increased when a so-called "insider" is involved.

…and emerging opportunities…

2.11 We also recognise that when criminals, terrorists and others use cyber space for malicious purposes they are also exposing themselves to new risks. Cyber space is therefore a useful domain for the UK to exploit to our advantage in fighting crime and terrorism, as well as in the military sphere.

2.12 There is an ongoing and broad debate regarding what 'cyber warfare' might entail, but it is a point of consensus that with a growing dependence upon cyber space, the defence and exploitation of information systems are increasingly important issues for national security. We recognise the need to develop military and civil capabilities, both nationally and with allies, to ensure we can defend against attack, and take steps against adversaries where necessary.

…mean that Government must lead a coherent UK response…

2.13 Cyber security cuts across almost all the challenges outlined in the *National Security Strategy*, and interlinks with a wide range of Government policies, involving many departments and agencies. The complexity and interdependence of these challenges means it is necessary to work coherently across all sectors in the UK, as well as with international partners, to ensure that the benefits of cyber space can be delivered in a rules-based, global environment.

2.14 That is why the Government is launching, alongside the *National Security Strategy: Security for the Next Generation*, the UK's first **Cyber Security Strategy.**

…a response where everyone – Government, business, the individual citizen – has their part to play.

2.15 As an increasingly digital nation, we need to be realistic about the risks that arise from our use of cyber space, and proportionate in our response. We all have an important contribution to make to ensure that we reduce those risks to the greatest extent possible: Government and businesses must work together to provide more secure products and services, to operate their information systems safely and to protect individuals' privacy. And the public too has a responsibility to take simple security measures to protect themselves, their families, and others in society. As we move forward, we will need to work collectively to further define the contributions that everyone can make, from the home computer user to the large business or government department.

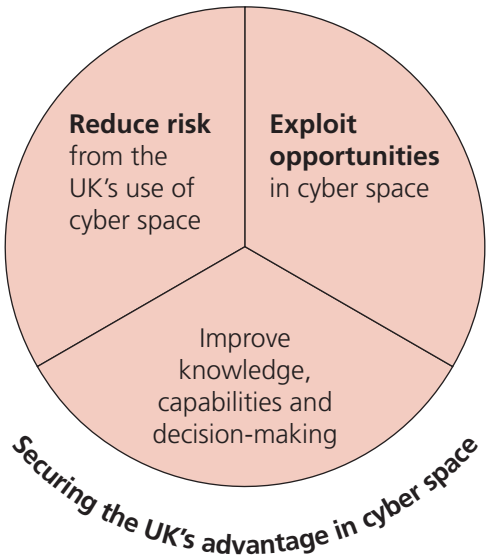
Chapter 3

A Coherent Response

3.1 This Strategy sets out an approach to meeting the security challenges in cyber space by outlining **the UK's strategic objectives** for cyber security, considering how we can move towards them, and **recommending areas of work to make this happen**.

Approach & Strategic Objectives

3.2 The Government's approach will **secure the UK's advantage** in cyber space by **reducing risk and exploiting opportunities**; enabling these strands through the **improvement of knowledge, capabilities and decision-making**.



3.3 Taking the aims in turn:

- **Reducing risk from the UK's use of cyber space** comprises the various ways in which the UK can defend its systems through preventing attacks, protecting against attacks, and reducing the impact of any attacks.
- **Exploiting opportunities in cyber space** covers the full range of possible actions that the UK might need to take in cyber space in order to support cyber security and wider national security policy aims; for example, in countering terrorism and in combating serious organised crime.
- **Improving knowledge, capabilities and decision-making** covers the wide range of tools and techniques, and the skills needed to employ them, that the UK needs in order to deliver the first two aims.
- Decisions on developing capabilities and undertaking actions either to reduce risk or exploit opportunities need to be carefully weighed to ensure that the UK **secures advantage** in cyber space.

3.4 In order to achieve these overarching aims, the Government will pursue the following strategic objectives:

The Government will…

"Secure the UK's advantage in cyber space …

…by **reducing risk from the UK's use of cyber space…**

- Reduce the threat of cyber operations by reducing an adversary's motivation and capability;
- Reduce the vulnerability of UK interests to cyber operations;
- Reduce the impact of cyber operations on UK interests;

…and **exploiting opportunities in cyber space…**

- Gather intelligence on threat actors;
- Promote support for UK policies; and
- Intervene against adversaries;

…through **improving knowledge, capabilities and decision-making.**

- Improve knowledge and awareness;
- Develop doctrine and policy;
- Develop governance and decision making;
- Enhance technical and human capabilities.

How will Government go about achieving these objectives?

3.5 The Government has undertaken a detailed analysis of the UK's existing cyber capabilities in all of these areas in order to define and prioritise areas of work. The disclosure of this detailed analysis in a public document would expose potential vulnerabilities to those who may want to use them for malicious purposes. We have not, therefore, gone into that level of detail here. However, the work outlined below flows from the strategic objectives, coupled with the analysis, and the two together give a cogent overview of how the programme will address our needs. New and more effective investment will be required to bring together existing work and to initiate new activity to meet these objectives – this will require a cross-government programme of work, and new structures to undertake it.

3.6 As already mentioned, cyber security is not an end in itself, and the new cyber structures will act as supplier organisations that provide policy guidance, expertise and situational awareness to those elements of government that deal directly with national security threats (for example the Home Office in the case of serious organised crime and terrorism), and to the private sector and the public.

New Cyber Structures

3.7 The following section outlines these **new cyber structures** and the key **workstreams** that they will initiate and drive forward. These new structures will need to be closely linked to, and ensure co-ordinated activity with, a number of existing organisations, as outlined at annex B.

What will the new cyber structures look like?

Cyber Security Operations Centre

3.8 The Government will establish a multi-agency unit (the Cyber Security Operations Centre (CSOC)) to monitor developments in cyber space (ultimately providing collective situational awareness), analyse trends, and to improve technical response co-ordination to cyber incidents. Not only will CSOC enable a better understanding of cyber security risks and opportunities, it will also help to ensure coherent dissemination of information across government, industry, international partners, and the public.

3.9 The CSOC will be a multi-agency body hosted by GCHQ in Cheltenham, with a membership drawn from across government and key stakeholders, and will report to an inter-departmental oversight board. It will be located alongside GCHQ's Information Assurance arm, CESG; thereby benefiting from existing knowledge and relationships that CESG has developed as the National Technical Authority for Information Assurance.

Office of Cyber Security

3.10 The Government will establish an Office of Cyber Security (OCS), that will initially be set up in the Cabinet Office. The OCS will have overall ownership of this Cyber Security Strategy, will provide strategic leadership across government for cyber security issues[12], and will drive delivery of the Strategy through a cross-government programme, elements of which are already underway, for example in the Information Assurance field under the *National Information Assurance Strategy*. There is no intention to replace or duplicate existing work, but rather to build on and extend where necessary to meet the strategic objectives. The programme will be organised into the following eight workstreams:

Workstream 1: Safe, Secure and Resilient Systems

3.11 This workstream will focus on enhancing the preparation for and protection from cyber attack in all sectors, to provide the greatest practicable resilience. This will require an improved understanding of potential vulnerabilities and the impacts were they to be exploited, as well as the establishment of appropriate mitigation measures. This will bring together ongoing work on redundancy and resilience in the telecommunications sector, for example, and feed into the business continuity arrangements for government and other critical sectors. It will need to consider, amongst other things, the encouragement of standards, and the need to refine procurement requirements.

12 Amongst others, the OCS will need to work closely with the Government's Chief Information Officer (CIO), the CIO Council, and the Central Sponsor for Information Assurance (CSIA).

Standards

The Cabinet Office, in conjunction with CESG and CPNI, provides up-to-date standards, policy and guidance on Information Assurance, Security and Resilience to the public and other critical sectors. This support, supplemented by international publications such as the ISO27000 series, helps people and organisations to manage their information security and other risks by understanding their vulnerabilities and applying mitigation measures.
www.iso.org
www.cabinetoffice.gov.uk

Workstream 2: Policy, Doctrine, Legal and Regulatory issues

3.12 In keeping with the programme approach outlined above, the OCS will identify gaps in the existing doctrinal, policy, legal and regulatory frameworks (both domestic and international) and, where necessary, take action to address them working with other departments. In some cases, the OCS will be best placed to lead the development of particular strands of policy work where they require cross-government co-ordination, such as the development and implementation of an industrial strategy for cyber security, in close collaboration with departments and key stakeholders in industry. This will seek to identify the national capabilities required in this area, set out how government will work in partnership with industry to develop and sustain these capabilities, in addition to stimulating innovative approaches to improve the UK's overall security. In other areas, for example in the future development of the legal framework for cyber security, it may be more appropriate for the work to be led elsewhere but overseen in the OCS.

Workstream 3: Awareness and Culture Change

3.13 The OCS will lead work to raise awareness of cyber security at all levels of government, and to identify and instil the changes in behaviour and working culture that our dependence on the cyber environment demands, as well as embedding cyber security in wider aspects of policy formulation.

3.14 The workstream will also encompass engagement with the public and key stakeholder groups on this issue to ensure appropriate information, support and advice is available on which to make risk-based decisions on a daily basis, and when more serious issues arise. This substantial and challenging stream of work will need to be designed and conducted in concert with existing work on Information Assurance to ensure consistency of message and approach.

Get Safe Online is a public and private sector joint campaign to raise awareness of online security aimed at the general public and small businesses. Get Safe Online is currently sponsored by the Cabinet Office, Serious Organised Crime Agency (SOCA), Microsoft, HSBC, Cable & Wireless, Ofcom and Paypal.

The Get Safe Online initiative works with a range of community organisations and aims to give people the confidence to go online securely. The initiative coordinates marketing and PR activities as well as providing a comprehensive website with up-to-date advice, tools and guidance on general internet security. The website includes information on protecting individuals, families and businesses online, as well as advice on topics such as Internet shopping, social networking sites, data theft and identity fraud.
www.getsafeonline.org

Workstream 4: Skills and Education

3.15 This workstream will examine the requirement to ensure the growth of skills and expertise needed by the Government and industry in the cyber security field. This is not limited to technical expertise but encompasses wider skills or combinations of skills which may be required to meet current or future skills gaps. This work will need to develop and initiate remedies to any identified shortfalls through, for example, development of training, provision of accreditation or incentives, and the longer-term development of viable career paths, within and outside Government.

Workstream 5: Technical Capabilities & Research and Development

3.16 This workstream will support and provide significant input into the work led by the Policy, Doctrine, Legal and Regulatory workstream to develop and implement an industrial strategy for cyber security. The workstream will take a longer term perspective on the health of our cyber security industrial base, informed by trends analysis undertaken at CSOC and ensure that our research and development efforts are focused, co-ordinated and exploited to best effect. This will involve close working with international and academic partners to ensure a truly coherent, international approach. As a first step the Government will provide additional funding to support and expand the collaborative work already being undertaken by Government and industry to help protect UK networks. The OCS will also work closely with the Network Security Innovation Platform (NSIP) in the Technology Strategy Board to provide opportunities for the UK's world class high-tech companies.

Workstream 6: Exploitation

3.17 This workstream will further develop the UK's understanding of the capabilities it needs to exploit cyber space to combat threats from criminals, terrorists and competent state actors, feeding into the policy work across Government in each of these areas. This work will identify gaps and develop strategies to address them. Finally, this workstream will drive forward the development of a consistent framework for understanding and communicating the risks, opportunities and impacts associated with our use of cyber space in pursuit of national security objectives.

Workstream 7: International Engagement

3.18 The OCS will be responsible for bringing greater coherence to the UK's work with overseas partners and international organisations. The OCS will not seek to take on the numerous bilateral and multilateral engagements that are currently undertaken by departments and agencies, though of course OCS staff will play their part. The value of the OCS function will be in co-ordinating the development and deployment of the UK's key messages in these fora, in conjunction with key allies, commissioning working groups to carry forward this work as required.

Workstream 8: Governance, Roles and Responsibilities

3.19 This stream will keep the evolving governance of UK cyber issues under review, will learn lessons, share best practice with key partners, and initiate amendments as required. There will also be the need to identify and tackle areas where governance arrangements are lacking, insufficient or are struggling to keep pace with the evolving

threats in cyber space. One area for early attention is e-crime, where the workstream will lead a review of the roles and responsibilities and strategic requirements in this area and ensure it is fed into the wider work of the OCS – as well as lead departments: this will result in a refreshed public e-crime strategy, set within the wider context of the Cyber Security Strategy.

E-crime

Due to the unique and international nature of the threat, an effective response to e-crime requires a broad cross-governmental response involving law enforcement, regulators and national security agencies. Each organisation has a key role to play in preventing e-crime and bringing those responsible to justice. At the strategic level, the OCS and Home Office will work together to co-ordinate the response to e-crime through the agencies sponsored by the Home Office. At the operational level, the forthcoming Association of Chief Police Officers' (ACPO) e-crime Strategy defines and scopes the national response of the police service to e-crime. SOCA will be the international lead for the UK operational response to e-crime.

3.20 These eight workstreams will form the basis for the cross-government programme that will deliver the Strategy. Fundamental to the success of all of these streams is the need to engage closely with key stakeholders to strengthen existing cross-cutting partnerships, and form new ones where required, with industry, civil liberties groups and other stakeholders internationally and in the UK.

3.21 The cross-government programme and both new structures will be overseen by interdepartmental oversight boards, the Cabinet committee for national security, international relations and development and its sub-committee focusing on protective security and resilience.

3.22 Both new structures will be established in September 2009 and will be operational by the end of March 2010.

3.23 This Strategy, the associated programme of work, additional funding, and the establishment of new structures mark a step-change in the UK's ability to deal with one of the most serious challenges to our national security – ensuring we can operate in a safe, secure and resilient cyber space.

Chapter 4

Conclusion

4.1 As the UK's dependence on cyber space grows, and we become increasingly reliant on it, so the security of cyber space becomes ever more important.

4.2 Just as in the 19th century we had to secure the seas for our national safety and prosperity, and in the 20th century we had to secure the air, in the 21st century we also have to secure our position in cyber space.

To address the UK's cyber security challenges, the Government will:

- ***Establish a cross-government programme**, with additional funding to address the following priority areas in pursuit of the UK's strategic cyber security objectives:*
  - Safe Secure & Resilient Systems
  - Policy, Doctrine, Legal & Regulatory issues
  - Awareness & Culture Change
  - Skills & Education
  - Technical Capabilities & Research and Development
  - Exploitation
  - International Engagement
  - Governance, Roles & Responsibilities

- ***Work closely with** the wider public sector, industry, civil liberties groups, the public and with international **partners**;*

- ***Set up an Office of Cyber Security (OCS)** to provide strategic leadership for and coherence across Government;*

- ***Create a Cyber Security Operations Centre (CSOC)** to:*
  - actively monitor the health of cyber space and co-ordinate incident response;
  - enable better understanding of attacks against UK networks and users;
  - provide better advice and information about the risk to business and the public.

4.3 This Strategy demonstrates that the Government recognises the security challenges of cyber space, it stresses the importance of a coherent approach, and it will put in place the structures that the UK needs to weave together new and existing work and drive forward a programme to meet our strategic objectives. The Strategy highlights the need for Government, business, international partners and the public to work together to meet our strategic objectives of **reducing risk and exploiting opportunities** by **improving knowledge, capabilities and decision-making** in order to **secure the UK's advantage in cyber space**.

Annex A

Frequently Asked Questions

Q. I work in a small business. Where do I get help with protecting computers and laptops?

A. Government is a founder supporter of the GetSafeOnline – a joint government and industry initiative to raise awareness of Internet safety. The website provides an authoritative and trustworthy source of simple advice to the public and small businesses about staying safe online.
www.getsafeonline.org

Q. I work in the public sector. Who is responsible for ensuring our information systems are secure?

A. Each public sector organisation is responsible for managing its own information risks. CESG (part of GCHQ) is the National Technical Authority for Information Assurance and provides advice and guidance to government departments and the wider public sector. In central government, departments should follow Cabinet Office policy as laid out in the Security Policy Framework which covers information security and assurance (Mandatory Requirements 31-49). Public sector organisations may wish to seek assistance from members of the CESG Listed Adviser Scheme (CLAS).

Q. I work for a company that is part of the UK's national infrastructure.[13] Where can I get security advice?

A. The Centre for Protection of National Infrastructure (CPNI) provides integrated security advice (combining advice on information, personnel and physical security) advice to the businesses and organisations that make up the national infrastructure. Through the delivery of this advice, it protects national security by helping to reduce the vulnerability of the national infrastructure to terrorism and other threats.

The CPNI web site contains a range of publicly available advice in relation to improving cyber security. It provides technical vulnerability notices for specific software products through to more general advice on how to avoid phishing attacks, reduce the risk from insiders and how to combat the use of deception to enable attacks.
www.cpni.gov.uk

Q. Where do I get help protecting my home computer or laptop?

A. The GetSafeOnline website provides an authoritative and trustworthy source of advice to the public.
www.getsafeonline.org

13 As defined by CPNI.

Q. How do I report an online crime or identity theft?

A. You should contact your bank, and might also consider contacting ConsumerDirect which is funded by the Office of Fair Trading, or Bank Safe Online which highlights the latest online scams and has a reporting mechanism – run by APACS on behalf of the UK banking industry. The Government is also setting up a National Fraud Reporting Centre which should be operating by the end of 2009. As more than 80 per cent of the e-crime seen by individuals would be classified as fraud, the Centre will take reports from the public, and will analyse them before passing them to the Police Central e-crime Unit or the Serious Organised Crime Agency for possible further action.
www.consumerdirect.gov.uk
www.oft.gov.uk
www.banksafeonline.org.uk

Q. How can I protect my children from viewing adult material on the Internet?

A. Advice is provided by the Child Exploitation and Online Protection Centre.
www.ceop.gov.uk

Q. I believe an organisation is misusing my personal information; who can help?

A. In the first instance, you should contact your organisation's Data Protection Controller and give them a chance to address your concerns. If the issue is not resolved, then you may need to approach the Information Commissioner's Office. The ICO is the UK's independent Authority responsible for regulating and enforcing access to and use of personal information. Government departments are required to publish Information Charters which clearly spell out how and why your personal information is used and who to contact if you have any concerns relating to that use.
www.ico.gov.uk

Q. What is the difference between Information Assurance and Cyber Security?

Information Assurance (IA) is about best management of the full spectrum of information security risks, including people, processes, technology and information assets. Government and industry have done much to advance this vital area of work for some time, and will continue to do so. The time is now right to bring additional focus and effort to the critical cyber domain and the Cyber Security Strategy builds on and extends the work of IA in this sphere. Cyber security will involve additional work, including some elements which necessarily are classified, as part of a coherent strategic approach to all aspects of security of data and of cyber space, as well as the exploitation of opportunities in cyber space to enhance the UK's overall security.

Annex B

Interfaces with Existing Organisations

Association of Chief Police Officers (ACPO) – on the development and direction of the police service in England, Wales and Northern Ireland; **ACPOS** in Scotland.
www.acpo.police.uk
www.acpos.police.uk

Attorney General's Office & the National Fraud Strategic Authority – for policy to combat online fraud and e-crime.
www.attorneygeneral.gov.uk

Cabinet Office – the National Security Secretariat, the Government Chief Information Officer (including the Central Sponsor for Information Assurance), and other Secretariats on specific policy issues, and the Assessments staff in relation to cyber threats.
www.cabinetoffice.gov.uk

Centre for the Protection of National Infrastructure (CPNI) – on protective security advice for businesses and organisations in the national infrastructure.
www.cpni.gov.uk

Department for Business, Innovation and Skills – for industrial and economic policy, and regulatory policy, particularly in the telecommunications sector.
www.bis.gov.uk

Devolved Administrations – for those functions which have been devolved to Northern Ireland, Scotland and Wales, according to their different devolution settlements.
www.scotland.gov.uk
www.wales.gov.uk
www.northernireland.gov.uk

Foreign Office – on foreign policy, international relations and international laws and behaviours in cyber space.
www.fco.gov.uk

GCHQ – for operations, capability and policy support, including CESG as the National Technical Authority for Information Assurance.
www.gchq.gov.uk

Home Office – for issues associated with the use of cyber space for criminality. The Home Office includes the Office for Security and Counter-Terrorism (OSCT): for terrorist-related use of cyber space.
www.homeoffice.gov.uk

Joint Terrorism Analysis Centre – on assessments of terrorist cyber intentions and capabilities.

Metropolitan Police – for e-crime issues, in particular, the Police Central e-Crime Unit.
www.met.police.uk

Ministry of Defence – for issues concerning the military use of cyber space, including defence policy and doctrine.
www.mod.uk

Secret Intelligence Service – on the collection of intelligence overseas to promote and defend the national security and economic well-being of the UK.
www.sis.gov.uk

Security Service – on protecting the country against covertly organised threats to national security.
www.mi5.gov.uk

Serious Organised Crime Agency – for issues relating to organised criminal use of cyber space.
www.soca.gov.uk

Technology Strategy Board – through its Network Security Innovation Platform, to develop innovative ways to improve online safety, security and resilience.
www.innovate.uk.org

Printed in the UK for The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 6173841 06/09

Printed on Paper containing 75% recycled fibre content minimum.

Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone Fax & E-Mail
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

The Parliamentary Bookshop
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/ General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

TSO@Blackwell and other Accredited Agents

Customers can also order publications from
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401