Cyber Security – A new national programme

Standard Note: SN/SC/5832
Last updated: 23 June 2011
Author: Emma Downing
Section Science and Environment Section

It is widely acknowledged that cyber attacks will increasingly be a key aspect of future warfare and organised crime. This note explains the increasing threat to national security posed by the new "front" of the cyber realm of networked, digital activities (often internet-based) and sets out the Government's response. The National Security Strategy (October 2010) has categorised "hostile attacks upon UK cyberspace by other states and large scale cyber crime" as one of its priority risks alongside terrorism, major accidents and natural hazards, and military crises. The associated Strategic Defence and Security Review (SDSR) responds to this with a new "transformative" £650m Cyber Security Programme to protect the UK from cyber attacks from both nation states and individuals.

Contents

1 Cyber space – a new UK security priority

The cyber realm of networked, digital activities (often internet-based) is now globally recognised as a 'new front' in military and security terms. The US has established a new Pentagon command for cyberspace (US Cybercom) and the Cabinet Office for Cyber Security and Information Assurance (OCSIA) has said that the UK faces "an ongoing, persistent risk from other states, terrorists and criminals operating in cyberspace." [1,2]

Cyber-based systems underpin our lives from energy generation to banking and shopping to emailing. Over 91% of UK businesses and 73% of UK households have internet access and £47.2 billion was spent online in the UK alone in 2009.[3,4,5] Information and Communications Technology (ICT) is a key part of the UK critical national infrastructure (CNI) along with water, energy and transport whose operational systems are also dependent on this sector. The growth of the Internet (estimated to be expanding by 60% a year) is increasing our reliance on cyber-based systems and bringing an increased vulnerability to any moves to disrupt such systems for political or individual gain as well as accidental disruption. [6]

In October 2010, the Director of Government Communications Headquarters (GCHQ), made an unprecedented, public address on cyber security prompted by an increasing public interest in the matter.[7] Meanwhile, General Sir David Richards (Chief of the Defence Staff) has said that Britain is devoting more energy to understanding and developing "weaponry" for cyber warfare than any other military area.[8] He has also highlighted that the UK must learn to defend, delay, attack and manoeuvre in cyberspace just as we might in on the land sea or air, and all together at the same time.[9]

The UK's national security planning now reflects this new terrain:

a) The National Security Council has assessed cyber attack as one of four most serious threats to the UK taking into account likelihood and impact over the next five years. The Government's new National Security Strategy (October 2010) therefore categorises "hostile attacks upon UK cyberspace by other states and large scale cyber crime" as one of the four Tier One Priority Risks alongside terrorism, major accidents and natural hazards and military crises.[10] These priorities closely mirror the five recently agreed EU strategic objectives for internal security.[11]

---

1 Who controls the Internet? *Financial Times Magazine*, 9/10 October 2010
2 Cabinet Office website, *Cyber security page* [on 19 January 2011]
3 Office for National Statistics, *E-commerce and ICT activity 2009*, 26 November 2010
4 Office for National Statistics, *9.2 million UK adults have never used the internet*, 27 August 2010
5 *GCHQ Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010 and Payments Council website, *Key Payment Facts (2009)* page [on 19 January 2011]
6 *GCHQ Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010
7 Ibid
8 Government concentrating on developing cyber "weaponry", *Reuters*, 23 November 2010
9 Army adds cyberattack to arsenal, *The Sunday Times*, 9 January 2011, p.6
10 Cm 7953, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, October 2010, p.27
11 As articulated in Com (2010) 673 final, *Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, 23 November 2010

b) The Strategic Defence and Security Review (SDSR) reflects this priority with a new "transformative" £650m CyberSecurity Programme to protect the UK from cyber attacks from both nation states and individuals.[12]

The Prime Minister's foreword to the SDSR explains the increased focus on cyber space:[13]

> Over the last decade the threat to national security and prosperity from cyber attacks has increased exponentially. Over the decades ahead this trend is likely to continue to increase in scale and sophistication, with enormous implications for the nature of modern conflict. We need to be prepared as a country to meet this growing challenge, building on the advanced capabilities we already have.

Cyberspace was evident in previous strategies but now has new emphasis. For example, the 2008 National Security Strategy (NSS) suggested that any state-led threat to the UK was likely to be via cyber-attack or covert, technical attacks by foreign intelligence organisations rather than conventional military means.[14]

The SDSR acknowledges this change in state-on-state conflict. It notes that those outmatched by conventional military capability can, and will, increasingly employ "asymmetric tactics" such as economic, cyber and proxy actions instead of direct military confrontation.[15] The 2007 cyber attack on Estonia (Box 1 below) was a wake-up call to the nation-scale disruption that can be caused. The NATO accredited cyber defence centre of excellence predicts that cyber attacks, employed in concert with conventional weapons, will become the standard operating procedure in future conflicts.[16] This was seen in Georgia in 2008, when cyber attacks on infrastructure by the supporters of South Ossetian separatism coincided with the Russian military offensive. The Georgian Government was unable to communicate with the international community to rally support.[17]

As the Royal United Services Institute has observed, the cyber threat has changed from the "spotty adolescent hackers making mischief" of a few years ago to the "game changing" feasibility of state-sponsored cyber attacks which could constitute an act of war.[18] However, international thresholds have yet to be agreed on when a cyber attack would be classed as an act of aggression.[19]

The Government's recognition of the importance of the cyberspace "arena" has been widely welcomed by the technology industry.[20] Intellect, the UK technology trade association, has

---

12 Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, Foreword

13 Ibid

14 Cm 7291, The National Security Strategy of the United Kingdom: Security in an independent world, HM Government, March 2008, p.16

15 Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, p.16 (Text Box)

16 Co-operative Cyber Defence Centre of Excellence website, *General Trends* page [on 8 December 2010]

17 Chatham House, *Transcript: Cyberwarfare – Addressing the Challenge, Speech by Nick Harvey MP, Minister of State for the Armed Forces*, 9 November 2010

18 Royal United Services Institute, *Preliminary RUSI briefing: The National Security Strategy 2010*, Prof. Michael Clarke – Director

19 Comment from International Institute for Strategic Studies as quoted in Cyber attacks test Pentagon Allies and Foes*, Wall Street Journal*, 25 September 2010

20 See HL Deb 12 November 2010 cc 393-507

described the creation of the National Cyber Security Programme as a "sensible reaction to the growing importance and vulnerability of cyberspace."[21]

In addition to the national security aspect, the Government recognises that cyber attacks can have a detrimental impact on the wider economic and social well-being of the country because Information Communications Technology (ICT) is such a key part of our critical infrastructure and means of doing business. A 2008 report by the US Centre for Strategic and International Studies, for the incoming President, concurred:

> In the new global competition, where economic strength and technical leadership are as important to national power as military force, failing to secure cyberspace puts us at a disadvantage.[22]

However, the SDSR is also keen to stress the opportunities available to the UK if we get cyber security right – a reputation for being a safe place to do business and a thriving export market in cyber security products. Analyst Gartner has forecasted that 2010 figures for worldwide spending on security software will show an increase of 11% to $16.5bn (approx £10.5bn).[23]

The new Cyber Security Programme (see Section 1.3) essentially seeks to build on the centralised approach to cyber security established by the previous Government and to tackle some of the emerging gaps. It establishes new cyber security institutions and education and skills initiatives with the aim of locating and addressing the weaknesses in existing cyber measures, anticipating future threats and building good working relationships in this area across UK sectors (both public and private) as well as nations.

The content of the Programme is not especially controversial. Most risk bases are covered with new initiatives.[24] As ever, execution, co-ordination and progress evaluation will be the key and whether the strategies and institutions can deliver sufficient protection, be sufficiently flexible and forge effective partnerships to tackle the ever changing threat.

1.1 What is the nature of the threat?

The cyber terrain is especially challenging because it is: complex, global, and constantly changing. Those seeking to cause disruption can be remote from their impacts, difficult (sometimes impossible) to trace and can cause mass impacts in seconds. There is also no defined perimeter in cyberspace which Government can defend and 80% of the critical national infrastructure is privately owned.[25] Chatham House has highlighted overly technical language as also posing a barrier to understanding and a danger of complacency because cyber attacks appear less destructive than acts of physical terrorism:[26]

The Director of GCHQ has described how cyberspace is contested around the clock. In the UK, there are over 20,000 malicious emails on Government networks each month, 1,000 of

---

21 Intellect reacts to the National Security Strategy and Strategic Defence and Security Review*, Intellect*, 21 October 2010

22 Centre for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency: A report of the CSIS Commission on Cyber security for the 44th Presidency*, December 2008

23 Gartner predicts positive future for software security industry, Techwatch,16 August 2010

24 Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, pp 11-12

25 Chatham House, *Transcript: Cyberwarfare – Addressing the Challenge, Speech by Nick Harvey MP, Minister of State for the Armed Forces*, 9 November 2010 and Intellect, *Strategic Defence and Security Review* 2010 (response), 21 October 2010

26 Chatham House, Evaluating the 2010 Strategy Review, October 2010, p.21

which are deliberately targeting them.[27] The Security Service estimates that at least 20 foreign intelligence services are operating to some degree against UK interests in cyberspace.[28] The US estimates that the Pentagon's computer systems are probed 250,000 times an hour with more than 140 foreign spy organisations trying to infiltrate US networks.[29] During the 2008 Olympic Games, Beijing alone experienced 12 million cyber attacks per day.[30]

The market leader security software firm, Symantec, produces world rankings of hotspots for malicious cyber activity. The UK was ranked 6th in quarter July - September 2010 behind the US, Brazil, India, China and Germany in line with its overall annual ranking for 2009. The latest report finds credit card information to be the most widely marketed on the underground economies that the company is aware of. It also notes a shift of malicious activity to emerging countries.[31]

The key cyber threats to security which GCHQ observes can be broadly categorised as:

- "worms" (malicious computer codes) disrupting Government systems, both those deliberately targeted and picked up from the Internet accidentally.
- use of cyber techniques by one nation on another to bring political or economic pressure to bear
- theft of intellectual property with both commercial and national security implications

GCHQ advises that Information Assurance practice (network security) can solve 80% of Government's Cyber Security vulnerabilities along with personnel security. The more difficult 20% of the threat is complex and "not easily addressed". GCHQ has warned that "patch and pray" will not be enough and new technologies, new partnerships and investment in the right people is necessary.

The Government is committed to moving more of its services online and within the next few years on-line tax and benefit payment systems could be processing over one hundred billion pounds' worth of payments each year. Even if systems are secure, identity theft of legitimate credentials still poses a problem.[32] Estimates for the overall costs to the economy of cyber crime are wide ranging but are always in the ballpark of billions of pounds.[33]

In his first speech on cyber security since inheriting the brief, Minister of the Cabinet Office and Cyber Security, Francis Maude commented:

> Exact figures are hard to pin down, but a recent study [by the Cabinet Office and Detica February 2011[34]] suggests that cyber-crime now costs the UK £27 billion annually - £2.2 billion of this to government, £3.1 billion to individuals, in the form of fraud and ID theft, and by far the largest portion - £21 billion – to industry, in the form of theft of intellectual property, customer data and price-

---

27 *GCHQ Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010
28 HC Deb 30 November 2010 c.763W
29 Who controls the Internet? *Financial Times Magazine*, 9/10 October 2010
30 Cm 7953, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, HM Government, October 2010, para 3.30 p.29
31 See Symantec, *Symantec Global Internet Security Threat Report – Trends for 2009*, Vol xv, Symantec, April 2010, Executive Summary and Symantec, *Symantec Intelligence Quarterly: July –Sept 2010*, October 2010
32 *GCHQ Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010
33 Ibid
34 Detica and Office of Cyber Security and Information Assurance, *The Cost of Cybercrime*, February 2011

> sensitive information. These are only rough estimates, but they give and idea of the vast scale of the problem. I wouldn't like to hazard a guess as to the global cost of such criminality but it is clearly a major inhibitor of international growth and prosperity.[35]

Recently, there has been a spate of cyber attacks on commercial companies. Attacks on Sony (compromising Playstation subscriber details);[36] and Nintendo have been attributed to LulzSec, a group of hackers thought to be an offshoot of Anonymous, the group behind Wiki Leaks. The group also targeted the NHS, US Senate and CIA.[37] In addition, there have been reported hacker attacks on the cosmetic brand Lush[38] whilst an attack on the European Union's emission trading system stole as much as €30m in carbon allowances and trading was halted due to the compromised system and loss of confidence. The incident highlighted the disparities in security among the national registries.[39]

These threats are also affecting how nations deal with internet freedom and security. For example, in 2010 various countries (including India and Dubai) threatened to ban Research in Motion (RIM), the Canadian manufacturer of the BlackBerry, from operating in their jurisdiction if the company did not lift its e-mail encryption or allow a local server to monitor the traffic in- country for security reasons. It is not clear what concessions RIM has made but it continues to operate normally in these areas.[40]

---

35 Cabinet Office, *Making Travel Safer in Cyberspace, Keynote speech of Francis Maude MP, Minister for the Cabinet and Cyber Security*, 1 June 2011

36 Sony press release, *Full restoration of playstation network services begins today*, 2 June 2011

37 We do it for laughs, says group that hacked Sony and the CIA, *The Times*, 18 June 2011

38 Hackers target cosmetics customers' bank details, *The Daily Telegraph*, 22 January 2011

39 Carbon trading shutdown spreads, *Financial Times*, 21 January 2011

40 UAE says BlackBerry dispute resolved before deadline, *msnbc.com* [on 19 January 2010]

Box 1: Fact not fiction - Recent examples of cyber threats

- **Stuxnet worm (July 2010):** The Stuxnet worm (a complex computer code) was used in the first cyber attack specifically targeting industrial control systems. This attack seemed to be directed at Iran, and its nuclear programme as it altered programmes regulating centrifuges refining uranium. Stuxnet is unprecedented in its design to allow hackers to manipulate real-world equipment without operators knowing (1). The worm targeted Siemens' systems, used in the energy sector to control nuclear and gas infrastructure and also in manufacturing and automotive industries. (2) Experts estimate that it took five to ten people to work on the Stuxnet worm for six months. The complexity and access to systems involved indicated a highly organised and well-funded project.(3) The European Network and Information Security Agency (ENISA) has called it a "paradigm shift" in threat.(4)

- **Chinese rerouting (April 2010):** All data traffic from military and civilian government networks in the UK, US, Australia and South Korea started re-directing through China Telecom. Although claimed to be accidental by the Chinese, security experts have highlighted some irregularities with the event.(5)

- **Operation Aurora' (December 2009)**: Google detected a highly sophisticated and targeted attack on its corporate infrastructure originating from China. The attack was found to have installed malware via email on computers in another 30 companies and Government Agencies.

- **Large scale fraud (2009/10):** An Essex-based gang, linked to Eastern Europe, was prosecuted for an on-line fraud making £2 million a month by stealing log-in details from 600 UK bank accounts and tricking users into providing additional information. The Police e-Crime Unit, working with the banking sector, detected the fraud which targeted weak security on individual's computers using Zeus Trojan malware (i.e. a malicious computer programme disguised as something else such as an email attachment).The fraud was co-ordinated from a single laptop with sophisticated software available on the internet.(6)

- **Pentagon breach (2008):** A virus hit Pentagon systems via a memory stick used by a soldier in the Middle East on a Pentagon laptop. This classified event was admitted in August 2010 and some software security experts noted the ability to detect the virus had been available since 2007.(7)

- **Conficker (2008)**: A botnet (8) on an unprecedented scale has been operating since November 2008 affecting millions of computers worldwide using the Windows operating system.(9)

- **Distributed Denial of Service Attacks (DDoS):** Estonia (2007) and Myanmar (2010) suffered high profile DDoS attacks thought to be politically motivated. In both cases, numerous computers overwhelmed the same target simultaneously. Myanmar was cut off from the Internet after more than 10 days of DDoS attacks which culminated in a massive data flood that overwhelmed the country's infrastructure ahead of the country's general elections.(10) Estonia's financial operations were severely compromised and Government communications networks were reduced to radio for a limited period.(11)

Footnotes

(1) *Symantec* briefing, The Stuxnet Worm [on 19 January 2011] (2) Stephen Trilling, Senior Vice President, Symantec, *Heading off targeted attacks*, Symantec CIO Digest, October 2010 3) *Symantec* briefing, The Stuxnet Worm [on 19 January 2011] (4)ENISA Press Release, *European Agency analysis of 'Stuxnet' malware – a paradigm shift in threats and Critical Infrastructure Protection*, 21 October 2010 (5) China hijacked UK internet traffic says McAfee, *ZNet UK*, 18 November 2010 (6) Metropolitan Police News Bulletin 1527*Gang sentenced for 'trojan' bank theft scam*,16 November 2010 and High tech crime police quiz 19 people over internet bank scam that netted hackers up to £20m from British accounts, Mail Online, 29 September 2010 (as linked to from Metropolitan Police website). (7) Pentagon official reveals "most significant" military breach, *SC Magazine* (for IT Security Professionals), 26 August 2010 (8) A botnet is a group of computers compromised and co-opted by an 'intruder'. A single compromised computer is known as a 'bot'.(9) SEC(2010) 1122 final, Council of the European Union, 14436/10 ADD 1, *Commission staff working document Impact Assessment: Accompanying document to the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222/JHA*, 4 October 2010 (10) DDoS attacks take out Asian nation: *Myanmar fades to black*, The Register, 3 November 2010 (11) House of Lords European Union Committee (Sub-Committee F Home Affairs), Fifth Report *Protecting Europe against large scale cyber attacks*, Session 2009-10, para 12

1.2 How does the UK currently manage cyber security?

The European Information Network Security Agency (EINSA) has identified the UK as one of the leading states in the EU dealing with internet incidents and the UK is generally seen as having sophisticated defences and "reasonably well placed" to cope with disruptions from cyber attacks.[41]

The UK's first Cyber Security Strategy was produced in 2009 which created central cyber security capability for the first time:[42]

- The Office of Cyber Security (and now also Information Assurance), to co-ordinate policy across Government and pool intelligence from police and security services and
- Cyber Security Operations Centre in GCHQ, to co-ordinate the protection of the country's major IT systems.

The Strategy (updated in March 2010)[43] was also intended to help co-ordinate existing cyber security efforts across Government in a "strategic enabling framework". It prioritised the development and growth of critical skills and additional funding for the development of innovative future technologies to protect the UK network.[44] In October 2010, the then Home Office Minister, Baroness Neville Jones, praised the previous Government for establishing the centralised approach which the current Government is seeking to build upon.[45]

The key infrastructure for UK cyber security is set out in Appendix 1 of this note. Nick Herbert, the Minister of State for Policing and Criminal Justice summarised how the system works in relation to the cyber security of Government Departments in answer to a Parliamentary Question in December 2010:

> Departments are required to have technical controls in place to protect their ICT systems from cyber threats. GCHQ, through its information assurance arm, CESG, and its Computer emergency Response Team, GovCertUK, provides Government Departments with guidance on how to protect themselves against, detect, and mitigate various types of cyber attack, and acts as a single point for reporting Government network security incidents.[46]

Cyber crime

UK Government policy has consistently been such that what is illegal offline is also illegal on-line.[47] However, there is some specific legislation targeted at on-line situations such as hacking and misuse of communications systems, for example, the Computer Misuse Act 1990.

The Home Office, the Serious Organised Crime Agency (SOCA) and the Police tackle cyber crime. The Police Central e-crime Unit (PCeU) was established in 2008 after the Association of Chief Police Officers (ACPO) made a business case to the previous Government to fill the gap left after the National Hi-Tech Crime Unit (NHTCU) was subsumed by the Serious

---

41 House of Lords European Union Committee, *Protecting Europe Against large-scale cyber-attacks*, HL Paper 68, 2009-10, March 2010, para 24

42 Cm 7642, Office of Cyber Security and UK Cyber Security Operations Centre, *Strategy of the UK: Safety, security and resilience in cyberspace*, June 2009

43 Cm 7842, Home Office, *Cyber Crime Strategy*, March 2010

44 Ibid, p.7, para 1.3

45 HL Deb 14 October 2010 col 696

46 HC Debate 13 December 2010 c.534W

47 HC Deb 14 July 2008 c.113W

Organised Crime Agency in 2006.[48] The PCeU co-ordinates the law enforcement approach to all types of e-crime, develops capability of the police force to deal with this type of crime in England, Wales and Northern Ireland and provides a national investigative capability for the most serious e-crime incidents.[49] In 2009, the PCeU had a budget of £2.75million.[50]

The ACPO e-crime strategy (May 2009) sets out the Police Service's strategic approach to e-crime.[51] It aimed to improve the Police's response to e-crime, make it consistent and better able to use intelligence to disrupt criminal networks. In October 2010, the Metropolitan Police Commissioner, Sir Paul Stephenson warned that the expertise available to deal with cyber crime was thin compared to the skills at the disposal of cybercriminals.[52] He highlighted a number of resource points ahead of the Spending Review in an article in The Sunday Telegraph:

- Of the 385 officers in England and Wales dedicated to online work, 85% are fighting people-trafficking and child pornography – leaving fewer than 60 to fight financial crimes such as bank fraud.

- It is estimated that the global 'virtual task force' of which the Met is part prevented £21 in potential theft for every £1 spent on it.

At the time, the then Minister, Baroness Neville-Jones publically acknowledged these remarks and agreed that not enough is being done to deal with cyber crime and Government needs to "up" its act.[53] However, the Government acknowledged that the PCeU made a significant number of arrests in 2010 and has been very successful in tackling organised crime groups targeting the UK through the internet.[54]

2 Key elements of the new National Cyber Security Programme

It is proposed that all departments will work to a "transformative" National Cyber Security Programme. This will be supported by £650 million (£500m new money) over the next four years.[55] Home Secretary, Theresa May confirmed in February 2011 that £63 million of this will be allocated to cybercrime[56] and £30m of the funding will be used to set up regional e-crime units.[57]

The Deputy Director of the Office of Cyber Security and Information Assurance outlined the breakdown of priorities and funding in a speech in April 2011:[58]

- Four "pillars" for Government focus: improving national cybersecurity, improving cyber-defence of critical infrastructure, combating cybercrime and enhancing education and skills.

---

48 House of Lords Science and Technology Committee, *Personal Internet Security: Follow-up*, 4th Report, Session 2007-08, HL Paper 131, Written evidence p.29
49 Metropolitan Police website, Police Central e-crime Unit page [on 19 January 2011]
50 Police Chief warns of rise in cybercrime, *The Telegraph* - Technology News, 2 October 2010
51 Association of Police Officers (ACPO), *ACPO e-Crime Strategy*, May 2009
52 Police Chief warns of rise in cybercrime, *The Telegraph* - Technology News, 2 October 2010
53 HL Deb 14 October 2010 c 698
54 HC Deb 29 November 2010 c507W
55 HC Deb 19 October 2010 c798
56 HC Deb 11 February 2011 c23WS
57 Home Office announces 63m funding boost for cybercrime prevention, *Infosecurity*, 17 February 2011
58 UK cybersecurity spending plans revealed, *ZdNet UK*, 20 April 2011

- The £650m to be split between 65% on capabilities, 20% on critical cyber-infrastructure, 9% on cybercrime specifics, 1% on education and 5% on reserves.

The important role of the private sector and academia is stressed in terms of leveraging the knowledge and resources necessary to co-design credible policy, achieve buy-in from those that own and operate large elements of the critical cyber infrastructure and to obtain value for money.

There is no mention of whether the Government thinks that there are any gaps in current enforcement regimes and whether further legislative measures or voluntary, technical standards might be necessary in this arena.

The lead Minister for Cyber Security was initially the Security Minister in the Home Office (a member of the National Security Council) working with the Director of Cyber Security and the National Security Secretariat both in the Cabinet Office. However, the lead Minister is now the Minister for the Cabinet Office and Cyber Security (currently Francis Maude MP).

The programme relates to all elements set out in the National Security Tasks and Planning Guidelines and there is something for everyone in terms of risk bases covered.[59] It is also closely aligned to the cyber crime actions and themes of the EU's Internal Security Strategy.[60] The Programme, as set out in the review, seems to be focused on protection against cyber threats but clearly these initiatives can equally inform offensive cyber measures. The Armed Forces Minister recently referred to UK cyber capabilities supplementing physical capabilities thereby giving the UK "protection where necessary and greater flexibility where required".[61]

The key elements of the Programme are set out below. These were supposed to be brought together in a new Cyber Security Strategy in spring 2011. The SDSR also refers to a "strengthened" Office of Cyber Security.[62]

Cyber crime

- An overhaul of the UK's approach to cyber crime including a new:

  a) Home Office National Cyber Crime Strategy (originally planned for late Autumn 2010, then expected early 2011 but still not published.[63])

  b) single point of contact for reporting cyber crime (public and businesses)

  c) programme of skills development for those tackling cyber crime

---

59 Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, pp 11-12

60 Com (2010) 673 final, *Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe*, 23 November 2010

61 Chatham House, *Transcript: Cyberwarfare – Addressing the Challenge, Speech by Nick Harvey MP, Minister of State for the Armed Forces*, 9 November 2010

62 Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, p.65

63 HC Deb 21 December 2010 c.1211W

Cyber Security

- Address deficiencies in the UK's ability to detect and defend itself against cyber attack e.g through improving the delivery of cyber products and services and investment in intelligence capability
- Create a new Defence Cyber Operations Group to mainstream cyber security through the MOD and integrate it across all defence operations.
- Address shortcomings in the critical cyber infrastructure of the UK, tackling immediate weaknesses and maintaining access to a trusted industrial base
- New Cyber Infrastructure Team within the Department for Business Innovation and Skills (BIS) to provide strategic leadership and regulatory oversight
- Sponsor long-term cyber security research to build and maintain excellence
- New programme of cyber security education and skills for the public and businesses to encourage a more preventative approach to cyber security throughout the UK
- Continue to build cyber security alliances e.g a Memorandum of Understanding with the US and undertake capacity building with partner countries to ensure that where the UK has key national interests at stake, minimum standards of cyber security are being met.

There is little more detail about these proposed initiatives, although the Armed Forces Minister, Nick Harvey MP, has provided some more insight into the proposed work of the Defence Cyber Operations Group:

> The Group will provide a cadre of experts from across Defence to support our own and allied cyber operations, to secure our vital networks and guide the development of our cyber capabilities. It will also be responsible for developing, testing and validating cyber techniques as a complement to traditional military capabilities.[64]

2.1 Progress to date

Closer working with the US

In January 2011, Theresa May hosted US counterpart Janet Napolitano for talks on cyber security (among other issues) as part of their regular meetings to discuss security matters.[65] The UK and US then reaffirmed their close bilateral co-operation and new steps forward on cyberspace issues, particularly cyber security, during President Obama's May 2011 visit to the UK. The short communiqué agreed is provided on the Cabinet Office website.[66] It covers all of the areas of the UK's own cyber security programme pledging co-operation and mutual support. For example, promoting the Council of Europe Convention on Cybercrime (also known as the Budapest Convention) as the world's foremost treaty to combat cybercrime internationally, working more closely with private sector and business partners and co-ordinating research and development by jointly requesting R&D proposals, providing joint funding and conducting cooperative reviews.

---

[64] Chatham House, *Transcript: Cyberwarfare – Addressing the Challenge, Speech by Nick Harvey MP, Minister of State for the Armed Forces*, 9 November 2010

[65] Home Office news, *Home Secretary meets US counterpart*, 28 January 2011

[66] Cabinet Office, US/UK Cyber Communiqué, 25 May 2011

National Crime Agency

The Government has announced the establishment of the National Crime Agency (NCA) which will house a new National Cybercrime Unit (NCU).[67] The NCA will have four "commands": Organised Crime, Border Policing, Economic Crime and the Child Exploitation and Online Protection Centre (CEOP – which already exists). Subject to legislation, the NCA will be fully operational by December 2013.[68] The NCU will span all of the commands recognising cybercrime as a crime in itself and a tool for the execution of other crimes. [69]

UK cyber security conference

The UK is working internationally to try and establish the norms of behaviour in cyberspace both in regard to countering cyber threats and upholding freedom of expression. To this end, the UK is hosting an international conference in November 2011 which aims to bring countries together to explore mechanisms for giving such standards "real political and diplomatic weight".

At the Munich Security Conference on 4 February 2011, the Foreign Secretary, William Hague announced this conference and set out the UK's view on the need for better international co-operation on cyber security:

> Cyber-security is on the agendas of some thirty multilateral organisations, from the UN to the OCSE and the G8. NATO's Lisbon Summit in November launched a new programme to defend NATO's communication systems from cyber attack. But much of this debate is fragmented and lacks focus.
>
> We believe there is a need for a more comprehensive, structured dialogue to begin to build consensus among like-minded countries and to lay the basis for agreement on a set of standards on how countries should act in cyberspace. How this dialogue is organised is up for discussion. But we need to get the ball rolling faster.[70]

2.2 Issues arising from the new approach

Future of the Police Central e-Crime Unit

Elements of an "overhaul" of the UK's approach to cyber crime are set out in the new Programme but the Government has not yet decided what will happen to the PCeU or how it will relate to the new National Crime Agency.[71] The plan for the new agency confirms that there will be no changes to Central Police E-crime Unit or Serious Organised Crime Agency until after the Olympics.[72]

As the Unit was only created in 2008 any major changes would be disruptive to operations in the short term and would clearly need to be in the context of an improved, long term strategy for e-crime.

---

67 Cm 8097, *Home Office*, Plan for the creation of a national crime fighting capability, June 2011

68 Home Office Press Release, *New national crime fighting agency to transform the fight against serious and organised crime*, 8 June 2011

69 HoC Deb 8 June 2011 c237-8

70 FCO, Speech by Rt.Hon William Hague, Foreign Secretary to the Munich Security Conference, *Security and Freedom in the cyber age – seeking the rules of the road*, 4 February 2011

71 HL Deb 14 October 2010 c.698

72 Cm 8097, Home Office, *The National Crime Agency: A plan for the creation of a national crime fighting capability*, June 2011

Liaison with industry and academia

The new cyber security programme aims to promote greater co-ordination and co-operation with the private sector and academia. A similar commitment was made in the 2009 UK Cyber Security Strategy and the ACPO e-crime strategy (2009-12).[73] It is not yet clear what new approaches will be tried and what areas for co-operation will be prioritised. Although the US/UK communiqué (see 2.1 above provides further direction). Effective cross-fertilisation is crucial because very sophisticated co-operation is taking place across sectors to orchestrate cyber attacks.

The Office of Cyber Security and Information Assurance (OCSIA) already works with the Research Councils, the Technology Strategy Board and individual departments to try and ensure a co-ordinated approach to cyber research and development.[74] Meanwhile, the PCeU has been successfully using a Virtual Task Force concept to improve joint working. This currently has a finance industry focus, with partners from banking, payment services, telecoms and Internet Service Providers with Chatham House providing facilitation and academic rigour. The approach will be extended to other sectors such as retail and property.[75]

OCSIA's Deputy Director has indicated that different departments intend to work with different industries on cyber security. BIS will work with the telecoms sector, Treasury with the financial sector and DECC with the energy sector.[76]

The Director of GCHQ believes that the Centre for the Protection of National Infrastructure (CPNI) and existing Whitehall/industry bodies already provide a strong foundation for co-operation.[77] He has also commented that such co-operation may also need to stretch to new financial models to support a joint government and private sector capability to protect critical national infrastructure as well as greater inter-connection e.g. the sharing of real time data to enable swifter response to cyber attacks.[78]

The Cabinet Office has admitted that further work needs to be done to develop mechanisms to identify scientific and technical experts in industry and academia in relation to cyber attacks.[79] The OCSIA is developing a private sector engagement strategy and associated science and technology plan. The software suppliers have their own cross-industry initiatives such as the Advancement of security on the Internet (to respond to issues affecting multiple platforms) and Safecode (agreeing best practices for building software securely). The industry is also sharing information about the activities of cybercriminals and may collaborate to respond to particular threats.[80] Microsoft recently commented that collaboration is making it harder for criminals to attack as long as organisations are using the correct, up-to-date technology.[81]

---

73 Association of Police Officers (ACPO), *ACPO e-Crime Strategy*, May 2009

74 HC 499, *Scientific Advice and evidence in emergencies: Memorandum submitted by the Government Office for Science and the Cabinet Office*, 14 September 2010

75 Association of Police Officers (ACPO), *ACPO e-Crime Strategy*, May 2009

76 UK cybersecurity spending plans revealed, *ZdNet UK*, 20 April 2011

77 *GCHQ Press Release*, Director GCHQ, Iain Lobban, makes Cyber speech at the IISS, 12 October 2010

78 Ibid

79 HC 499, *Scientific Advice and evidence in emergencies: Memorandum submitted by the Government Office for Science and the Cabinet Office*, 14 September 2010

80 For example, the Conficker Working Group organised by Microsoft. *Conficker Working Group website,* Home Page [on 19 January 2011

81 Software producers collaborate to turn tide on cybercrime, *Computer Weekly*, 22-28 June 2010, p.6

Despite existing liaison structures, a greater variety of fora offering safe information exchange environments would be welcomed by many. EURIM (the Information Society Alliance of Parliamentarians, government and industry), has reported that concerns of state security, commercial advantage and reputation often hamper the necessary information exchange. [82] Intellect, the technology industry trade association, agrees and has also suggested the mandated sharing of some forms of information loss. Such loss is often not acknowledged or publicised because of the reputational repercussions for businesses.[83] Meanwhile, at EU level, the Commission is urging Member States to share information through the European Public-Private Partnership for Resilience (EP3R).[84]

Standards

The new programme does not refer to any particular initiatives relating to the role of security standards. However, this may be a useful area of discussion between industry and Government. A January 2011, OECD report on cyber security risks identified one of the key actions for Governments to take to tackle cyber security as:

> Use procurement power, standards-setting and licensing to influence computer industry suppliers to provide properly tested hardware and software. [85]

There are an array of standards for cyber security and national security and organisations can choose those which suit their business or any particular supply chain requirements set by the organisations that they do business with. Price Waterhouse Coopers has estimated that in the UK 40% of large organisations are being asked to demonstrate compliance with ISO 27001, part of the ISO 2700 family of standards which are internationally recognised models for informational security management outside of government.[86]

Intellect, a trade association for the technology industry, has suggested that it would be helpful to have some rationalisation of the cyber security standards used in the UK, favouring international benchmarks as so many organisations delivering ICT and cyber security solutions are international organisations, not headquartered in the UK. Intellect has also commented that Government itself uses an array of standards across departments.[87] Clearly, it is important that the standards most appropriate to need are employed but closer discussions on this topic with industry may identify opportunities for improved consistency.

The Government published its ICT Strategy in March 2011.[88] This undertakes to " develop an appropriate and effective risk management regime for information and cyber-security risks for all major ICT projects and common infrastructure components and services" within the next

---

82 EURIM (The Information Society Alliance), *Can Society afford to rely on security by afterthought not design? Status report and recommendations of the ISA (EURIM) subgroup on Security by Design*, October 2010, section 4.2 p.11.

83 *Intellect*, Improving cyber security partnerships: Government – industry information sharing mechanisms on cyber threats, November 2010

84 *Com (2010) 673 final*, Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 23 November 2010, p.11

85 *Sommer, P (London School of Economics) and Brown I (Oxford Internet Institute)*, Reducing systemic cybersecurity risk, OECD, January 14 2011, p.9

86 UK firms embrace ISO 27001 security standards, *Computing.co.uk*, 27 May 2010

87 *Intellect*, Improving cyber security partnerships: Government – industry information sharing mechanisms on cyber threats, November 2010, p.8

88 Cabinet Office, *Government ICT Strategy*, March 2011

6-12 months.[89] The strategy also states that the Government will be imposing compulsory open standards (publically available), starting with interoperability and security.[90]

Skills and education

The Cyber Security Programme is to include a programme of education and up-skilling for the public, businesses and those tackling cyber crime as part of a more preventative approach. A recent OECD report on reducing systemic cyber security risks highlighted education as a key element of cyber security policy:

> There will never be enough policing resource to investigate all computer-related criminal attacks. The public will have to continue to learn to protect itself – and that suggests a strong argument for some public funding for relevant user education.
>
> Many cyber attacks depend on the use of compromised personal computers. Improved public understanding of security therefore benefits governments as well as individuals and makes the task of the attacker more difficult.
>
> As with other forms of hazard where large sections of the public are likely to be affected, education is needed to help citizens appreciate that while the risks and the damage from them cannot be eliminated, they can very often be managed.[91]

The Deputy Director of OCSIA has indicated that funding from the cyber security pot will allow the Department for Business, Innovation and Skills to provide "clever strategic leadership" in developing cyber security capabilities in the private sector using incentives rather than regulation to improve information security.[92]

Professional skills

EURIM (the Information Society Alliance of Parliamentarians, government and industry) has identified a potential shortage of cyber security skills from information assurance to forensics to surveillance and electronic warfare. EURIM is seeking to organise educational and training programmes with parts of the industry that have agreed to work together.[93]

Baroness Neville-Jones recently agreed "we do not have enough people" in terms of the level of expertise that will be needed for both maintaining and developing systems.[94] In July 2010, the Government launched The Cyber Security Challenge, a series of national online games and competitions to "identify and nurture" the UK's future cyber security workforce. The Challenge is run by a management consortium of cyber security professionals across the public and private sectors and academia and is an approach which is already being tried in the USA. Prizes include internships at net security companies and funded courses at eminent institutions such as the SANS Institute.[95]

---

89 Cabinet Office, *Government ICT Strategy*, March 2011, p.17
90 Cabinet Office, *Government ICT Strategy*, March 2011, p.5
91 *Sommer, P (London School of Economics) and Brown I (Oxford Internet Institute)*, Reducing systemic cybersecurity risk, OECD, January 14 2011, p.88
92 UK cybersecurity spending plans revealed, *ZdNet UK*, 20 April 2011
93 Email from Philip Virgo to EURIM members of 29 October 2010 outlining new exercise on cyber skills
94 HL Deb 14 October 2010 c. 697
95 Cyber security Challenge website [on 19 January 2010]

Public and business awareness

The National Security Agency has commented that relatively few practitioners and security officers in large corporations, even internet providers, know what the normal configuration of their system is so that they can spot when there is anomalous behaviour.[96]

There are a number of organisations and initiatives already offering cyber security advice, some with Government support. For example, Click Clever Click Safe, the Information Commissioner's Office, and CPNI, getsafeonline.org. Specific advice is also often provided on the websites of banks, telecommunications operators, and retailers. Such advice is clearly available but, except for the CPNI, tends to be offered in the context of protecting individual interests rather than also highlighting the national security angle.

The European Commission wants Member States to ensure that people can easily report cyber crime incidents and the UK Government's new programme proposes a single contact point for such reporting. The Commission also wants Member States to ensure that citizens have easy access to guidance on cyber threats, how to detect them, and the basic security precautions that need to be taken.[97]

3 International co-operation

The new cyber security programme recognises that the interconnected nature of the cyber domain makes international co-operation vital. It particularly promotes co-ordination with the USA.

3.1 Europe

There are already numerous EU and International initiatives on cyber attack/cyber crime and critical infrastructure as well as individual agreements between nations as an extension of their existing security or co-operation agreements.[98] The SDSR refers to capacity building in other countries. A move supported by the House of Lords European Union Committee which concluded that all Member States have an interest in bringing the defences of the lowest up to those of the highest, making capability a legitimate area of concern at EU level.[99]

Council of Europe Convention on Cybercrime

The UK finally ratified the Council of Europe's 2001 Convention on Cybercrime (also known as the Budapest Convention) in May 2011 having signed in November 2001 and having already made some legislative changes in line with the convention.[100] The Convention requires that signatories have legislation creating criminal offences for certain acts relating to computers. These relate to matters such as: system misuse, illegal interference, fraud and copyright. The US (a non-member) ratified the Convention in 2006.

Communication on Critical Information National Infrastructure Protection

In 2009 the European Commission issued a communication setting out co-ordinated measures to protect Europe from large-scale cyber-attacks and disruptions. This was largely

---

96 HL Deb 14 October 2010 c.698

97 *Com (2010) 673 final*, Communication from the Commission to the European Parliament and the Council – The EU Internal Security Strategy in Action: Five steps towards a more secure Europe, 23 November 2010

98 For example, COM (2009) 149 final, Council Document 8375/09, *Communication on Critical Information National Infrastructure Protection. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*

99 House of Lords European Union Committee, *Protecting Europe Against large-scale cyber-attacks*, HL Paper 68, 2009-10, Summary, March 2010

100 CETS No 185, Convention on Cybercrime, Status as at 22 June 2011 [22 June 2011]

spurred by the cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.[101] Developments relating to this communication have been kept under review by the European Scrutiny Committees in the Commons and Lords.[102]

The Commission's recent progress against this Communication was reported by the Commons European Scrutiny Committee summarising a recent Commission update:[103]

- the **European Forum of Member States** (EFMS), which is said to have made significant progress in fostering discussion and exchanges between relevant authorities on good policy practices and to be acknowledged by Member States as an important platform for discussions and exchange of good policy practices;

- — the launch of the **European Public-Private Partnership for Resilience** (EP3R) as a Europe-wide governance framework for the resilience of ICT infrastructures, fostering the cooperation between the public and the private sectors on strategic EU security and resilience policy issues;

- — the development of a minimum set of baseline capabilities and services and related policy **Recommendations** for National/Governmental CERTs [Computer Emergency Response Teams] to function effectively and act as the key component of national capability for preparedness, information sharing, coordination, as the precursor of a network of well-functioning National/Governmental CERTs and, thereby, of a European Information Sharing and Alert System (EISAS) for citizens and SMEs, to be built with national resources and capabilities by 2013

As security is a shared responsibility, all Member States are also asked to ensure that their national measures and efforts will collectively contribute towards a coordinated European approach and to commit to: [104]

- — enhancing EU preparedness by establishing a network of well-functioning National/Governmental CERTs by 2012, thereby enhancing the development of a European Information Sharing and Alert System (EISAS) to the wider public by 2013;

- — a European cyber-incident contingency plan by 2012 and regular pan-European cyber exercises: ENISA (European Network and Information Security Agency] will work with Member States on the development of such a European cyber incident contingency plan by 2012. In the same timeframe, all Member States should develop regular national contingency plans and response and recovery exercises; and

- — coordinated European efforts in international fora and discussions on enhancing security and resilience of Internet: Member States should cooperate together and with the Commission on promoting the development of a principles or

---

[101] For example, COM (2009) 149 final, Council Document 8375/09, *Communication on Critical Information National Infrastructure Protection. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience*

[102] See for example, *House of Commons European Scrutiny Committee*, 27th Report of Session 2010-2012,Section 5, 4 May 2011

[103] *House of Commons European Scrutiny Committee*, 27th Report of Session 2010-2012,Section 5, 4 May 2011 summarising Com (2011) 163, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information*, *Infrastructure Protection "Achievements and next steps: towards global cyber-security*",31 March 2011,

[104] *House of Commons European Scrutiny Committee*, 27th Report of Session 2010-2012,Section 5, 4 May 2011, para 5.18

norms-based approach to the issue of the global stability and resilience of the Interne

The Commission wants to see these efforts extended to the international stage and has set out a number of actions to achieve this:

- — **promote principles for the resilience and stability of the Internet:** with other countries, with international organisations and, where appropriate, with global private sector organisations, and by using existing fora and processes, such as those related to Internet Governance;
- — **build strategic international partnerships:** based on ongoing efforts in critical areas, like cyber-incident management, including exercises and cooperation among CERTs, in which the engagement of the private sector, which operates on a global scale, is seen to be of paramount importance;
- — **develop trust in the cloud:** by strengthening discussions on the best governance strategies for emerging technologies with a global impact, such as cloud computing.

New directive on cybercrime

Following on from the Communication above, in September 2010, the European Commission has proposed a new Directive on cybercrime to deal with large scale cyber attacks and the co-ordination of Member State responses to them. The UK has opted in to this Directive which has yet to be ratified by the European Parliament.[105] The directive builds on an existing 2005 EU framework decision with which Britain was already compliant. It is also consistent with the Council of Europe convention on cybercrime.[106]

The Directive seeks to:[107]

- ensure that there is a basic set of agreed minimum rules in relation to online crimes and penalties across the EU that member states must build into their legislation.
- ensure that Member States respond quickly to requests from other member states for assistance in cybercrime cases.
- to address the threat from large-scale attacks on information systems by ensuring that member states have adequate legislation to allow the prosecution and punishment of those organising, committing or supporting large-scale attacks.
- tackling emerging new threats such as the creation of malicious software and other innovative tools that criminals have invented to commit offences.

3.2 European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (EINSA) was established in 2004 to enhance the capability of the EU, Member States and the business community to prevent, address and respond to network and information security problems. It acts as a centre of

[105] HoC Deb 3 February 2011 col 1051
[106] HC Deb 3 February 2011 col 1051
[107] Based on information provided in HoC Deb 3 February 2011 col 1051

expertise working between the public and private sectors and aims to be a European hub for the exchange of information and best practice in information security.[108]

ENISA is based in Crete (which has posed some staff recruitment and general co-ordination issues). Its latest mandate was up for renewal in March 2012 and has been extended for 18 months whilst the Commission agrees a regulation setting out a modernisation programme for its next five years.[109]

It is envisaged that under its new mandate, ENISA will engage EU Member States and private sector stakeholders in joint activities across Europe, such as cyber security exercises, public private partnerships for network resilience, economic analyses and risk assessment and awareness campaigns.[110]

EU Security Strategy in Action

A recent EU Security Strategy document, *The EU Security Strategy in Action: Five Steps towards a more secure Europe*, sets out a number of areas for co-operation and new structures for achieving capacity building in relation to information security. For example, a new European cyber crime centre is to be established within existing structures by 2013 as the focal point of Europe's efforts to fight cyber crime. The new centre is expected to co-operate with the ENISA and interface with a network of national/governmental Computer Emergency Response Teams (CERTs).

3.3 Role of Nato

The SDSR commits the UK to ensuring that NATO's new Strategic Concept (the document which sets out its approach and key security tasks) recognises "the importance of NATO's wider role in responding to new types of threat such as those from cyber attack".[111] NATO already has the authority to respond immediately to cyber-attacks on its Member States and to deploy support teams.[112] The NATO Summit in November 2010 agreed a new Strategic Concept which identifies cyber attacks as a key threat and recommends developing NATO's ability to prevent, detect and defend against cyber attacks.

A NATO cyber defence policy was adopted on 8 June 2011. NATO reports that this revised policy will:

> ...offer a coordinated approach to cyber defence across the Alliance with a focus on preventing cyber threats and building resilience. All NATO structures will be brought under centralised protection, and new cyber defence requirements will be applied. The policy clarifies political and operational mechanisms of NATO's response to cyber attacks, and integrates cyber defence into NATO's Defence Planning Process. The policy also sets the principles on NATO's cyber defence cooperation with partner countries, international organisations, the private sector and academia.

---

[108] ENISA website, *About ENISA* [on 22 June 2011]

[109] ENISA press release, *Agency Mandate prolonged by the Council*, 30 May 2011

[110] EUROPA press releases IP/10/1239, *Commission to boost Europe's defences against cyber-attacks*, 30 September 2010

[111] Cm 7048, *Securing Britain in an age of uncertainty: The Strategic Defence and Security Review*, HM Government, October 2010, p.62

[112] House of Lords European Union Committee, *Protecting Europe Against large-scale cyber-attacks*, HL Paper 68, 2009-10, March 2010, para 81

> In parallel to the policy, a cyber defence Action Plan has been agreed. The Action Plan will serve as the tool to ensure the timely and effective implementation of the policy.[113]

3.4 G8 initiatives

The G8 agreed a set of principles on Protecting Critical Information Infrastructures (CIIP) in 2003. These were very broad and support the requirements on the Council of Europe Cybercrime Convention (see above). They cover issues such as warning and training systems and co-ordinated legal measures.

The current French Presidency of the G8 is focusing on internet issues including security.[114]

3.5 United Nations

Cyber security is regularly discussed in UN fora. Most recently, in April 2010, the Russians proposed a global treaty on cybercrime but the EU and US, in particular, were not in favour as they are already signatories to the European Council's Convention on Cyber Crime. The 12th pentennial UN Crime Congress in Brazil agreed a compromise. A UN advisory committee is now considering conducting a study of cyber crime, legislation and law enforcement. [115]

[113] NATO press release, *NATO Defence Ministers adopt new cyber defence policy,* 8 June 2011
[114] G20-G8 France 2011, *Priorities of the French Presidency of the G8* [on 22 June 2011]
[115] UN rejects international cybercrime treaty, *Computer Weekly*, 20 April 2010

Appendix 1: Overview of current government responsibilities for cyber security

ROLE	BODY	REMIT
Policy co-ordination	The Office of Cyber Security and Information Assurance (OCSIA)	Based in the Cabinet Office and set up at the same time as CSOC (see below) to provide coherence and strategic leadership across the Government's cyber security policy interests. This includes horizon scanning to consider impact of an evolving cyber landscape for the UK's cyber security and working with partners across government to identify and implement the appropriate policy responses.
Strategic Analysis	The Cyber Security Operations Centre (CSOC) .	Established in September 2009 as part of GCHQ with staff from a range of government and other stakeholders. Provides a hub for strategic analysis of developments in cyberspace and improving the co-ordination of the UK's response to cyber incidents. CSOC's work aims to draw together a range of sources to enable a better understanding of the risks and opportunities of cyberspace, ensure information is coherently distributed to government, industry, international partners and the public and help inform strategic decision making.
Response and analysis	UK's Government Computer Emergency Response Team (GovCert UK)	Provide response and analysis to the public sector.
	MOD Computer Emergency Response Teams (CERTs)	MOD dedicated team
	Combined Security Incident Response Team (CSIRTUK)	Provide response and analysis to critical infrastructure providers.
Advice and Guidance	The Centre for the Protection of National Infrastructure (CPNI)	Provide advice and guidance on electronic attack/cyber attack to the critical national infrastructure and to government departments.
	CESG (the national technical authority for information assurance)	

Source: Information taken from HC Deb 9 February 2010 WA 108