House of Commons
Defence Committee

Defence and Cyber-Security

Sixth Report of Session 2012–13

Volume I: Report, together with formal minutes, oral and written evidence

Additional written evidence is contained in Volume II, available on the Committee website at www.parliament.uk/defcom

Ordered by the House of Commons to be printed 18 December 2012

HC 106 [incorporating HC 1881-i of Session 2010-12]
Published on 9 January 2013
by authority of the House of Commons
London: The Stationery Office Limited
£15.50

Defence Committee

The Defence Committee is appointed by the House of Commons to examine the expenditure, administration, and policy of the Ministry of Defence and its associated public bodies.

Current membership

Rt Hon James Arbuthnot MP *(Conservative, North East Hampshire)* (Chair)
Mr Julian Brazier MP *(Conservative, Canterbury)*
Thomas Docherty MP *(Labour, Dunfermline and West Fife)*
Rt Hon Jeffrey M. Donaldson MP (*Democratic Unionist, Lagan Valley*)
Mr Dai Havard MP *(Labour, Merthyr Tydfil and Rhymney)*
Adam Holloway MP (*Conservative, Gravesham*)
Mrs Madeleine Moon MP *(Labour, Bridgend)*
Penny Mordaunt MP *(Conservative, Portsmouth North)*
Sandra Osborne MP *(Labour, Ayr, Carrick and Cumnock)*
Sir Bob Russell MP *(Liberal Democrat, Colchester)*
Bob Stewart MP *(Conservative, Beckenham)*
Ms Gisela Stuart MP *(Labour, Birmingham, Edgbaston)*

Powers

The Committee is one of the departmental select committees, the powers of which are set out in House of Commons Standing Orders, principally in SO No 152. These are available on the internet via www.parliament.uk.

Publications

The Reports and evidence of the Committee are published by The Stationery Office by Order of the House. All publications of the Committee (including press notices) are on the internet at www.parliament.uk/parliament.uk/defcom.

The Reports of the Committee, the formal minutes relating to that report, oral evidence taken and some or all written evidence are available in a printed volume. Additional written evidence may be published on the internet only.

Committee staff

The current staff of the Committee are Alda Barry (Clerk), Judith Boyce (Second Clerk), Dougie Wands (Second Clerk), Karen Jackson (Audit Adviser), Ian Thomson (Inquiry Manager), Frances Haycock (Inquiries Assistant), Christine Randall (Senior Committee Assistant), Shane Pathmanathan (Committee Assistant), and Sumati Sowamber (Committee Support Assistant).

Contacts

All correspondence should be addressed to the Clerk of the Defence Committee, House of Commons, London SW1A 0AA. The telephone number for general enquiries is 020 7219 5745; the Committee's email address is defcom@parliament.uk. Media inquiries should be addressed to Alex Paterson on 020 7219 1589.

Contents

Report

		Page
	Conclusions and recommendations	**3**
1	**Introduction**	**9**
	The inquiry	10
	Nature of the threat	11
2	**MoD networks, assets and capabilities**	**15**
	Operating and defending the network	16
	Promoting good cyber-security practice throughout MoD	18
	Securing the supply chain	18
	Developing military cyber capabilities	20
	Structures within the MoD	22
3	**Military activity in cyberspace – conceptual framework**	**24**
4	**Relationships with allies**	**28**
5	**Resources and skills supporting military activity in cyberspace**	**30**
	Research and development	30
	People – skills and capability	32
	Reservists	34
	Finance	35
	Measuring progress	36
6	**Cyber-security across Government**	**38**
	Responsibility in the event of a major cyber-security incident	41
7	**Conclusion**	**43**
	Annex: List of Abbreviations	**44**
	Formal Minutes	**45**
	Witnesses	**46**
	List of printed written evidence	**46**
	List of additional written evidence	**46**
	List of Reports from the Committee during the current Parliament	**47**

Conclusions and recommendations

Introduction

1. There is a consensus that cyberspace is a complex and rapidly changing environment. In the remainder of this report, we consider the implications for UK defence and security. (Paragraph 23)

MoD networks, assets and capabilities

2. The evidence we received leaves us concerned that with the Armed Forces now so dependent on information and communications technology, should such systems suffer a sustained cyber attack, their ability to operate could be fatally compromised. Given the inevitable inadequacy of the measures available to protect against a constantly changing and evolving threat, and given the Minister for the Cabinet Office's comment, it is not enough for the Armed Forces to do their best to prevent an effective attack. In its response to this report the Government should set out details of the contingency plans it has in place should such an attack occur. If it has none, it should say so – and urgently create some. (Paragraph 28)

3. The MoD's most important cyber-security responsibility is to manage and protect the systems and networks on which the UK's Armed Forces depend. The Committee was impressed with the GOSCC as a model of how industry contractors with particular expertise can be integrated with MoD personnel, and reassured by the clarity with which its mission was communicated. It is clearly a world-class facility. Changes to the MoD's procurement function will also have a bearing on the responsibilities of Information Systems and Services as a whole, and we ask that the Secretary of State keep Parliament informed about the impact of such changes on ISS's cyber functions. (Paragraph 34)

4. The GOSCC constitutes a pool of expertise which can be drawn on to spread good 'cyber hygiene' and awareness of everyday threats throughout the Defence workforce. In its response to this report the MoD should explain how the GOSCC's capability and the experience of its staff can be linked to the responsibility of the DCOG for bringing cyber-security into the forefront of all Government does. We consider that the GOSCC should be held up as a Centre of Excellence to promote good practice within the MoD and other Government Departments. (Paragraph 35)

5. We appreciate the MoD witnesses' frank assessment of the work still to be done on securing its supply chain and industrial base. Despite this frankness, the witnesses gave the impression that they believed that an admission of the problem took them close to resolving the problem. It does not. It is imperative that we see evidence of more urgent and concrete action by suppliers to address this serious vulnerability, and of energy and determination on the part of the MoD to enforce this action. This evidence should include, for example, efforts to improve the technical processes involved, identification of adequate resources, and provision of training to address the human aspects of good cyber defence. (Paragraph 42)

6. We consider that the opportunity created by cyber tools and techniques to enhance the military capabilities of our Armed Forces should be explored thoroughly by the MoD. To this end, we support the use of National Cyber Security Programme funding for the purpose of developing such capabilities. In addition, the opportunity to draw upon capabilities from strategic partners, particularly the USA, should be fully exploited. (Paragraph 53)

7. Good cyber-security practice needs to permeate the whole of the MoD and the Armed Forces. It would be a cause for concern if different units were to compete for particular roles and resources, if lines of accountability were to be unclear, if they were to operate in silos that would obstruct the best use of skills across the organisation, or if policy were to become fragmented. (Paragraph 56)

8. The MoD's thinking on the best internal structures for cyber-security appears to us to be still developing, particularly as the Joint Forces Command becomes more established. Getting this right must be a top priority. We recommend that the MoD should report to Parliament regularly about proposed and actual changes to those structures, and improvements in delivery that come about as a result. (Paragraph 57)

9. At present the stated unifying role of the DCOG is more illusory than real, and among its long list of tasks are some which appear to overlap with those of the GOSCC or Information Services and Systems more generally. We urge the MoD to communicate its cyber-security structures a more comprehensible fashion, setting out strands of work and lines of accountability unambiguously. Only by doing this can we be assured that there is indeed clarity about roles and responsibilities within the MoD and the Armed Forces. We recommend, in particular, that the respective roles of the Chief Information Officer and the Joint Forces Commander are clarified in relation to cyber-security. (Paragraph 58)

Military activity in cyberspace – conceptual framework

10. Events in cyberspace happen at great speed. There will not be time, in the midst of a major international incident, to develop doctrine, rules of engagement or internationally-accepted norms of behaviour. There is clearly still much work to be done on determining what type or extent of cyber attack would warrant a military response. Development of capabilities needs to be accompanied by the urgent development of supporting concepts. We are concerned that the then Minister's responses to us betray complacency on this point and a failure to think through some extremely complicated and important issues. We recommend that the MoD makes development of rules of engagement for cyber operations an urgent priority, and that it should ensure that the necessary intelligence, planning and coordination functions are properly resourced. (Paragraph 67)

11. We recommend that the Government ensure that civil contingency plans identify the military resources that could be drawn upon in the event of a large-scale cyber attack, such as additional staff, planning resources or technical expertise. In its response to this report the Government should set out what work it is doing to identify the reliance of the Armed Forces on the integrity and resilience of the Critical National Infrastructure, the steps it has taken to ensure that the CNI will remain sufficiently

robust to meet the needs of the Armed Forces and its contingency plans for the event that any relevant part of the CNI should fail. (Paragraph 69)

Relationships with allies

12. We welcome the Government's decision to play a more active role in the future work of the NATO Cyber-Defence Centre of Excellence. We ask that the MoD keeps Parliament fully apprised of future decisions regarding participation in this and other international co-operative arrangements. (Paragraph 74)

Resources and skills supporting military activity in cyberspace

13. The rapidly changing nature of the cyber threat demands that a premium be placed on research and development to enable the MoD to keep pace with, understand and anticipate that threat. We recommend that this should be addressed. The Government should also make it a priority to develop robust protocols for sharing information with industry to allow expertise to be pooled, and we recommend that the MoD set out clearly in its response to this report how it will do so. (Paragraph 81)

14. We recommend that the 'Cyber Future Force' work focuses on the development of career structures for MoD and Armed Forces personnel that will allow them not only to develop, but build on, their cyber skills. The MoD may not be able to compete with the private sector on salary terms, but it must be able to give staff opportunities and responsibility as well as rewarding work. (Paragraph 90)

15. MoD thinking about how reservists will help to deliver cyber-security is evolving, with many issues to be resolved. Although we welcome the initial steps taken by the MoD to develop the Joint Cyber Reserve it is regrettable that information about its establishment was not shared with us during our evidence taking. As a consequence, we were unable to explore with Ministers the details of this important development. (Paragraph 93)

16. We recommend that the MoD should build on existing strengths in the ways reservists contribute to cyber-defence and operations, and to retain the particular reserve-led command structures that facilitate those contributions. If any new reserve structure is to succeed, it is important that reservists who work in the civilian world should play a part in its design. The close relationships that have been established with contractors at the GOSCC could provide an avenue for recruiting more reservists from those companies, and we recommend that the MoD prioritise, as part of Future Reserves 2020, a strategy for recruiting personnel with specialist skills from the private sector. (Paragraph 94)

17. We recommend that the MoD must be rigorous in ensuring that all cyber-security activity—legacy and routine work as well as new initiatives—is fully funded. We were encouraged by the then Minister for the Armed Forces' explanation that spending on cyber would be included as a matter of course in future programme budgets. Continued investment in skills and resources is vital. We seek the MoD's assurance that this will not in practice mean cuts in other areas. Quantifying the 'right' amount to spend on cyber-security is a challenge which the MoD must not shirk; military and wider Government intelligence capability depends on it. (Paragraph 99)

18. It is vital not only that the MoD and the Government have ways of measuring their own progress in cyber-security, but also of communicating that progress to Parliament and the public. We are pleased that the MoD is engaging with the challenge of devising appropriate metrics and measurements for assessing progress. We acknowledge the difficulty of this task, and look forward to seeing how pan-Government, international and cross-sector thinking influences the outcomes of this work. We recommend that the MoD should provide Parliament with a report on cyber incidents and performance against metrics on at least an annual basis. (Paragraph 102)

Cyber-security across Government

19. It is our view that cyber-security is a sufficiently urgent, significant and complex activity to warrant increased ministerial attention. The relevant minister should have the authority to direct government departments to take action if they are not performing as required. We also consider that the National Security Council should dedicate time, with the relevant minister in attendance, to consider cyber-security matters on a more regular basis. (Paragraph 113)

20. The National Cyber Security Programme requires robust governance and we note that the Minister for the Cabinet Office chairs the Programme Board. However, the Programme represents only the tip of the iceberg of the necessary cyber-security activity across government. High-profile and authoritative leadership is required for all such activity. (Paragraph 114)

21. In a previous inquiry we expressed concern that no one government department was identified to take immediate lead responsibility should there be a severe space weather event. The machinery in the event of a cyber attack appears to be under development, with an important role being played by the Cyber Security Operations Centre. However, before a 'lead Government Department' is identified for a particular cyber incident there is a potential gap during which the Cabinet Office has a coordinating role but the location of executive authority is not clear. It is vital that clear procedures are in place, and communicated, about how ownership of incident response is escalated when necessary from individual departments to higher, central authorities. We recommend that the National Security Council review these arrangements to ensure that the UK's response to major cyber-incidents is as streamlined, rapid and effective as it can be, and that a programme of regular exercises, involving ministers as well as officials, is put in place to test the arrangements. The MoD should also conduct exercises for its own internal arrangements and their interface with the rest of government. (Paragraph 120)

Conclusion

22. We recommend that the MoD and the National Security Council keep under review the delineation of the military role in national cyber-security, not with a view to expanding that role unnecessarily, but to ensure that threats are dealt with in the most appropriate and effective manner, and that the MoD can focus its resources accordingly. (Paragraph 122)

23. The cyber threat is, like some other emerging threats, one which has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation's security. The Government needs to put in place – as it has not yet done – mechanisms, people, education, skills, thinking and policies which take into account both the opportunities and the vulnerabilities which cyber presents. It is time the Government approached this subject with vigour. (Paragraph 123)

1 Introduction

1. The 2010 National Security Strategy (NSS) identified "hostile attacks upon UK cyberspace by other states and large-scale cyber crime" as one of four Tier One risks, explaining that "Government, the private sector and citizens are under sustained cyber attack today, from both hostile states and criminals."[1]

2. Recent examples of high profile cyber attacks include:

- the leaking of thousands of British email addresses and encrypted passwords, including those of 221 British military officials, 242 NATO staff, and staff of the Joint Intelligence Organisation;[2]
- a 'denial of service' attack on HSBC;[3] and
- the loss of £800 million in revenue by a British company following cyber attacks by a foreign state.[4]

3. In November 2011 the Government published the second UK Cyber Security Strategy (the first was in 2009), *Protecting and promoting the UK in a digital world*.[5] The Strategy has four main objectives:

1. The UK to tackle cyber crime and to be one of the most secure places in the world to do business in cyberspace;
2. The UK to be more resilient to cyber attacks and better able to protect our interests in cyberspace;
3. The UK to have helped shape an open, stable and vibrant cyberspace which the UK public can use safely and that supports open societies;
4. The UK to have the cross-cutting knowledge, skills and capability it needs to underpin all our cyber-security objectives.[6]

The Cyber Security Strategy emphasises the limits of the Government's powers to act in this arena, and the close collaboration that will be needed with industry and academia.

4. A National Cyber Security Programme (NCSP) has been launched under the management of the Office of Cyber Security and Information Assurance in the Cabinet Office, and the oversight of the Minister for the Cabinet Office. £650 million has been allocated to the NCSP over the period 2011–2015, of which 14% (£90 million) has been allocated to the Ministry of Defence, and 59% to the Single Intelligence Account. (The

1 Cabinet Office, A Strong Britain in an Age of Uncertainty: The National Security Strategy, Cm 7953, para 3.27

2 "Hackers expose defence and intelligence officials in US and UK", The Guardian, 8 January 2012

3 "Millions affected after cyber attack on HSBC", Daily Telegraph, 19 October 2012

4 "UK firm 'lost £800m to cyber attack'", The Independent, 26 June 2012

5 Cabinet Office, *UK Cyber Security Strategy*

6 Cabinet Office, *UK Cyber Security Strategy,* Executive Summary

Cabinet Office, Home Office, Business Innovation and Skills and Government ICT account for the remainder.)

5. The Strategy states that around half of the £650 million funding will go towards "enhancing the UK's core capability, based mainly at GCHQ at Cheltenham, to detect and counter cyber attacks. The details of this work are necessarily classified, but it will strengthen and upgrade the sovereign capability the UK needs to confront the high-end threat."[7]

6. In his evidence, Francis Maude MP, Minister for the Cabinet Office, commented that, in an "incredibly tight financial settlement generally, this was one of the few areas to which additional funds were apportioned, as a recognition that it was a growing threat".[8]

7. Asked what the £90 million set aside for the Defence Cyber Security Programme would be used for, Nick Harvey MP, then Minister of State for the Armed Forces, told us that the intention was to "mainstream cyber into all of our departmental business". He continued:

> It will be up to an SDSR and a National Security Strategy in 2015 to assess how far we have got and how much more of an investment we will need to make in it from there forward.[9]

The inquiry

8. This report is the second in a series examining what we have termed "developing threats", the first of which examined the risks posed by Electro-Magnetic Pulses.[10] Some of the themes of that inquiry—the need for a joined-up response across Government, and the vulnerabilities inherent in our ever-growing reliance on technology—feature in this report as well. We announced the following terms of reference on 19 January 2012:

- The nature and extent of the cyber-security threat to Ministry of Defence and Armed Forces systems, operations and capabilities;
- The implications of the 2011 UK Cyber Security Strategy for the Ministry of Defence; including:
  - the MoD's role in cross-governmental cyber-security policy and practice, including the protection of critical national infrastructure;
  - the relationship of MoD's actions and planning to the National Security Council, the Cabinet Office and GCHQ.
- How the Ministry of Defence and the Armed Forces are managing and planning responses to threats in the cyber domain; including:

7 Cabinet Office, *UK Cyber Security Strategy*, para 4.12

8 Q 140

9 Q 98

10 Defence Committee, *Developing threats: electro-magnetic pulses (EMP)*, Tenth Report of Session 2010-12, 22 February 2012

- skills, capacity and expertise within the MoD and the Armed Forces, including in research and development;
- how MoD and National Cyber Security Programme resources are being used to address cyber-security.

9. The full list of organisations from which we received written evidence is published at the end of the report, along with the list of those who gave oral evidence. We held three oral evidence sessions, including one, which focused on the role of the Cabinet Office, in which we took evidence from the Minister with overall responsibility for cyber-security across Government, Rt Hon Francis Maude MP. We also visited the Global Operations Security Control Centre (GOSCC) at MoD Corsham in Wiltshire, and benefited from a number of briefings by Ministry of Defence staff and Service personnel. We are grateful to all who assisted us in the course of our inquiry, to our Specialist Advisers, particularly Graham Wright, for their advice and insight, and to our staff.[11]

10. In this report we discuss first the two tasks which the MoD has told us are its principal cyber-security responsibilities: protecting its own networks in order to enable military operations, and developing cyber capabilities which could in future be used to enhance military operations. We then go on to consider some of the challenges which the MoD will need to address in order to fulfil those responsibilities, including the development of concepts and the provision of resources to support its cyber-activity. We offer our assessment of the progress the MoD is making towards tackling these challenges, indicating the areas in which it seems to us more rapid progress is required at this stage, and those to which we are likely to return in a future inquiry.

11. Finally, we consider the role of the MoD as part of the Government's wider approach to cyber-security. Threats to national security cross organisational boundaries, and in order to assess the effectiveness of one department's contribution, it is necessary to understand how it fits into the whole and how effective that whole is.

Nature of the threat

12. Professor Paul Cornish and colleagues, Chatham House, describe the nature of the threat:

> In cyberspace the boundaries are blurred between the military and the civilian, and between the physical and the virtual; and power can be exerted by states or non-state actors, or by proxy. [...] Cyberspace has made it possible for non-state actors, commercial organisations and even individuals to acquire the means and motivation for warlike activity.[12]

13. The UK Cyber Security Strategy notes that a number of different groups—criminals, terrorists, politically-motivated 'hacktivists', foreign intelligence services and militaries—are active today against the UK's interests in cyberspace, "but with the borderless and

11 For the interests of advisers, see Minutes of the Defence Committee, 13 July 2010, 13 September 2011, and 29 February 2012.

12 Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *On Cyber Warfare*, Chatham House (November 2010)

anonymous nature of the internet, precise attribution is often difficult and the distinction between adversaries is increasingly blurred".[13] Threats to security and information in the cyber domain include state-sponsored attacks, ideological and political extremism, serious organised crime, lower-level/individual crime, cyber protest, cyber espionage and cyber terrorism.

14. The UK Cyber Security Strategy states that:

> Some of the most sophisticated threats to the UK in cyberspace come from other states which seek to conduct espionage with the aim of spying on or compromising our government, military, industrial or economic assets, as well as monitoring opponents of their own regimes. 'Patriotic' hackers can act upon states' behalf, to spread disinformation, disrupt critical services or seek advantage during times of increased tension. In times of conflict, vulnerabilities in cyberspace could be exploited by an enemy to reduce our military's technological advantage, or to reach past it to attack our critical infrastructure at home.[14]

The Strategy notes that "some states regard cyberspace as providing a way to commit hostile acts 'deniably'. Alongside our existing defence and security capabilities, the UK must be capable of protecting our national interests in cyberspace."[15]

15. Techniques used by hostile actors in cyberspace are various: malicious software (malware), networks of 'botnets'[16] and 'logic bombs'[17] can be employed to navigate target systems, retrieve sensitive data or overrule command-and-control systems. GCHQ estimates that 80% or more of currently successful cyber attacks could be defeated by simple best practice, such as updating anti-virus software regularly.[18]

16. 'Advanced Persistent Threat' (APT) is the term used most often to describe subtle threats that are unlikely to be deterred by simple cyber hygiene measures[19]. Traditional 'boundary' defences may not be effective against "more subtle threats like APT and social engineering techniques"[20] such as manipulating people into performing actions which lead to confidential information being divulged.

17. Acts of aggression or malice in cyberspace differ from those in other domains. Cyberspace is regarded as an asymmetric domain, meaning that even adversaries of limited means can pose a significant threat to military capabilities. Attribution of attacks is difficult, time-consuming and sometimes impossible, as is discerning motives (some

13 Cabinet Office, *UK Cyber Security Strategy*, para 2.8

14 Cabinet Office, *UK Cyber Security Strategy*, para 2.5

15 Cabinet Office, *UK Cyber Security Strategy*, para 2.14

16 A network of private computers infected with malicious software and controlled as a group without the owners' knowledge, for example, to send spam.

17 A set of instructions secretly incorporated into a program so that if a particular condition is satisfied they will be carried out, usually with harmful effects.

18 Cabinet Office, *UK Cyber Security Strategy*, para 4.37

19 Cyber hygiene refers to steps that computer users can take to improve their cyber-security and better protect themselves online.

20 Ev w12, para 37

security breaches may owe as much to intellectual curiosity as intent to do harm). The then US Deputy Secretary of Defense William J. Lynn further wrote:

> In cyberspace, offence has the upper hand. The Internet was designed to be collaborative and rapidly expandable and to have low barriers to technological innovation; security and identity management were lower priorities. For these structural reasons, the US government's ability to defend its networks always lags behind its adversaries' ability to exploit US networks' weaknesses.[21]

18. The Intelligence and Security Committee in its Annual Report 2010–11 considered the activities of state actors in cyberspace:

> Cyber space means that countries no longer have to invest in global networks and pursue complex operations with high-level agents when it comes to espionage: they can access much of the same information using relatively inexpensive cyber attacks. The Director General of the Security Service told us in February 2011 that "the barriers to entry to cyber espionage are quite low. We have found a number of […] countries taking an interest in this".[22]

19. In evidence provided to that Committee, GCHQ had elaborated on the source of the threat:

> The greatest threat of electronic attack continues to be posed by State actors and, of those, Russia and China are [suspected of carrying out] the majority of attacks. [...]. Their targets are in Government as well as in industry. [...]. There are also a number of other states with credible electronic attack capabilities [...].[23]

20. We note the finding of the Intelligence and Security Committee that the main purpose of such attacks is espionage and the acquisition of information; however, there is a concern that this capability could be turned towards disruption activities – for example, interrupting supply of utility services.

21. The UK Cyber Security Strategy's executive summary states that:

> The networks on which we now rely for our daily lives transcend organisational and national boundaries. Events in cyberspace can happen at immense speed, outstripping traditional responses. Although we have ways of managing risks in cyberspace, they do not match this complex and dynamic environment. So we need a new and transformative programme to improve our game domestically, as well as continuing to work with other countries on an international response.[24]

22. Asked whether current cyber threats were containable, the Minister for the Armed Forces said:

---

21 William J. Lynn III (US Deputy Secretary of Defense), 'Defending a new domain', Foreign Affairs, September/October 2010

22 Intelligence and Security Committee Annual Report 2010-11, para 188

23 'Update on the Nature of the Threat Posed by Electronic Attack', Briefing provided by GCHQ, September 2010.

24 Cabinet Office, *UK Cyber Security Strategy*, Executive Summary

> I think that it would be bold to say that. It is a very fast-changing threat. We recognise how serious it is and that is why we give it the priority that we give it. [...] It is something to which we take a very cautious approach.[25]

23. **There is a consensus that cyberspace is a complex and rapidly changing environment. In the remainder of this report, we consider the implications for UK defence and security.**

25 Q 95

2 MoD networks, assets and capabilities

24. The increasing dependence of the Armed Forces on information and communication technology—in weapons systems, in satellite networks and in intelligence-gathering—introduces into operations many more points of vulnerability to cyber attack.[26] Symantec set out some of the ways in which cyber attackers could threaten or compromise military networks and operations:

> Depending on the motivation of the attacker, the objectives could range from traditional signalling intelligence, in which case the targeted systems are likely to be communication and information systems, all the way to the creation of a deceptive picture in the command structure, where sensor systems and observation systems such as radars or satellites, or even Command and Control systems, may be targeted. Attacking systems controlling the logistical supply may also be an option in order to limit and strain the regular supply of a running operation. Perhaps the most worrisome scenario of all is a cyber attack that could render dysfunctional main combat units such as airplanes or ships, or that could limit their operational capability or reliability. [...] Moreover the increased utilisation of robotic devices such as drones, battlefield robots and UAVs over the battlefield has numerous advantages, but also creates a new type of information security challenge that is not yet fully understood, studied or realised.[27]

25. The UK Cyber Security Strategy stated that "there can be no such thing as absolute security". The Government would, therefore, "apply a risk-based approach to prioritising our response."[28] General Shaw, Assistant Chief of Defence Staff, elaborated on what this meant in practice:

> All organisations and all people need to make a very severe and clear judgement on what is their vital information that they really want to lock away, and what level of risk they are prepared to take with all their information. [...] what you have is a graduated response, because you can't defend everything. You take risks on certain bits. That's how you cope with a penetrated system. [...] making very clear commanders' judgments about what information is vital and how tightly you are going to protect it, and what bits we are just prepared to operate.[29]

26. We asked General Shaw about the extent to which the Armed Forces retained the ability to operate in a compromised cyber environment. He stated that the UK had moved beyond "reversionary modes"[30], meaning that we could no longer depend on simple backup systems. However, Air Vice-Marshal Rigby, Director, Cyber, Intelligence and Information Integration, stated that: "In the Cold War we made sure that we could cope without our principal systems. We must have fall-back and contingency methods of

26 Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *On Cyber Warfare*, Chatham House (November 2010)

27 Ev w24

28 Cabinet Office, *UK Cyber Security Strategy*, para 3.2

29 Q 57

30 Q 61

operating, particularly in command and control."[31] We therefore asked the Minister for the Armed Forces how the MoD was mitigating the risks posed by the reliance on networked technologies. His answer focused on improving security measures rather than reverting to back-up non-networked technologies. He responded:

> Belt and braces and backups—sort of defence in depth, I suppose you would say. By working with intelligence and security agencies to assess the threat to our systems. By putting in place, as far as we can, technical measures to protect ourselves, restrict access and protect key data from compromise. By carefully segregating the most sensitive systems, carefully patrolling the links and gateways between different elements of systems and ensuring elements are completely autonomous. It is almost a sense of replicating in the cyber domain some of the approaches we would take to security in the physical space.[32]

27. Francis Maude MP, Minister for the Cabinet Office, told us that "One of the challenges is that we do not know what threat we will be facing next month, let alone in a year's time"[33].

28. **The evidence we received leaves us concerned that with the Armed Forces now so dependent on information and communications technology, should such systems suffer a sustained cyber attack, their ability to operate could be fatally compromised. Given the inevitable inadequacy of the measures available to protect against a constantly changing and evolving threat, and given the Minister for the Cabinet Office's comment, it is not enough for the Armed Forces to do their best to prevent an effective attack. In its response to this report the Government should set out details of the contingency plans it has in place should such an attack occur. If it has none, it should say so – and urgently create some.**

Operating and defending the network

29. Securing the networks on which UK military operations depend is the foremost cyber-security responsibility of the MoD. This role is not funded by the National Cyber Security Programme, as, in the words of James Quinault, Director, Office of Cyber Security and Information Assurance, Cabinet Office, it "ought to be business as usual for the MoD".[34] In 2010, the MoD put in place three 'network authorities' which have been assigned responsibilities for the governance and security of the networks on which the MoD and the Armed Forces depend. They are as follows:

- The Network Capability Authority – led by the Deputy Chief of Defence Staff (Capability), deals with the cyber-proofing and information requirements of future systems;

31 Q 63

32 Q 111

33 Q 153

34 Q 180

- The Network Technical Authority – develops technical solutions to meet capability requirements and ensures that systems and platforms linking with the Defence network are able to communicate and will not introduce vulnerabilities;
- The Network Operating Authority – provides day-to-day operational management of the defence network, monitoring and managing more than 750,000 configurable IT assets.[35]

30. The latter two are teams within Defence Information Systems and Services (ISS), part of Defence Equipment and Support, which provides the procurement and support functions for integrated information and communication services across the Armed Forces, the Ministry of Defence and to overseas bases, operations and ships. The Director of ISS reports to the Chief of Defence Materiel.

31. The Network Operating Authority, which delivers and operates the MoD's own networks and defends them from attack, is based within the Global Operations and Security Control Centre (the GOSCC). The rationale for combining the two roles of 'operating' and 'defending' the networks is not only that overlapping skills are needed, but that defenders need to have an in-depth understanding of how the network is used in order to identify abnormal performance which might indicate the presence of threats. They also need to be able to strike a balance between the two roles because "in general, networks that are optimised to support business needs are more vulnerable to cyber attack".[36] The Head of the GOSCC is empowered to take rapid action without direction from above to defend the network when necessary. The Centre is also responsible for ensuring that software applications, updates and patches are applied consistently across MoD networks.

32. Staff at the GOSCC are a mix of military, MoD civilian and contractor personnel from major industry partners involved in delivering and supporting the MoD network; these include Fujitsu, BT DFTS, Cassidian, EADS, Babcock and Paradigm.[37] These delivery partners have all been encouraged to establish their commercial Network Operating Centre or Security Operating Centre physically within the GOSCC.[38] Of the staff, only military personnel can be sent to operational theatres if the need arises.[39] A Joint Cyber Unit ("joint" meaning across all the three services, but also with links to GCHQ) has been established at the GOSCC; MoD has described the GOSCC's role as "to proactively and reactively defend MoD networks 24/7 against cyber attack to enable agile exploitation of MoD information capabilities across all areas of the Department's operations."[40]

33. Changes to structures elsewhere in the MoD, particularly the evolving role of Joint Forces Command and nature of Defence Equipment and Support, will have an impact on cyber functions in terms of who sets the requirements for and procures cyber capabilities

35 Q 82; see also MoD Defence ICT Strategy, October 2010; Ev 48-9

36 Ev 49

37 Ev 44

38 Ev 48

39 Q 87

40 Ev 44

and equipment, and their relationship to those who operate those capabilities and manage the networks that they use.

34. **The MoD's most important cyber-security responsibility is to manage and protect the systems and networks on which the UK's Armed Forces depend. The Committee was impressed with the GOSCC as a model of how industry contractors with particular expertise can be integrated with MoD personnel, and reassured by the clarity with which its mission was communicated. It is clearly a world-class facility. Changes to the MoD's procurement function will also have a bearing on the responsibilities of Information Systems and Services as a whole, and we ask that the Secretary of State keep Parliament informed about the impact of such changes on ISS's cyber functions.**

Promoting good cyber-security practice throughout MoD

35. Teams within the GOSCC have oversight of cyber-security housekeeping and hygiene issues: spotting missing patches to software and updating anti-virus measures, promoting the use of complex passwords, spreading awareness of how personal information or personal devices might be employed by cyber attackers, and running exercises to check on progress. 'Mainstreaming' of cyber-security throughout the MoD workforce is, however, also a responsibility of the Defence Cyber Operations Group (DCOG) (discussed later in this report). **The GOSCC constitutes a pool of expertise which can be drawn on to spread good 'cyber hygiene' and awareness of everyday threats throughout the Defence workforce. In its response to this report the MoD should explain how the GOSCC's capability and the experience of its staff can be linked to the responsibility of the DCOG for bringing cyber-security into the forefront of all Government does. We consider that the GOSCC should be held up as a Centre of Excellence to promote good practice within the MoD and other Government Departments.**

Securing the supply chain

36. Military operations depend not only on the security of networks, but the security of equipment and components and the supply chain which delivers them. The MoD therefore needs to have confidence in the resilience of its industrial base and supply chain to cyber attack. The UK Cyber Security Strategy and the "National Security Through Technology" White Paper published in February 2012 both committed the Government to raising the standard of cyber-security expected from suppliers of sensitive equipment.[41] The Cabinet Office has a supporting role in advising about the cyber-security aspects of acquisition, and the Department for Business, Innovation and Skills is working with GCHQ to develop a cyber kite-marking system for Government suppliers more generally.[42] However, it is the MoD's responsibility to manage relations with its own suppliers.[43]

37. BAE Systems warned that "the increasing use of Commercial Off-the-Shelf products and dependency on internet protocol (as opposed to proprietary) networks will have

41 MoD, National Security Through Technology: Technology, Equipment and Support for UK Defence and Security, Cm 8278, para 160; Cabinet Office, UK Cyber Security Strategy, para 4.5

42 Qq 216-7; Q 76

43 Q 214

brought a wider range of vulnerabilities into MoD systems, some of which will already be known to attackers."[44] Professor Sir David Omand, King's College London, argued that:

> there is a conflict for defence between the current fashion for buying things off the shelf at the cheapest price and taking the time and expenditure to write computer code that is genuinely secure. Somewhere, somebody in defence has to strike a balance between those two. [...] If we go about just buying stuff off the shelf, including computer software that has been bundled together from pre-existing blocks of software, then I am afraid we are making ourselves vulnerable.[45]

38. We asked MoD witnesses what cyber-security measures it requires its suppliers to take. The MoD's Chief Information Officer, John Taylor told us that:

> This is an area that we are giving increasing attention to. I am not convinced we have got this quite right yet. As you rightly say, we are very dependent on those suppliers. Having [...] got our own house in reasonable order, we are now starting to work particularly with our key suppliers to help them raise their game in this space. I am clearly not going to talk about any individual supplier but I think we are getting an understanding of what that landscape looks like.[46]

The Minister for the Armed Forces added:

> There is a mutual recognition of and understanding of the problem and a determination and will to help each other improve our defences. I think that the ingredients are there to get us to where we need to be, but it is a big task. As we have already commented a couple of times, there is an ever-changing, fast-evolving threat. You have to be very sure of yourself to say that you have cracked the problem.[47]

39. MoD witnesses described the range of factors that are balanced when decisions are made to procure equipment and network components 'off-the-shelf'. The Minister for the Armed Forces acknowledged there was a potential risk, but this had to be balanced with cost, speed and efficiency of delivery, the urgency with which the piece of kit is needed, "and the extent to which you have any known concerns about the product that the supplier is potentially going to supply to you. If it has any components that you have a concern about, you have quite a complex risk balance to perform."[48] He told us that "there is no reason why you wouldn't" use commercial off-the-shelf products in cyber-defence systems, subject to advice from the National Technical Authority about whether the specific product was appropriate for the job.[49]

40. The relationship of the MoD with its industrial suppliers also depends on robust and honest information-sharing about attacks and potential vulnerabilities. Contractors may in the past have been reticent for commercial reasons to admit to cyber-security incidents

44 DCS 006, para 6; DCS 011, para 16

45 Q 13

46 Q 76

47 Q 114

48 Q 115

49 Q 116

affecting their organisations, but MoD witnesses offered the view that such relationships are becoming more open, and contractors are increasingly willing to approach the MoD for help in the event of an incident.[50]

41. Under the UK Cyber Security Strategy, a pilot for a joint private-public sector forum for pooling threat information was established, defence being one of five sectors involved. In its first annual progress report on the Cyber Security Strategy, the Government reported that 160 companies had engaged successfully in the pilot. The Government, in conjunction with industry, is now developing a permanent information sharing environment called CISP (Cyber-security Information Sharing Partnership) to be launched in January 2013. Initially, this will be open to companies within Critical National Infrastructure sectors, but membership will be made available more broadly, including to SMEs, in a second phase.[51]

42. **We appreciate the MoD witnesses' frank assessment of the work still to be done on securing its supply chain and industrial base. Despite this frankness, the witnesses gave the impression that they believed that an admission of the problem took them close to resolving the problem. It does not. It is imperative that we see evidence of more urgent and concrete action by suppliers to address this serious vulnerability, and of energy and determination on the part of the MoD to enforce this action. This evidence should include, for example, efforts to improve the technical processes involved, identification of adequate resources, and provision of training to address the human aspects of good cyber defence.**

Developing military cyber capabilities

43. If the foremost responsibility of the MoD is to enable and protect military operations, its next most important role is to explore how military operations might be *enhanced* by exploiting cyber tools and techniques. Witnesses told us that 'cyberwar'—in the sense of a conflict entirely fought and decisively won in cyberspace—may be a distant prospect, but it was reasonable to expect the armed forces to explore how they might gain a military advantage by delivering effects through cyberspace.[52] Cyber can in this sense be regarded as a 'fifth domain' of warfare, presenting an opportunity as much as a threat, and the Minister (Nick Harvey) set out an aspiration for the UK's Armed Forces to do everything in cyberspace that they do in every other domain: prevent, deter, coerce or intervene.[53]

44. The development of military cyber-capabilities also requires substantial investment in research and intelligence. Witnesses emphasised the long lead-in times for cyber-weapons, and that the effectiveness of such weapons depends on intelligence and a willingness to tailor-make weapons particular to each target.[54] Professor Sir David Omand stated:

50 Q 114

51 Cabinet Office, Written Ministerial Statement, 3 December 2012

52 Qq 9-10; Q 31

53 Nick Harvey MP, speech at Chatham House, November 2010; Q 122

54 Q 60 and 65

> if you really want to knock out the enemy's air defence system, you are going to have to design something very specifically for that purpose.[55]

45. Talking about the Stuxnet worm[56] as an example of a cyber-weapon, John Bassett noted that:

> this is something that has clearly had a huge amount of intellectual capital poured into it. [...] it could only be used once for one thing, so we are really talking about almost hand-crafted weapons in that sense. This is not something where one can easily imagine a production line of high impact cyber-weapons.[57]

46. The Strategic Defence and Security Review stated that the Government would "work to develop, test and validate the use of cyber capabilities as a potentially more effective and affordable way of achieving our national security objectives".[58] The National Cyber Security Programme's funding to the MoD is partly to be used for the purpose of developing such capabilities.[59] Joint Forces Command is to take the lead in the "development and integration of defence cyber capabilities", but the main focus for this activity will be the Defence Cyber Operations Group (DCOG), which reports to the Joint Forces Commander.

47. The DCOG, due to be fully operational by March 2015, is a federation of cyber units working closely together to deliver a defence capability. It will mainstream cyber-security throughout the MoD and ensure the coherent integration of cyber activities across the spectrum of defence operations.

48. The role of the DCOG was described by MoD as to "ensure coherence across Defence planning for cyber operations and ensuring that commanders have situational awareness of the impact of cyberspace on their operations, and [are] able to use cyber tools and techniques to assist them in conducting successful operations."[60] General Shaw, Assistant Chief of Defence Staff, told us that: "What we have learned over the past year about the nature of operating in cyberspace means that the idea that we can just have cyber defence as one hived-off piece has been overtaken conceptually."[61] He argued that the military needed to reach the stage where "cyber is not seen as something separate". He continued:

> Cyber is just another effect, or rather, to put it another way, it is merely the latest medium through which to achieve effect. Therefore, all the normal effects that we try to achieve, and all the normal relationships that we have, suddenly have a cyber dimension to them or cyber ways of achieving them.[62]

---

55 Q 21

56 Stuxnet is a highly sophisticated computer virus (a complex computer code). First discovered in June 2010, Stuxnet spread via Microsoft Windows, and targeted Siemens industrial control systems, including those used in the energy sector to control nuclear and gas infrastructure.

57 Q 21

58 Strategic Defence and Security Review, 19 October 2010

59 Cabinet Office, UK Cyber Security Strategy

60 Ev 44

61 Q 38

62 Q 36; Q 43

49. The full list of tasks and responsibilities given to the DCOG is long and varied, and includes developing a recognised career structure in cyber, "agile procurement and rapid pull through of research and development", putting in place robust structures for intelligence support with GCHQ, and factoring in cyber resilience to all MoD equipment.

50. We were told by the MoD after the final evidence session that it is currently working on plans to form a Joint Forces Cyber Group (JFCyG), with the aim of bringing all aspects of cyber affecting operations under one unified command structure. The JFCyG will not replace the DCOG, but brings a number of the elements that previously existed within it together to improve coordination of effort and increase efficiency in operational planning.

51. A Joint Cyber Unit within DCOG—distinct from that based within the GOSCC—is to work with GCHQ on developing "new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace," and will be fully operational by 2015.[63] GCHQ is recognised as the pre-eminent national repository of expertise in the cyber field, and is, according to the Minister for the Armed Forces, "performing the central role that in some of our allied countries would be exercised somewhere within the defence arena".[64] General Shaw told us that:

> the British response to the cyber threat [...] is to create a national bucket of capability, from which everyone draws. [...] That one bucket of expertise is GCHQ. We are contributing personnel into it to ensure that in the development of cyber-capability there are military people there, both to add their expertise to that development and to give the military input on what sorts of effects we might be looking for in cyber-space.[65]

52. Air Commodore Bishop, Head of the GOSCC, explained that information and staff exchanges between the MoD and GCHQ were well developed, and included the sharing of "for want of a better word, our tradecraft: tactics, techniques and procedures, and the way we would address issues when they arise".[66] Air Commodore Bishop also assured us that command and control arrangements were "very clear".[67]

53. **We consider that the opportunity created by cyber tools and techniques to enhance the military capabilities of our Armed Forces should be explored thoroughly by the MoD. To this end, we support the use of National Cyber Security Programme funding for the purpose of developing such capabilities. In addition, the opportunity to draw upon capabilities from strategic partners, particularly the USA, should be fully exploited.**

Structures within the MoD

54. Structures and lines of responsibility within the MoD for cyber-security appear not yet to be set in stone. In mid-2012, MoD conducted a Directorate of Operational Capability

63 Ev 44

64 Q 81

65 Q 39

66 Q 78

67 Q 82

review of command and control "governance" and "the detailed relationships between the different components of the cyber world".[68] John Taylor, MoD Chief Information Officer, told us that this came about as a result of transformation processes within the MoD, notably the formation of the Joint Forces Command.[69] General Shaw, Assistant Chief of Defence Staff, described the purpose of the DOC audit as to consider "how we achieve unity". He also commented that the creation of the Joint Forces Command "instituted a new process, which has yet to be finally decided upon".[70]

55. The MoD has said that the DCOG, which is part of Joint Forces Command, would assist in concentrating all cyber expertise in one structure. There are, however, significant exceptions to this: the GOSCC, the Research and Development function at Porton Down, and "cyber policy" in MoD Main Building all remain outside the ambit of the DCOG. The logic for the organisational split between GOSCC and DCOG is not clear to us: the skills, techniques and tools required for network defence and for the development of capabilities overlap significantly. The relationship between the Chief Information Officer and the Joint Forces Commander has been described by the MoD as "operating together closely in a 'supporting' and 'supported' relationship to achieve a Single Information Enterprise across Defence", a description which does little to help us understand where responsibility ultimately lies.

56. **Good cyber-security practice needs to permeate the whole of the MoD and the Armed Forces. It would be a cause for concern if different units were to compete for particular roles and resources, if lines of accountability were to be unclear, if they were to operate in silos that would obstruct the best use of skills across the organisation, or if policy were to become fragmented.**

57. **The MoD's thinking on the best internal structures for cyber-security appears to us to be still developing, particularly as the Joint Forces Command becomes more established. Getting this right must be a top priority. We recommend that the MoD should report to Parliament regularly about proposed and actual changes to those structures, and improvements in delivery that come about as a result.**

58. **At present the stated unifying role of the DCOG is more illusory than real, and among its long list of tasks are some which appear to overlap with those of the GOSCC or Information Services and Systems more generally. We urge the MoD to communicate its cyber-security structures a more comprehensible fashion, setting out strands of work and lines of accountability unambiguously. Only by doing this can we be assured that there is indeed clarity about roles and responsibilities within the MoD and the Armed Forces. We recommend, in particular, that the respective roles of the Chief Information Officer and the Joint Forces Commander are clarified in relation to cyber-security.**

68 Q 36

69 Q 84

70 Q 36

3 Military activity in cyberspace – conceptual framework

59. If cyberspace is to be considered a 'fifth domain' of warfare, any military activity in that domain will require a firm basis in terms of doctrines, rules of engagement and clarity about when an Armed Forces contribution or lead is justified or expected. In 2010, Nick Harvey MP, then Minister of State for the Armed Forces, said that while cyber activity added a new dimension to conflict, "what it seeks to achieve should be subject to the same strategic and tactical thought as a conventional military operation."[71]

60. Whether the Armed Forces should engage in cyber warfare will depend on whether particular actions in cyberspace are considered to be acts of war. Symantec elaborated on some of the scenarios in which it might be difficult to decide whether or not a cyber-security incident was 'military' in nature:

> Is an attack on a defence contractor, for example, enough to justify involvement of the military on the basis of the fact that the compromise is likely to impact sensitive information of military interest? What would be the 'rules of engagement' that would trigger the involvement of the military? Would the involvement of the military be linked to a particular political context, for example escalating tensions with a particular country and the possibility of military confrontation when cyber attacks are attributed to that country? Or, would military involvement be linked to defending a specific target of military interest, such as the control of a weapons system? Would this extend also to systems that are critical to the performance of military operations but do not belong to the core of the military functions, for example parts of the national telecommunication network? Or would the military be involved in the case of a cyber attack that would not target defence assets but would be of such catastrophic proportion and effect for the nation that could constitute the equivalent of an armed attack? An example here could be the use of cyber attack to sabotage a nuclear power plant. These are very difficult questions to answer and policy makers may well need to leave open some of their options, because any of these possibilities, as well as others we cannot imagine, may lead to situations that justify the involvement and use of defence assets and ultimately of the MoD. [72]

61. As yet there is no internationally-accepted definition of a breach of sovereignty in cyberspace, nor is it clear what types of response would be deemed proportionate to particular types of breaches. Responses to cyber attack would not need to be themselves in the cyber domain—they could be economic, judicial or of a conventional military nature.

62. Addressing the "policy, doctrinal and legal basis surrounding the use of cyber tools and techniques" is one of the tasks that has been given to the Defence Cyber Operations Group (DCOG). Internationally, the NATO Co-operative Cyber Security Centre of Excellence in Estonia is working towards the production, in 2013, of a legal manual to cover such

71 Nick Harvey MP, speech at Chatham House, November 2010

72 Ev w27

issues.[73] We asked the Minister for the Armed Forces about the work that had been done on this issue in the MoD. He responded:

> For me, the law of armed conflict applies as much to cyberspace as it does to any other domain of operation. The principles of proportionality, discrimination and humanity apply to actions that we might take in this domain, as they do elsewhere. We should focus on the intent and the consequences, rather than the means of delivering the effect. [...] At this stage we have not sought to develop specific rules of engagement for cyber, but as our understanding of cyber-operations, their potential, their capabilities and the associated norms of behaviour develop and evolve, I could envisage us coming back to that and possibly devising specific rules of engagement at some point in the future.[74]

63. The Minister expressed confidence that no new legal code was needed to regulate military activity in cyberspace, including the potential application of Article 5 of the North Atlantic Treaty[75] to a cyber attack and the protection afforded to legal combatants: "we think that the application of existing law and norms of behaviour will serve us perfectly well"[76]. General Shaw, Assistant Chief of Defence Staff, argued that a cyber attack could be construed as an armed attack under Article 5 "if the effect of that attack is so severe that it is judged to be an Article 5 attack. [...] it is the effect that matters, not the means through which it is delivered."[77] John Taylor, MoD CIO, commented that the principal challenge was making judgements on proportionality.[78]

64. One of the military functions which the Minister foresaw the Armed Forces carrying out through cyber means was to deter attacks on UK national interests.[79] The UK Cyber Security Strategy noted that "with the borderless and anonymous nature of the internet, precise attribution [of attacks] is often difficult and the distinction between adversaries is increasingly blurred".[80] General Shaw told us:

> The deterrent value of cyber is overstated at the moment, because there are huge problems with attribution. To take the simple example of Estonia, to all intents and purposes, the attack on Estonia appeared to come from California. It makes it extremely difficult. Until you attribute it, until you can work out a proportionate response and definite intent, it is a murky area. We should be hesitant to leap straight to nuclear deterrent, to theology, and apply it to the world of cyber.[81]

---

73 NATO, The Tallinn Manual on the International Law Applicable to Cyber Warfare [draft]

74 Qq 123-5

75 Article 5 provides that if a NATO Ally is the victim of an armed attack, each and every other member of the Alliance will consider this act of violence as an armed attack against all members and will take the actions it deems necessary to assist the Ally attacked.

76 Q 124

77 Q 51

78 Q 129

79 Q 79

80 Cabinet Office, *UK Cyber Security Strategy*, para 2.8

81 Q 66

65. The then Minister for the Armed Forces, however, told us that "in terms of cyber attacks on networks, we can in many cases tell pretty much exactly where they have come from—not in all cases, by any means."[82] He saw no inherent problem in applying the concept of deterrence to cyberspace:

> Perhaps as we go forward and there are more cyber attacks, or attributable cyber attacks, and people gain a greater understanding of others' capabilities, that will, perforce, begin to play into the psychology and logic of deterrence.[83]

66. John Taylor acknowledged, however, that certainty in attributing attacks could take "two or three days", which poses challenges for a posture of "active defence".[84] General Shaw, when asked about planning assumptions for cyber, commented that:

> We will need very agile policy decision-makers to keep up with the reality of the threats facing us. [...] the threat is evolving probably faster, I would say, than our ability to make policy to catch up with it.[85]

67. **Events in cyberspace happen at great speed. There will not be time, in the midst of a major international incident, to develop doctrine, rules of engagement or internationally-accepted norms of behaviour. There is clearly still much work to be done on determining what type or extent of cyber attack would warrant a military response. Development of capabilities needs to be accompanied by the urgent development of supporting concepts. We are concerned that the then Minister's responses to us betray complacency on this point and a failure to think through some extremely complicated and important issues. We recommend that the MoD makes development of rules of engagement for cyber operations an urgent priority, and that it should ensure that the necessary intelligence, planning and coordination functions are properly resourced.**

68. The MoD and the Cabinet Office have been very clear that the MoD's cyber-security role is confined to defending its own networks and developing cyber capabilities: it does not have any sort of general responsibility for protecting national infrastructure, nor is it expected to take the lead in coordinating a UK response to a major cyber-security incident.[86] The former task is instead the preserve of the Centre for the Protection of National Infrastructure (CPNI), which is a government authority accountable to the Director General of the Security Service.[87] CPNI advises organisations in the national infrastructure—including those in the private sector—on reducing their vulnerability to a range of threats including cyber attack.[88] Some of the evidence we received, however, questioned whether the military role could be so tightly circumscribed. In its written submission, McAfee argued that a military interest in the cyber-defence of Critical

82 Q 134

83 Q 130

84 Q 134

85 Q 58

86 Q 180; Q 48

87 Ev 42, para 2.2

88 Cabinet Office, *UK Cyber Security Strategy*, para 4.19

National Infrastructure could be justified by the reliance of some MoD functions on that infrastructure, and by the potential of cyber attacks to "threaten real loss of property and life" by targeting those systems.[89]

69. MoD witnesses conceded that a cyber equivalent of 'military aid to the civil authorities' could be envisaged if the Government felt that military expertise was needed.[90] **We recommend that the Government ensure that civil contingency plans identify the military resources that could be drawn upon in the event of a large-scale cyber attack, such as additional staff, planning resources or technical expertise. In its response to this report the Government should set out what work it is doing to identify the reliance of the Armed Forces on the integrity and resilience of the Critical National Infrastructure, the steps it has taken to ensure that the CNI will remain sufficiently robust to meet the needs of the Armed Forces and its contingency plans for the event that any relevant part of the CNI should fail.**

89 Ev w18, paras 2.3-4; Ev w9, para 9; Ev w33, para 2.12

90 Q 48

4 Relationships with allies

70. In addition to its other tasks, the Defence Cyber Operations Group (DCOG) takes the lead in establishing links with "key allies" on cyber.[91] In March 2009, in the course of an inquiry into Russia's relationship with NATO, the Committee visited the NATO Co-operative Cyber-Defence Centre of Excellence in Tallinn, Estonia. In our report, we noted that the Centre did not receive core NATO funding, being funded instead by the contributions of sponsoring nations, and we asked the MoD to explain why the UK was not a sponsor.[92] In its response, the Government stated that it believed the best way of making use of its resources was to contribute to the work of the Centre by assisting with specific workstreams, rather than by attaching personnel permanently.[93] During oral evidence for this inquiry, we asked Francis Maude MP, Minister for the Cabinet Office, who had recently visited Estonia, and James Quinault, Director, Office of Cyber Security and Information Assurance, Cabinet Office, why the UK was still not a sponsor of the Centre. They replied that the Centre was developing "know-how and research" rather than being engaged in operations, which means that it is "not the place from which cyber-defence of NATO would be commanded".[94]

71. However, since the final oral evidence session, the MoD told us that, as the role of the Centre expands under the auspices of the NATO Cyber Defence Action Plan (CDAP), the MoD has decided, from 2013, to send a national representative and to pay the annual €20,000 subscription using funds from the Defence Cyber Security Programme (DCSP). It is proposed that the UK would initially make a two year commitment, with the intent to review ongoing participation. Long term, the MoD will have to make a decision on the continuation of funding once the DCSP ends.

72. Provision of a national representative will give the UK a seat on the Steering Committee with the opportunity to influence future work. This action will confirm UK commitment both to the Centre and to broader NATO Cyber Defence activity and, we understand, will be welcomed by close international partners, particularly the United States.

73. The UK also participates in the NATO Incident Response and Command Centre (a 'GOSCC' for Alliance operations) in Belgium, and pursues cyber work in collaboration with a number of allies, notably the United States and Australia, with whom a tri-lateral memorandum of understanding has been agreed.[95] Cyber is also a strand of the UK-France defence co-operation agreements. General Shaw told us that the UK found that "bilateral relationships are where you can make progress. [...] In terms of creating unified NATO

91 Ev 45

92 Defence Committee, Tenth Report of Session 2008-09, *Russia: a new confrontation?*, para 153

93 Defence Committee, Sixth Special Report of Session 2008-09, Russia: a new confrontation? Government response to the Committee's Tenth Report of Session 2008-09

94 Qq 231-2

95 Q 43

policy, I think that is a very slow boat indeed. That policy is coming along, like all NATO policy, at the speed of the slowest runner".[96]

74. **We welcome the Government's decision to play a more active role in the future work of the NATO Cyber-Defence Centre of Excellence. We ask that the MoD keeps Parliament fully apprised of future decisions regarding participation in this and other international co-operative arrangements.**

96 Q 43

5 Resources and skills supporting military activity in cyberspace

Research and development

75. A constant theme in the literature and comment about cyber-security is the rapid pace at which threats develop and evolve.[97] Professor Paul Cornish and colleagues, Chatham House, have written that:

> The pace of change can be so abrupt as to render the action/reaction cycle of traditional strategy out of date before it has begun. [...] It is as if a government operational analyst has been sent to observe the effects in battle of the flintlock musket, only to discover upon arrival that the Maxim gun has been invented.[98]

Not only does the technology develop rapidly, but, as John Bassett of RUSI said, "people are actually capable of using these things in unexpected and unforeseen ways very much sooner than the technology changes".[99] As noted earlier in this report, Francis Maude MP, Minister for the Cabinet Office, told us that "One of the challenges is that we do not know what threat we will be facing next month, let alone in a year's time" [100].

76. Professor Brian Collins, a former Chief Scientific Adviser in the Department for Business, Innovation and Skills and the Department for Transport, argued that the necessary tools are not yet in place across Government to understand and plan in this way:

> If I had suggested three years ago that people would be organising riots in the streets using Facebook, no one would have even understood what the words meant. Last summer, that is what we saw. Now, if you say to law enforcement or, indeed, maybe to parts of our military operations, 'Do you expect to see those sorts of applications being used to organise a significant threat to us?', I do not believe that we have the mechanisms in place *a priori*, as opposed to by way of response, to anticipate where some of those things may be hitting us.[101]

77. He went on to say that across government "there is maybe too much emphasis on the short-term tactical as opposed to the long-term strategic".[102] He continued:

> Tactically, I don't think we are in bad shape at all. However, to be in a situation in which you can anticipate where some of these things might be coming from is a combination of intelligence-gathering [...] together with some idea of where

97 Cabinet Office, *UK Cyber Security Strategy*, p.7; Q 6

98 Paul Cornish, David Livingstone, Dave Clemente and Claire Yorke, *On Cyber Warfare*, Chatham House (November 2010)

99 Q 18

100 Q 153

101 Q 18

102 Q 17

individuals or groups might be taking their thinking, when we would regard that as undesirable for us. That horizon-scanning function is a piece that I see missing.[103]

78. Francis Maude MP, Minister for the Cabinet Office, told us that he was confident that the Government had the capacity to keep up with the latest threats, pointing out, however, that the Cabinet Office proposals for civil service reform explicitly referred to the need to strengthen horizon-scanning across Government.[104] James Quinault said that "intelligence and anticipation of the threat" was a thread in many of the funding allocations that had been made from the National Cyber Security Programme, and had been a particular feature of the investment in GCHQ. Research strands in other departmental programmes relate to cyber-crime and e-business, where the objectives of attacks may differ, but much of the same technology is employed.

79. Similarly, Air Commodore Bishop, Head of the GOSCC, highlighted the value of the MoD sharing threat information and security techniques with industry, because the means of attack against both these targets were often the same.[105]

80. MoD evidence states that £80 million a year is being provided for research in the related areas of cyber and influence, through the Cyber and Influence Science and Technology Centre at Porton Down, by working with research councils, and by investing in pan-Government programmes that place work in universities and designate a number of universities as centres of excellence.[106] The MoD is also funding a programme of studies at Seaford House, London (part of the Defence Academy), to consider the future character of conflict, and the implications of the developing cyber-threat for the security environment.[107] When we invited the then Minister for the Armed Forces to comment on whether the proportion of the Ministry of Defence budget being spent on research and development was, at 1.2%, currently too low, he agreed.[108]

81. We have considered the issue of the percentage of the defence budget which is spent on research and development in the course of our inquiry into Defence Acquisition: there is general agreement that it is currently too low. This applies to cyber-security as much as to any other field. **The rapidly changing nature of the cyber threat demands that a premium be placed on research and development to enable the MoD to keep pace with, understand and anticipate that threat. We recommend that this should be addressed. The Government should also make it a priority to develop robust protocols for sharing information with industry to allow expertise to be pooled, and we recommend that the MoD set out clearly in its response to this report how it will do so.**

103 Q 14

104 Q 195

105 Q 105

106 Q 136 and Q 196

107 Q 105

108 Q 139

People – skills and capability

82. The UK Cyber Security Strategy noted that people with a deep understanding of cyberspace and how it is developing are currently "a scarce resource" across both Government and the business world, and set as one of its main aims the development of knowledge, skills and capability sufficient to underpin all the UK's cyber-security objectives.[109] 'Cyber Future Force' is one of four strands of work in the Defence Cyber Security Programme, and will design the cyber component of Future Force 2020. The MoD's intention is to "embed" cyber skills throughout Defence by 2015, and all MoD personnel will receive some degree of education in cyber awareness. Those in operational command roles will be trained to integrate the cyber domain with operations. Specialist training will be provided to those in dedicated cyber roles, and their skills will be recorded against a cyber competency framework on HR systems.[110] The MoD stated that it would "grow a cadre of dedicated cyber experts".[111]

83. We note a degree of concern expressed in evidence to our inquiry that the MoD does not have sufficient skills at its disposal in this area.[112] IT industry body Intellect stated that:

> The perception of industry is that the MoD does not appear to have sufficient skills available for modern cyber-based warfare. […] there may be scope for an enhanced military-industry partnership to address this capability gap. […] Intellect members commented that within MoD there are individuals with an extremely high level of cyber knowledge, however recent movements in personnel across Government have affected the MoD's cyber capacity.[113]

Intellect concluded that greater investment in education, both within academia and government, was necessary to ensure sufficient future capability.[114] Dave Clemente, a researcher at Chatham House, wrote:

> Some sensitive tasks cannot be contracted to foreign nationals, and it will be necessary to develop UK talent […]. Talent retention is a regular concern and one that is becoming more urgent. Cyber-security experts can earn far more in the private sector than in government, and more thought needs to be given to retaining and incentivising talent.[115]

84. John Bassett, RUSI, when asked what the MoD's priorities in cyber-security should be, responded:

> It is about ensuring that we have enough good people in the Ministry of Defence, other parts of Government, academia and industry, and I think that we do not have

109 Cabinet Office, *UK Cyber Security Strategy*, para 4.22

110 Ev 45

111 Ev 43, para 3.6

112 Ev w9-10, paras 15-16

113 Ev w3

114 Ev w3

115 Ev w2, paras 9-10

> anything like enough at the moment. I think that growing and skilling the people is, for me, the single most important thing for us to do.[116]

85. We observed during our visit to the GOSCC that the application of the usual length of Armed Forces rotation to a post in cyber-security results not only in churn, but in potential dissatisfaction for personnel who develop a cyber specialism but subsequently are given little opportunity to build on or pursue this. To counteract this, the GOSCC is not only actively searching for personnel throughout the Forces who may have the necessary skills or aptitude, it is trying to ensure that staff who develop those skills are tracked throughout their careers so that they can be re-deployed in this area if necessary. Air Commodore Bishop described the range of backgrounds that could be put to use in the Centre: "We are looking at people with intelligence backgrounds, we are looking at people with technical backgrounds and we are looking at people with police backgrounds, because there was always a forensic and potential police issue around some of the stuff that we do."[117] John Taylor explained that the MoD was "agnostic" about the paths individuals took into the cyber parts of the organisation, provided they had the skills and training needed to fulfil their role.[118]

86. Following our final oral evidence session, the MoD told us that it had recently implemented a new Cyber Skills Strategy, setting out the vision and strategic policy for generating and sustaining cyber skills across the Department.

87. Existing single Service training had been surveyed and tailored interventions delivered to enable a strong base level of cyber-security awareness to be adopted across the Service Commands and the MoD Civil Service. Initial training had been augmented so that the MoD may more easily generate suitable personnel for later employment as cyber specialists. Other training packages had also been reviewed and augmented.

88. Finally, we were told that the MoD had designed a new cyber competence framework, which was comparable with civilian industry frameworks. Through integration with the Joint Personnel Administration system (Military HR system), it will now be possible to identify, track and better manage suitably qualified and experienced cyber-security personnel.

89. High demand for these same skills in the private sector may give rise to problems with recruitment and retention. In the short term, the MoD is able to rely on the unique nature of the work it offers to attract and keep skilled personnel and the investment it is willing to make in training.[119] Similarly, Francis Maude MP argued that "By and large, brilliant people do not go and work at GCHQ for the money; they do it because it is fascinating and it is very big-picture, serious stuff."[120] However, it was acknowledged that an upturn in the

116 Q 32

117 Q 87

118 Q 91

119 Q 91

120 Q 226

economy could result in more severe challenges.[121] Air Commodore Bishop stated that, although competition for posts at the GOSCC was currently very stiff:

> It would be naive if we thought that, having got some of the best training in the world and then somebody offers a big fat pay cheque, people would not decide to go. We do lose some, but we don't lose very many. A lot of them stay because they do enjoy what they do, and they do have the authority to do the job they have been put in there to do.[122]

90. **We recommend that the 'Cyber Future Force' work focuses on the development of career structures for MoD and Armed Forces personnel that will allow them not only to develop, but build on, their cyber skills. The MoD may not be able to compete with the private sector on salary terms, but it must be able to give staff opportunities and responsibility as well as rewarding work.**

Reservists

91. One important means of securing expertise is through the recruitment of reservists. The Minister for the Armed Forces assured us that he was very interested in developing the potential for reservists to contribute in this area, as a way of complementing the skills that could be developed 'in-house'.[123] BAE Systems suggested that it would be possible for the private sector to deliver a "surge capacity" through a "cyber reserve".[124] We encountered at the GOSCC some enthusiasm for involving more reservists, with the caveat that they had to be available for substantial enough blocks of time to develop sufficient understanding of the normal functioning of the network. General Shaw alluded to a potential culture clash between the Armed Forces and the sort of individuals who might have the expertise the MoD most needs; he envisaged a national reserve:

> that really will attract people with ponytails and earrings and will not force them to go through the same military strictures that we conventionally think of, so that we pull in the people with the requisite talent to get involved in the national effort.[125]

92. Following our final oral evidence session, the MoD told us that it intends to develop a Joint Cyber Reserve whose function will be to provide support to the Joint Cyber Units at the GOSCC and GCHQ and Regular Information Assurance units across all three Services. It is envisaged that the Reserve will be established by the end of March 2013 with full operating capability to be achieved by April 2015.

93. **MoD thinking about how reservists will help to deliver cyber-security is evolving, with many issues to be resolved. Although we welcome the initial steps taken by the MoD to develop the Joint Cyber Reserve it is regrettable that information about its establishment was not shared with us during our evidence taking. As a consequence, we were unable to explore with Ministers the details of this important development.**

121 Q 91

122 Q 55

123 Q 90

124 Ev w10, para 16

125 Q 40

94. **We recommend that the MoD should build on existing strengths in the ways reservists contribute to cyber-defence and operations, and to retain the particular reserve-led command structures that facilitate those contributions. If any new reserve structure is to succeed, it is important that reservists who work in the civilian world should play a part in its design. The close relationships that have been established with contractors at the GOSCC could provide an avenue for recruiting more reservists from those companies, and we recommend that the MoD prioritise, as part of Future Reserves 2020, a strategy for recruiting personnel with specialist skills from the private sector.**

Finance

95. The funding provided by the national programme to the Defence Cyber Security Programme—£90m over the period to 2015—is being supplemented by the MoD itself to the tune of £30m in 2012–13. This funding is only for specific new strands of work and to improve broader "transformation".[126] General Shaw described the programme work as "merely the tip of the iceberg. Far greater than that is the bill that every department faces for looking after its own internal security of its existing systems."[127] Speaking before the announcement of Planning Round 2012 (PR12) spending plans, General Shaw commented:

> one of the greatest risks I see in the entire national response to the cyber-threat is an unbalanced response, where there is new money for new stuff, but departments, which are so strapped for cash, will not give sufficient priority to the security of legacy systems and new systems. That is a much bigger part of the iceberg underneath the water. That challenge exists for the MoD as well. Certainly, last year, in PR11, we bid for new money from defence for [that] other part of the cyber equation. We got nothing. This year, we made a more modest and more realistic bid—we hope.[128]

96. We were subsequently assured by the then Minister for the Armed Forces that, as part of the mainstreaming of cyber throughout Defence, it would henceforth be "ingrained" in all budgets:

> every time we are assembling budgets for any significant programme, this will be part and parcel of it [...] I am envisaging a time when this is so absolutely automatic to everything we do that all the programme budgets we devise to do anything will include ensuring that we have the necessary defences in place to guarantee and assure what we are doing.[129]

97. We were told that PR12 included a clearly identified stream of funds set aside to address resilience and security.[130] Francis Maude MP, Minister for the Cabinet Office,

126 Ev 43, para 3.1

127 Q 70

128 Q 70

129 Qq 100-1

130 Qq 103-4

argued that although it would always be possible to dedicate even more funds to cyber-security, deciding how much was the right amount to spend was not "a perfectly judged and precise science". Given the number of competing claims for the money, Mr Maude argued that it was necessary to pitch spending at a point beyond which additional expenditure would not confer proportionate additional protection.[131]

98. We also noted the findings of the Intelligence and Security Committee in its Annual Report 2011–2012 regarding Defence Intelligence:

> Defence Intelligence (DI) is part of the Ministry of Defence (MoD) and is mostly funded from within the MoD budget. DI provides strategic intelligence to inform MoD policy and procurement decisions and tactical and operational intelligence to support military operations overseas. However, large parts of its strategic analysis work also support wider government – and particularly the Joint Intelligence Committee – and so it has a national role to play alongside the three main intelligence and security Agencies. Indeed, DI has the largest pool of all-source analysts in government.[132]

99. **We recommend that the MoD must be rigorous in ensuring that all cyber-security activity—legacy and routine work as well as new initiatives—is fully funded. We were encouraged by the then Minister for the Armed Forces' explanation that spending on cyber would be included as a matter of course in future programme budgets. Continued investment in skills and resources is vital. We seek the MoD's assurance that this will not in practice mean cuts in other areas. Quantifying the 'right' amount to spend on cyber-security is a challenge which the MoD must not shirk; military and wider Government intelligence capability depends on it.**

Measuring progress

100. We were keen to establish what measures might reasonably be used, in the MoD, in Government more generally, and by us to assess progress and effectiveness in cyber-security. Such measures are crucial to deciding whether money has been spent intelligently and efficiently. However, our witnesses agreed that developing metrics in this area was extremely difficult, particularly if what was sought were concrete outcome measures rather than inputs.[133] Air Vice-Marshal Rigby, Director, Cyber, Intelligence and Information Integration, even suggested that it could be a waste of time to try to identify any, although he believed that a range of input measures could be of value: personnel trained to a particular standard, or the inclusion of cyber in contingency plans, for example.[134] Although information is held on how many attacks have been thwarted, there is always the possibility—even likelihood—of some attacks going undetected, and the extent and nature of the damage averted by thwarting attacks is difficult to judge.[135] Comparisons with business or other institutions are made difficult by the relative attractiveness of Defence

131 Q 194

132 Intelligence and Security Committee, Annual Report 2011-12, Cm 8403, para 174

133 Q 44

134 Qq 45-6

135 Q 221 and Q 222

and the Government as a target and the sensitivity of the information that needs to be protected.[136] James Quinault, Director, Office of Cyber Security and Information Assurance, Cabinet Office, explained that it was relatively straightforward to tell whether the funding provided by the National Cyber Security Programme was being spent on the desired activity:

> but what is less clear, as the Minister [Francis Maude] said, is whether overall that is making the dent in the outcome that we want to see, with the overall problem. The problem there is that we do not have a baseline, we do not know how big the problem is that we are trying to shrink. We are working on that, but if we had waited to solve it before we cracked on, we would be further behind the curve than we are.[137]

101. The development of metrics is being worked on across Government, led by the MoD's CIO, John Taylor.[138] Mr Taylor told us:

> we are doing some work on metrics to give us positive evidence that we are as safe as we need to be. That involves looking at metrics in the business infrastructure space, making sure that we understand what assets we have and that we have processes that review information risk on a regular basis. We then need to look in the technology space, making sure that our information is backed up, that we have up-to-date antivirus software—all the hygiene things that you need to do. Then there is the people space—for example, is our security vetting process working properly?[139]

102. **It is vital not only that the MoD and the Government have ways of measuring their own progress in cyber-security, but also of communicating that progress to Parliament and the public. We are pleased that the MoD is engaging with the challenge of devising appropriate metrics and measurements for assessing progress. We acknowledge the difficulty of this task, and look forward to seeing how pan-Government, international and cross-sector thinking influences the outcomes of this work. We recommend that the MoD should provide Parliament with a report on cyber incidents and performance against metrics on at least an annual basis.**

136 Q 110

137 Q 222

138 Q 45

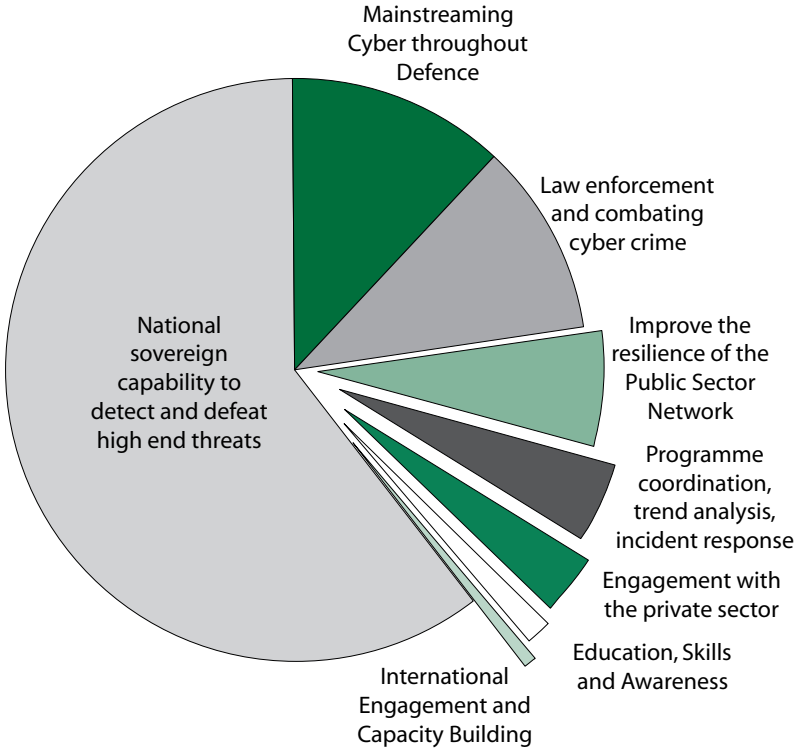
139 Q 70

6 Cyber-security across Government

103. The National Cyber Security Programme (NCSP) was launched in October 2010 (for more details see paragraphs 4 to 7 of this report).

104. In its first annual progress report on the National Cyber Security Strategy, the Cabinet Office reported on how the £650 million allocated to the NCSP had been spent so far.[140]

How the National Cyber Security Programme money has been spent



Source: Cabinet Office, Progress against the Objectives of the National Cyber Security Strategy – December 2012

105. Outturn and forecast spending in the first two years of the NCSP was as follows:

- National sovereign capability to detect and defeat high end threats (Security & Intelligence Agencies, £157M)[141]
- Mainstreaming Cyber throughout Defence (MoD, £31M)
- Law enforcement and combating Cyber Crime (Home Office, £28M)
- Engagement with the private sector (BIS, £17M)
- Improving the resilience of the Public Sector Network (Cabinet Office, £12M)

140 Cabinet Office, Progress against the Objectives of the National Cyber Security Strategy – December 2012

141 A breakdown of 'sovereign capability' spend in the Intelligence Agencies is not provided for reasons of national security, but the capability this buys supports activity across all strands of the Programme.

- Programme coordination, trend analysis and incident management / response (Cabinet Office, £9M)
- Education, skills and awareness (Cabinet Office, £4M)
- International engagement and capacity building (FCO, £2M)
- TOTAL = £260M[142]

106. The fact that many Departments have an interest in aspects of cyber-security means it is important to establish who bears responsibility for what elements of the agenda (beyond all agencies having a responsibility to protect their own data and systems). This is necessary in order to limit duplication, minimise the chance of gaps developing, and ensure that each Department is clear about its mission.

107. The Intelligence and Security Committee in its 2010–11 Annual Report identified 18 departments, units or agencies with particular responsibilities for aspects of cyber-security, spread across the intelligence and security Agencies, law enforcement, and other government departments including the Home and Foreign Offices, MoD and BIS. That Committee expressed concerns about "structural issues", noting that between them these 18 bodies:

> cover policy, management, intelligence operations, protective advice, detection and analysis, with some focused on crime, some on hostile activity from overseas, some on counter-terrorism and others covering all three. This risks duplication and confusion and cannot be cost-effective.[143]

108. When we put these concerns to Francis Maude, he responded, "It may not be particularly tidy, but we are getting quite a lot done in rather an effective way. [...]I would be concerned if there were only a few departments that had any interest in this, and if they rigidly stuck to concerning themselves only with what lay within their narrowly-drawn boundaries. This is very far-reaching, and it is changing all the time."[144]

109. Located in the Cabinet Office, the Office for Cyber Security and Information Assurance coordinates cyber-security activity across Government and administers the National Cyber Security Programme under the oversight of the Minister for the Cabinet Office. The Minister chairs the Programme Board, and the Government's Chief Information Officer reports to him, as does the Ministry of Defence CIO, John Taylor, on the specific project of the public sector network. Francis Maude MP explained to us that he did not have the authority to instruct officials in other Departments, but that the Programme Board held Departments to account for their delivery and spending under the NCSP.[145] The Cabinet Office has executive authority for certain aspects of this work, for example the identity assurance programme, but in other respects, Francis Maude told us,

142 Cabinet Office, Progress against the Objectives of the National Cyber Security Strategy – December 2012

143 Intelligence and Security Committee, Annual Report 2010-11, para 12

144 Q 151 and Q153

145 Q 167 and Q 198

"responsibility, very properly, is spread across the Government".[146] James Quinault outlined why the Cabinet Office's role was to coordinate rather than direct:

> we see this absolutely as not just a Government and military issue. It touches everything in life, not just everything in Government, which is precisely why the approach to it has to be one of coordinating activity, rather than directing it all from the centre. If you want to reach business, the business Department needs to be mainstreaming this into its other communications with business. [...] It has to lead on that. That cannot be done from the Cabinet Office.[147]

110. It is the National Security Council (NSC) which identified cyber-security as one of the four most important risks to the UK's national security. The head of the Office for Cyber Security and Information Assurance reports to the deputy National Security Adviser. However, we were told that it was discussed by the NSC as a discrete subject perhaps only two or three times a year and that a session dedicated to the topic in the autumn of 2012, would be the first such meeting.[148] An 'ad hoc' cross-Whitehall ministerial group, chaired by the Foreign Secretary and including Ministers with a cyber-security responsibility in their portfolio, meets roughly every six weeks, and is complemented by a similar officer group.[149]

111. Professor Brian Collins, Chair of Engineering Policy, UCL, commented on a potential weakness of the UK Cyber Security Strategy:

> History shows us that continuity of stewardship of strategies of this nature is quite difficult to achieve through our democratic process. [...] Unless we maintain that stewardship over a period that is much longer than the five-year electoral cycle, we will fail to deliver the desired outcomes.[150]

112. There is no Minister dedicated to cyber-security; it is one of the responsibilities of the Minister for the Cabinet Office. In the past, ownership of the issue has been vested in ministers of more junior rank, but who had fewer diverse responsibilities to attend to. Francis Maude put it to us that it was important for cyber-security to be represented by a senior figure with authority to operate across many Departments.[151] However, he estimated that some 25-30% of his time was spent on cyber-security, and he described the breadth of his portfolio as that of "Minister for everything else".[152]

113. **It is our view that cyber-security is a sufficiently urgent, significant and complex activity to warrant increased ministerial attention. The relevant minister should have the authority to direct government departments to take action if they are not performing as required. We also consider that the National Security Council should**

146 Q 145

147 Q 179

148 Qq 168-74

149 Q 174

150 Q 5

151 Q 149

152 Q 147

dedicate time, with the relevant minister in attendance, to consider cyber-security matters on a more regular basis.

114. **The National Cyber Security Programme requires robust governance and we note that the Minister for the Cabinet Office chairs the Programme Board. However, the Programme represents only the tip of the iceberg of the necessary cyber-security activity across government. High-profile and authoritative leadership is required for all such activity.**

Responsibility in the event of a major cyber-security incident

115. EADS stated in its memorandum to this inquiry that "at present it is not clear who owns the coordinated response to a national cyber-security incident"[153]. The Institute for Security and Resilience Studies argued that:

> There are outstanding practical questions about the coherence of activities in the wake of the 2011 UK Cyber Security Strategy. For example, at the cyber summit hosted by the Foreign Secretary in November last year the French had a clear answer to the question "who would you call in the event of a cyber incident?" It is their Prime Minister. This answer resolves the geographic and thematic contradictions cyber crises can otherwise precipitate. During the conference the answer for the UK was unclear. Subsequently it was said to be the Minister for the Cabinet Office, Francis Maude. Whilst he attends Cabinet, is at the centre of UK Government and can act with the authority of the Prime Minister, it is not clear his post commands the capabilities necessary to be the Lead Government Department.[154]

116. The Institute also said that it would be difficult to imagine international crises not being handled by the Foreign Secretary, internal crises by the Home Secretary, or incidents in the financial sector pointing to the Chancellor, but that what it calls "the Lead Government Department question" "could create unnecessary duplication of capabilities among government departments".[155]

117. The then Minister for the Armed Forces, Nick Harvey MP, said:

> I think that an analogy might be drawn with the COBR principle. When there is some sort of an incident anywhere within Government, the Cabinet Office has this COBR capability that kicks in. In and of itself, it does not have a great organisational empire at its disposal, but it has a coordinating role among other Government Departments, which have the mechanical functions. In a sense, I think, in the cyber sphere, the small unit in the Cabinet Office operates somewhat similarly. The principal levers at their disposal actually reside in GCHQ. That is where the serious firepower would come from to deal with things in a practical sense.
>
> In the event of some sort of cyber attack against the Government, the coordinating role for a response will be exercised by the Cabinet Office. [...] Depending on the

153 Ev w12, para 30

154 Ev w32, paras 2.8-2.9

155 Ev w32, paras 2.9-2.11

> precise nature of the attack and which parts of the Government networks were subject to the attack, a lead Government Department would be appointed. Other Government Departments would render any assistance that they could. [...] Depending on the scale and severity of the attack, it might well be that COBR would meet and bring together Ministers and/or officials from the relevant Departments to coordinate the Government's response.[156]

118. Asked who would take the lead, and on whose authority, in the event of a major cyber attack on the UK, Francis Maude replied:

> It depends on the scale and the nature of it. If it is deemed essential—if it is of a scale that it cannot be dealt with just by the Cyber Security Operations Centre at Cheltenham—then it would come up to the Cabinet Office. If it was of sufficient scale, it could lead to COBR being convened at different levels, depending on the scale, with different Departments, potentially, in the lead, depending on what it was. If it was an attack on the energy infrastructure, for example, unless it was at a level where the Prime Minister would want to chair it, you would ordinarily expect the Energy Secretary to chair COBR. Similarly, if it was an attack on transport infrastructure, the Transport Secretary would, and so on. [...] If something looked like it could be a sovereign attack, that would clearly be for the Prime Minister.

119. James Quinault described the role of the Cyber Security Operations Centre (CSOC) as: "monitoring and triaging incidents and making sure there is a single version of the truth for Government to act on".[157] CSOC is hosted by and reports to GCHQ rather than the Cabinet Office.[158]

120. **In a previous inquiry we expressed concern that no one government department was identified to take immediate lead responsibility should there be a severe space weather event.[159] The machinery in the event of a cyber attack appears to be under development, with an important role being played by the Cyber Security Operations Centre. However, before a 'lead Government Department' is identified for a particular cyber incident there is a potential gap during which the Cabinet Office has a coordinating role but the location of executive authority is not clear. It is vital that clear procedures are in place, and communicated, about how ownership of incident response is escalated when necessary from individual departments to higher, central authorities. We recommend that the National Security Council review these arrangements to ensure that the UK's response to major cyber-incidents is as streamlined, rapid and effective as it can be, and that a programme of regular exercises, involving ministers as well as officials, is put in place to test the arrangements. The MoD should also conduct exercises for its own internal arrangements and their interface with the rest of government.**

156 Q 75 and 80

157 Q 186

158 "GCHQ to host UK Cyber Security Operations Centre", GCHQ, 26 June 2009, http://www.gchq.gov.uk/Press/Pages/Cyber-Security-Operations-Centre.aspx

159 Defence Committee, Tenth Report of Session 2010-12, Developing Threats: Electro-Magnetic Pulses (EMP) HC 1552

7 Conclusion

121. Within the complex landscape of cyber-security threats and responses, it is imperative that each agency, department and Minister knows what it is that they are responsible for, either uniquely or in partnership with others. This role must be articulated clearly and understood fully in government at large. The amorphous, boundary-less nature of cyberspace, and the specific skills and capabilities needed to operate within it, mean that responsibilities which apply in the physical sphere cannot simply be read across to the analogous activity in the cyber sphere.

122. We welcome the Government's commitment to foster a vibrant and innovative cyber-security sector in the UK including a distinct role for the MoD to deliver military capabilities both to confront high-end threats and to provide potential offensive capability. However, we are concerned that in the long term, under unforeseen circumstances, such a narrow role might prove untenable. Our national understanding of 'defence' has widened to encompass a range of security threats not traditionally within the purview of the Armed Forces, and the same may be true of the cyber domain. For this reason, we consider that the Government as a whole needs to base decisions about responsibilities on a clear and conscious rationale, and be prepared to re-examine those decisions as events warrant. **We recommend that the MoD and the National Security Council keep under review the delineation of the military role in national cyber-security, not with a view to expanding that role unnecessarily, but to ensure that threats are dealt with in the most appropriate and effective manner, and that the MoD can focus its resources accordingly.**

123. **The cyber threat is, like some other emerging threats, one which has the capacity to evolve with almost unimaginable speed and with serious consequences for the nation's security. The Government needs to put in place – as it has not yet done – mechanisms, people, education, skills, thinking and policies which take into account both the opportunities and the vulnerabilities which cyber presents. It is time the Government approached this subject with vigour.**

Annex: List of Abbreviations

BT DFTS	BT Defence Fixed Telecommunications Service
CDAP	Cyber Defence Action Plan
CIO	Chief Information Officer
COBR	Cabinet Office Briefing Room
CPNI	Centre for the Protection of National Infrastructure
CSOC	Cyber Security Operations Centre
DCOG	Defence Cyber Operations Group
DCSP	Defence Cyber Security Programme
DI	Defence Intelligence
DOC	Directorate of Operational Capability
EADS	European Aeronautic Defence and Space Company
GCHQ	Government Communications Headquarters
GOSCC	Global Operations and Security Control Centre
ISS	Information Systems and Services
JFCyG	Joint Forces Cyber Group
MoD	Ministry of Defence
NATO	North Atlantic Treaty Organisation
NCSP	National Cyber Security Programme
NSC	National Security Council
NSS	National Security Strategy
PR12	Planning Round 2012
SDSR	Strategic Defence and Security Review
UAV	Unmanned Aerial Vehicle

Formal Minutes

TUESDAY 18 DECEMBER 2012

Members present:

Mr James Arbuthnot, in the Chair

Mr Julian Brazier	Mrs Madeleine Moon
Mr Thomas Docherty	Sir Bob Russell
Mr Jeffrey M. Donaldson	Bob Stewart
Mr Dai Havard	Ms Gisela Stuart

Draft Report (*Defence and Cyber-Security*), proposed by the Chair, brought up and read.

Ordered, That the draft Report be read a second time, paragraph by paragraph.

Paragraphs 1 to 123 read and agreed to.

Annex agreed to.

Resolved, That the Report be the Sixth Report of the Committee to the House.

Ordered, That the Chair make the Report to the House.

Written evidence was ordered to be reported to the House for printing with the Report, together with written evidence reported and ordered to be published on 26 March 2012, in the previous Session of Parliament (HC 106).

Ordered, That embargoed copies of the Report be made available, in accordance with the provisions of Standing Order No. 134.

[Adjourned till Tuesday 8 January at 2 p.m.

Witnesses

Wednesday 18 April 2012

Page

John Bassett, Associate Fellow, Cyber-security, Royal United Services Institute, **Professor Brian Collins**, Chair of Engineering Policy, Faculty of Engineering Science, University College London, and **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London — Ev 1

Air Vice-Marshal Jonathan Rigby, Director, Cyber, Intelligence and Information Integration, and **Major-General Jonathan Shaw**, Assistant Chief of Defence Staff (Global Issues) — Ev 9

Wednesday 16 May 2012

Nick Harvey MP, Minister for the Armed Forces, **Air Commodore Tim Bishop**, Head of Global Operations Security Control Centre, and **John Taylor**, Chief Information Officer, Ministry of Defence — Ev 16

Wednesday 27 June 2012

Rt Hon Francis Maude MP, Minister for the Cabinet Office, and **James Quinault**, Director, Office of Cyber Security and Information Assurance, Cabinet Office — Ev 29

List of printed written evidence

1 Ministry of Defence — Ev 42

List of additional written evidence

(published in Volume II on the Committee's website www.parliament.uk/defcom)

1 Dave Clemente, Researcher, International Security Programme, Royal Institute of International Affairs, Chatham House — Ev w1
2 Intellect — Ev w3
3 Trend Micro — Ev w4
4 Russ Bubley — Ev w5
5 BAE Systems — Ev w8
6 EADS — Ev w10
7 Research Councils UK — Ev w14
8 McAfee — Ev w17
9 Raytheon UK — Ev w21
10 Symantec — Ev w22
11 Institute for Security & Resilience Studies, UCL — Ev w30

List of Reports from the Committee during the current Parliament

The reference number of the Government's response to each Report is printed in brackets after the HC printing number.

Session 2012–13

First Special Report	Ministry of Defence Annual Report and Accounts 2010–11: Government Response to the Committee's Eighth Report of Session 2010–12	HC 85
First Report	Ministry of Defence Supplementary Estimate 2011–12	HC 99 (HC 577)
Second Report	The Armed Forces Covenant in Action? Part 2: Accommodation	HC 331 (HC 578)
Third Report	MoD Main Estimate 2012–13	HC 133 (HC 607)
Fourth Report and First Joint Report	Scrutiny of Arms Exports (2012): UK Strategic Export Controls Annual Report 2010, Quarterly Reports for July to December 2010 and January to September 2011, the Government's Review of arms exports to the Middle East and North Africa, and wider arms control issues	HC 419
Fifth Report	Future Maritime Surveillance	HC 110 (HC 827)

Oral evidence

Taken before the Defence Committee

on Wednesday 18 April 2012

Members present:

Mr James Arbuthnot (Chair)

Mr Julian Brazier
Thomas Docherty
Mr Jeffrey M. Donaldson
John Glen
Mr Dai Havard
Mrs Madeleine Moon
Sandra Osborne
Bob Stewart

Examination of Witnesses

Witnesses: **John Bassett**, Associate Fellow, Cyber-security, Royal United Services Institute, **Professor Brian Collins**, Chair of Engineering Policy, Faculty of Engineering Science, University College London, and **Professor Sir David Omand GCB**, Visiting Professor, Department of War Studies, King's College London, gave evidence.

Q1 Chair: Gentlemen, welcome to the Defence Committee. I am sorry to have kept you waiting outside. We will get on as speedily as we can. Would you like to begin, please, by introducing yourselves for the record?
Professor Collins: My name is Brian Collins. I am professor of engineering policy at University College London.
John Bassett: I am John Bassett. I am associate fellow for cyber-security at the Royal United Services Institute.
Professor Sir David Omand: I am David Omand, currently visiting professor at King's College London, previously security and intelligence co-ordinator and, probably of relevance here, Director of GCHQ.

Q2 Chair: You are all most welcome. This is our second Cyber-security inquiry, and we will be doing a third in due course. The SDSR described the National Cyber-Security Programme and its impact as transformative. Do you think it has been?
Professor Sir David Omand: Transformation is needed, and transformation will take time. It would be wrong to say that the programme has already been transformative, but it has the potential to make significant improvement in the vulnerabilities, which we will no doubt discuss, in a number of areas of national life that are subject to cyber-threat.

Q3 Chair: Do you think there has been a change of approach since 2009, or merely a promise of a change of approach?
Professor Sir David Omand: More money has been allocated, and that makes a big difference. The conceptual approach is very similar. I do not detect a great difference in that. The strategy itself is perhaps more clearly mapped out in terms of the areas of priority, and there are some important political statements, notably the importance of the cyber-realm for future national prosperity and economic growth, and the social benefit that will come from having it. I think it is more clearly stated that the purpose of cyber-security is to secure those gains. It is not an activity in its own right.

Q4 Chair: Would either of you like to add to that?
John Bassett: I endorse Sir David's comments. It seems to me that the benefits there have been from this and the previous strategy are essentially conceptual; that there is recognition of the nature of the threat that is faced and what we need to protect. There is also some sense that it is going in the same direction, and that it is evolving and will continue to evolve if we are successful, because there are still some areas of lack of understanding. We just do not know exactly how the internet will impinge on society. It is healthy that it continues to evolve, and I look to other strategies in due course to replace this one over a period of years rather than decades.

Q5 Chair: Professor Collins, what do you think the 2011 Strategy does well, and what do you think it does badly?
Professor Collins: I would reinforce the comments that have just been made with regard to an overarching strategy that is designed to pull together the whole Government around the issue, rather than it being seen as an intelligence issue, a defence issue, or probably a Home Office issue in isolation. It is holistic for the well-being of the Defence of the Realm; the military aspect is only one part of that. What it does well is to do that.
What it does not address is the pace of change that is needed. The organisational inertia that exists in Whitehall will get in the way of delivery. Perhaps as a codicil to that, going back to your previous question, there is an assumption that there will be continuity of stewardship of the strategy over a period of many years. History shows us that continuity of stewardship of strategies of this nature is quite difficult to achieve through our democratic process. We need to flag up the fact that that is so important to the well-being of our society—and, indeed, developed societies around the world, because we are not in isolation from other developed societies. That is what cyber-space does to us: it connects us richly to everywhere else on supply chains and economic and social well-being. Unless we maintain that stewardship over a period that is much

longer than the five-year electoral cycle, we will fail to deliver the desired outcomes.

Q6 John Glen: Building on that, is not one of the issues the internal co-ordination within Government? One of the challenges is how you identify who should be responsible for what among the National Security Council, the Ministry of Defence, the Armed Forces and the GCHQ, and how they fit together. How do you see the effectiveness of that cyber-security planning process at the moment?

Professor Collins: I would say it was work in progress. It is getting better, from my perception, given where it was, let us say, seven or eight years ago, when in a previous role I worked for the Defence Academy as a professor educating the military on information assurance and cyber-security matters. It was clear that that was completely disconnected from what was happening in the rest of the commercial world—and other parts of Government, even. Now we are beginning to see a much deeper understanding of the interconnectedness and interdependency between these various elements of our well-being. We are moving in the right direction, but I still come back to the fact that the threat is moving much faster than we are.

Q7 John Glen: Is it not a fact that, in some cases, some of the actors can be benign, curious individuals, versus actually identifying where malign intent exists? Does that not create ambiguities and uncertainties over who should take responsibility? How are those things being resolved, in terms of who owns it? The Whitehall structures tend to focus on a single point of ownership yet, by its very nature, it necessitates the involvement of multiple agencies. How is that resolved at the moment?

Professor Sir David Omand: I am not sure that I would put it quite that way. One of the improvements that has been brought in is to have central policy co-ordination. It is a very small team, located in the Cabinet Office. I have questions about whether there are enough people in that team with really deep expertise but, in principle, that is the right place to have that co-ordination.

Then we have to look, for example, to the Ministry of Defence to be responsible for safeguarding its own networks and transactions, for making sure that its networked equipment and network-enabled capability is not sabotaged by cyber means and so on. That is clearly its responsibility. Where does it look for its professional technical advice? It has capability of its own in the defence scientific and technical laboratories (DSTL), but the national centre of expertise is in GCHQ in Cheltenham. Again, one of the innovations that has been introduced is to set up the cyber-operations centre (CSOC) down in Cheltenham as a joint organisation, with representation across the interested Departments, so that there is that connection.

As a nation, we cannot afford—particularly in the current circumstances—to duplicate expertise. It would be nice to have different centres of expertise but I don't think that we can afford it, so what has happened is we have put it in one place and made sure that everyone is contributing to it, and can draw from it, particularly in relation to the most sophisticated, advanced persistent threats, where there is now a centre of expertise. The Ministry of Defence can go there for advice and technical assistance. That seems okay to me.

Then you go round the rest of Government. HMRC has a big cyber problem with all its networks. It is its responsibility to sort that and make sure that it takes on the right kind of professional technical expertise to do it. I do not think that it is so difficult. As Brian has said, what is more difficult is looking ahead. How will this evolve? Will we be ahead of the curve and spot the next generation of threat appearing? I hope that research is going into that but I am outside the system now so cannot comment.

John Bassett: If I might make just one observation, looking at international partners and so on, we are rather better joined-up than some of our international partners. Accepting that it is work in progress, and that it is still ongoing, there seems to me to be quite a lot more co-ordination and jointery here than overseas, in some cases.

Professor Sir David Omand: To add a specific example, which perhaps goes to your point, I would advise the Office for Security and Counter-Terrorism at the Home Office to put more effort into the cyber domain, not because we currently face a big threat from terrorist use of the cyber method, but because we very well could, and it needs to start thinking about that. It needs to start thinking about the role of the police in being able to access social media to derive intelligence, for example, to help in riots and crowd control, and all the rest of it. There are lots of things that Departments like the Home Office need to be thinking about now, all within the overall strategy that the centre is setting up.

Q8 Chair: Do you think that the 2011 strategy represents a proportionate approach to the different types of cyber-threat, for example, in relation to cyber-crime, terrorism and other national security threats?

Professor Sir David Omand: There is a real problem in trying to devise something called a strategy that would meet your standards of connecting ends, ways and means, because this is a big, baggy monster of a subject. It covers everything from the vandalism of websites at one end to what putatively could be acts of armed aggression at the other, with crime in between. I would limit the expectations of what you should look for in a national strategy. You have to break the subject back down into, for example, financial crime or countering espionage and then really have sub-strategies looking specifically at those kinds of threat. There is a limit to how far you can take strategising at the grand level on a subject like this, and it is moving so fast.

Professor Collins: The Government are not the only organisation that have a strategy in this domain. Clearly, if you work in the financial markets in the City, you will find that all the major banks, clearing houses and insurance companies have major strategies and major investment. Some of that might dwarf what the Government are doing because they are seeing real

money being put at risk, in the way that the Government have other things that they value being put at risk. You have to take a more holistic view of what the total investment—financial and political—is in this subject. To answer your question in a more accurate way, just to look at the Government piece is not sufficient.

Q9 Chair: The Strategy talks about "exploiting the cyber environment for our own national security needs". What do you think that means?
Professor Sir David Omand: I could hazard a guess.

Q10 Chair: Would you care to do so?
Professor Sir David Omand: It may be completely wrong, since I did not write the document.
Chair: Of course.
Professor Sir David Omand: I suspect that it is a euphemism for the fact that, while cyber-security focuses on defending ourselves from aggression from elsewhere, we, too, would be capable should it come to it to use the cyber-domain for our own offensive purposes, for example, in taking out an air defence system where we are engaged in military operations. We have to look not just at the defence, but at the potential offence within the law, within international humanitarian law and within all the constraints that armed force would normally find itself. That is one possible explanation—we can actually exploit this.
John Bassett: Perhaps one would add that ongoing active intelligence gathering that the state would wish to do will be done in cyber-space as well as in other areas. That is another activity that would fit into that description, I believe.

Q11 Chair: Professor Collins, would you like to add to this?
Professor Collins: No, I concur with what has just been said.

Q12 John Glen: Some of what I ask has been covered in your answers. The Intelligence and Security Committee report identified 18 departmental bodies that were interested in cyber-security. You have explained how there has been a significant effort to co-ordinate efforts into a single entity, but each of those bodies will have a different perspective on the threat and its nature. Going forward, it is difficult to see how the MoD would have the same perspective on malign threats as the Home Office, for example. There will surely need to be some movement in terms of who takes responsibility and ownership. If that central co-ordinating agency does not do justice to the interests of one part of it, it will, of necessity, become fractured. How do you see that organisational model evolving? How will different ownership for the different bits of cyber-security evolve as the threats and people's interpretations of the risks differ across different parts of government?
Professor Sir David Omand: I shall answer that slightly indirectly, by saying, "Were you to ask me in 1910 the same question in relation to the invention of the internal combustion engine, you would immediately see that here is a transforming technology." Every part of government has a potential interest. There is a big upside in economic growth, and the nation needs to develop the technology to master the use of such devices, but there is a dark side. There was a dark side to the motor car—criminality, warfare. In exactly the same way, in the cyber-domain, we can see a dark side. Every part of government has got to be involved in this. I would be very against trying to over-centralise this kind of thinking about cyber.

Q13 John Glen: The Department for Transport, in the end, owned it, with respect.
Professor Sir David Omand: It has a policy responsibility. In the case of cyber, that is what we must look for from the central Cabinet Office policy team. It is at a high level. Work will continue on the cyber-implications of the work of Government Departments and their communications, their databases and so on, and the public's use of these. For example, the Government might use social media to inform the public about their responsibilities, benefits that they might need and so on. In an emergency, they might give the public information about what is going on. That, too, will need analysis.
As I say, you have to be quite devolved about this, and then have a powerful centre that can lay down some high-level policy and sort out arguments, when they arise, about whether it is more important to go for economic advantage or try to get more security over there, because there will be conflicts. For example, I think there is a conflict for defence between the current fashion for buying things off the shelf at the cheapest price and taking the time and expenditure to write computer code that is genuinely secure. Somewhere, somebody in defence has to strike a balance between those. Most of the successful cyber-attacks have come about because of flaws in the computer code that should not have been there if it had been written properly. If we go about just buying stuff off the shelf, including computer software that has been bundled together from pre-existing blocks of software, then I am afraid we are making ourselves vulnerable. But that costs, so somewhere there are trade-offs. For some of these higher-level issues, again I look to the co-ordinating policy centre to put this before Ministers and try to get some guidance on where to strike the balance.

Q14 John Glen: Thank you; that is a very helpful analogy.
John Bassett: I wonder if the historical perspective isn't helpful in this in a slightly different way. If we look to the cold war, we would see then that the Home Office would have a particular set of national security concerns, which might be in the espionage area, and the Ministry of Defence might have interests that are in the nature of the deterrent or the central front. In some ways, that is the kind of reconciliation we would need now. It isn't so very different from the kind of reconciliations that we have done in the past with some degree of success. I don't know that the co-ordination challenges are so very different from some of the challenges we have faced in this and the previous century.

Professor Collins: I would add one point, if I may, John, that does complicate things, and that is the complexity of the nature of the multifarious threats that we face and the lack of clarity, as you have indicated, as to what their purpose might be. Is it bravado or is to damage or steal something valuable? That complexity compounds the difficulty of this co-ordination process strategically. Tactically, I don't think we are in bad shape at all. However, to be in a situation in which you can anticipate where some of these things might be coming from is a combination of intelligence-gathering, which we should not go into here, together with some idea of where individuals or groups might be taking their thinking, when we would regard that as undesirable for us. That horizon-scanning function is a piece that I see missing. We don't appear to have resourced that as effectively as we could have done. Although there are words in the strategy that say that is what should be done, I don't think we have put enough anticipatory investment in place, not just in Government, going back to my previous point, but Government with others who play in this space. The need for national secrecy sometimes impedes that collaborative activity.

Q15 John Glen: That is exactly my point. The nature of that collaboration means that compromises are made in order to have co-ordination and a single view.
Professor Collins: There shouldn't be any within Government, but my point relates to between Government and other bodies inside the nation—not international collaboration, which has its own problems of course—such as the City, other operators and other critical national infrastructure activities.

Q16 John Glen: I just want to get to the bottom of this point with respect to the MoD. If the MoD felt as a single Department that that horizon-scanning was inadequate—those that were represented in the central planning body—then it would probably be a failure if it decided to undertake a separate departmental activity that was in some way extended.
Professor Collins: It would certainly be less efficient than it might be.

Q17 John Glen: That is a reasonable measure of success perhaps.
Professor Collins: Yes. That is entirely right. However, at the technical level I should have mentioned that I left the position of Chief Scientific Adviser in BIS and DFT last May, so I sat on the National Security Council sub-committee for Science and Technology, as one of all the chief scientific advisers involved in this matter who sat at that table. That body was the one that would advocate a rise in scanning activity in a pan-departmental way, at least about social science and the physical sciences. I emphasise that because we were very keen to ensure that more social science research was done on futures and horizon-scanning. That was work in progress. I am no longer on that body so I don't know whether that work is proceeding. There are indications that it is. I still do not believe that it is being resourced as effectively as it could be. There is maybe too much emphasis on the short-term tactical as opposed to the longer-term strategic.

Q18 Chair: You said earlier, Professor Collins, that the strategy did not pay sufficient attention to the pace of change. Are you able to give us any quick example of that?
Professor Collins: If I had suggested three years ago that people would be organising riots in the streets using Facebook, no one would have even understood what the words meant. Last summer, that is what we saw. Now, if you say to law enforcement or, indeed, maybe to parts of our military operations, "Do you expect to see those sorts of applications being used to organise a significant threat to us?", I do not believe that we have the mechanisms in place a priori, as opposed to by way of response, to anticipate where some of those things may be hitting us. That is one example not so much in the defence domain as in law enforcement, but you can clearly see how that could be expanded into more international domains, which would be of interest to the Ministry of Defence.
Professor Sir David Omand: Another interesting cyber-example, which I certainly did not predict and I am not sure that the Ministry of Defence had anticipated, was what the impact of soldiers and Service personnel equipped with mobile telephones with cameras would have on the home front—the blogging and the sending-back of real-time video of combat. It is completely unheard of in history to face that kind of situation, and I think people are just getting their minds round it now.
John Bassett: If I may make one point to build on those themes, these examples, whether it is Facebook and the riots or mobile phone cameras and so on, are existing forms of technology, but they are used in different ways. Facebook had been around for some years before it was used in the riots and cameras likewise. It is important to think of cyber-security not just in terms of changing technology but, perhaps critically, in terms of how people are using that technology. The technology develops and can develop quickly, but people are actually capable of using these things in unexpected and unforeseen ways very much sooner than the technology changes. It is the people who, as ever, are most adaptive and the fastest moving.

Q19 Mrs Moon: I am just wondering whether the people of Tunisia, Egypt and Libya are not absolutely grateful that the technology to predict what has been organised is not in place. We can talk about it in terms of riots, but it has also had beneficial effects for people living with tyranny, so I do not think that we should underestimate that. I certainly have seen the police force using Facebook to look at criminal networks, but can you give us a summary of threats to the Ministry of Defence and Armed Forces networks and of the nature of cyber-security threats?
Professor Sir David Omand: As I read it at the moment, they perhaps fall into four or five categories. The first is straightforward criminality. The MoD, as any other large organisation, has bills to pay and staff to pay, and it has to protect itself from criminal activity. That is no different from any other

organisation, but it is quite a big organisation, so it has to be taken rather seriously.

Then we have a trio of espionage, subversion, and sabotage, which are not cyber-war. They are far short of cyber-war, but they are very serious. So that means stopping hacking into networks in order to gain intelligence, either on equipment or on military activity. What I would regard as subversion is the Jihadist websites and suchlike. There is also the possibility of sabotage, where the particular bit of network or kit that you are relying on in combat suddenly does not perform as it should because it has been degraded and you did not know that a Trojan had been planted.

Not currently, but in the future, we have the possibility of more widespread and more serious cyber-attacks, which, in a situation of national emergency, could mean that the electricity does not work and you have attacks on the infrastructure. That is of interest to the Ministry of Defence, because it will of course depend on that infrastructure both to mobilise and then actually to support military operations. That would be my spectrum.

Q20 Chair: That's three.

Professor Sir David Omand: No, that's five.

Q21 Mrs Moon: Can you give us some examples of where this has actually happened, not necessarily in the UK but where a military network or operational asset around the globe has actually been impacted? Are there key ones that stand out as good examples for us to look at?

Professor Sir David Omand: That might be a question you want to address in a closed session. I can only rely on what I read in the newspapers.

On espionage, there is plenty of evidence of penetration. The Canadian discovery of GhostNet, as they called it, was a major penetration by a state power looking for intelligence and commercial information. The Australians also suffered in the same way, and they did actually pin that to a Chinese source. Again, that was for commercial purposes. I think we are all familiar with the subversion side and the jihadist websites.

I am not aware of many properly documented cases of sabotage in which somebody has planted some Trojan or virus. Stuxnet is the one everyone talks about, but, in my view, people jumped to the wrong conclusions on the Stuxnet experience. What Stuxnet shows, now that the code has been examined in very great detail, is that it was a very specific attack on the centrifuges at Natanz, although, as viruses do, it actually spread elsewhere. The virus would not have harmed anything else, because it was written and designed, and had to be written and designed, only to attack that target, including the specific location of the centrifuges and the way they were patterned. All of that is clear, I am told, from the code.

So there is a relationship: the more damage you want to do, the more specialised your attack has to be. Therefore, if you really want to knock out the enemy's air defence system, you are going to have to design something very specifically for that purpose. It won't knock out their civil infrastructure. Not only that, to design it you are going to have to have a huge amount of intelligence—detailed technical intelligence, and probably insider knowledge and insider help. Finally, you have to be attacking a system that has some flaws in it. If the system is really well designed and protected, you will find it rather hard. As we know with Stuxnet, they were attacking a Siemens control system that everybody knew had a flaw in it. As far as I know, the flaw still hasn't been fixed. That is the kind of approach that I take.

The thought I would leave with you on that is that the threat of sabotage at the moment is probably relatively low, but it is likely to rise because knowledge of how to do this is likely to increase. It would be a reasonable prediction to say that this kind of threat will increase. So now is the time to start work on it and now is the time to do the research and development, but I would not overwrite it or overhype it. As I say, we haven't faced a massive cyber-threat of sabotage of our systems. That is only one view, and I could be wrong.

John Bassett: It seems to me that, if we take Stuxnet as in any way representative of cyber-weapons, Sir David's comments are very apposite. This is something that has clearly had a huge amount of intellectual capital poured into it. Sir David has illustrated very clearly that it could only be used once for one thing, so we are really talking about almost hand-crafted weapons in that sense. This is not something where one can easily imagine a production line of high impact cyber-weapons. I may be wrong in saying that, but that is just my perception, if we can in any way see this one example of Stuxnet as indicating anything of the future.

Professor Sir David Omand: A modern anti-radiation missile fired from an aircraft will home in on the sorts of frequencies you would expect from an air defence radar. What we are talking about here is spending a lot of time and energy building something that will attack only one specific kind of system. That will rather tend to limit it, and it is one of the reasons why I do not personally believe in cyber-war. This is a helpful adjunct in some circumstances to some nations, giving them perhaps a bit of an edge in certain circumstances, but we are not going to see battles going on in something called cyber-space.

Q22 Chair: Professor Collins, do you disagree?

Professor Collins: I do not disagree with the position we are currently in, but I think anyone who has the ambition to make things much more difficult for us will realise the limitation of what has just been described, and will be starting to look at targets that we have that do not have those very singular properties, so that they can not only attack, but mount campaigns—in other words, sets of attacks in different dimensions, whether social, technical, or political—in order to achieve their objectives. I do not think we should be in any way complacent about investigating what that might look like hypothetically, in order to at least understand what the threat mindset might look like, were they to go down that road. They will be looking for the appropriate economic balance between what it costs them to mount the threat versus what the impact will be. As has just been described, it is

probably disproportionate against them at the moment, but they will not tolerate that for very long. They will be looking for softer ways of achieving what they want to achieve.

For instance, one example that I have had conversations with colleagues in the Department of Energy and Climate Change about is smart meters. If there are 35 million of them littered throughout households and industrial premises in this country, and there is a degree of uniformity about them, so that electricity monitoring can be carried out easily and at a very low cost to us, that uniformity—in contrast to what has just been described about Stuxnet—provides a blanket mode of attack. You can attack all of them all at once and disable them, subvert them or do things with them. Although defence may be one stage away from relying on the energy systems of this country, were the electricity to disappear for very long, I think MoD would have some problems. That is just one hypothetical example of where we are actually putting in systems that have uniformity, and we are putting them in at scale.

Q23 Mr Brazier: My question follows straight on from that last point. The rather good pamphlet, I thought, by Graeme Lamb and Richard Williams makes the point that we tend to focus on security in cyber and protecting our systems, and we have missed the opportunities for offensive warfare as we move from the industrial to the information age. In the First World War, we were not trying to design anti-tank weapons before we built tanks. Do you think that there is a very significant offensive capability in the cyber world?

Professor Collins: There will be a capability, but whether we should use it for our national purposes is one issue. It is rather like chemical and biological weapons: we had treaties to stop us doing it, but that did not stop us thinking about what such things might look like, so that we could defend ourselves appropriately. I think we are in exactly the same space. We have to try to put ourselves in the threat mindset to understand what they might try to create that would cause us damage. That is not quite answering your question. In doing that, we will understand—were we to want to, and were we to feel it was ethical and legal to do so—that we would be in a position to go down that road. That is a decision one would have to take at that time.

Q24 Mrs Moon: Professor Collins, in terms of the actors that we might be needing to defend ourselves against, a lot of focus has been on criminality, anarchistic groups and terrorist groups, but what about state actors? How significant is state-sponsored action thought to be, where one state uses cyber as a way of attacking another state? Is that a realistic expectation of the threat that we face?

Professor Collins: Clearly, you would not expect me to answer specifically whether it is a realistic one, in the sense of knowing whether such a thing exists, in open session. Is it realistic to assume that it might be possible? Yes, because it has happened in the past, and we should not repeat the mistakes of history by not examining what happened in the past, which I think we have a propensity for doing.

Q25 Mrs Moon: In that case, you are probably not going to like my next question. Where do you think the attacks would come? Would they come on supply chains, a particular asset, or networks, or would they be trying to influence the individual in the field—their communication systems, or the particular weapons that they carry?

Professor Collins: The answer to all of it is yes, because all of them have value propositions to a threat. I think what one has to understand is the value proposition to the threat in attempting to disrupt, destroy or steal from an asset that we would regard as valuable. That is the very simple equation that I think we need to examine. It goes back to my much earlier comment about horizon scanning. Part of what horizon-scanning activity ought to be doing is looking at those sorts of possibilities in this space, much as the Ministry of Defence does in its more traditional military operations space over a 30 to 50-year horizon. It looks at geopolitics. I know, because I have been involved in it. Is it doing that as vigorously and thoroughly in this space, in collaboration with other Departments, as it could? I suspect not.

Professor Sir David Omand: From a slightly different point of view, the most prevalent form of attack that falls into the state-versus-state category is espionage and the theft of intellectual property. It is very much in certain nation's interests, for economic and commercial purposes, to get an edge by getting early sight of research work done in pharmaceutical labs, oil exploration, or whatever, so I think that is where we will see the leading edge of threat. Why would a state attack another state only with cyber-weapons? It wouldn't. You could just about construct a scenario where a competent state used a proxy—Iran and Hezbollah, for example, if Iran were particularly pissed off with us and decided that something ought to be done. However, it gets far-fetched quite quickly, as against rather more straightforward ways of using your proxy to cause trouble. So I do not see this is as cyber-domain stuff.

Professor Collins: No, nor do I.

Professor Sir David Omand: I see this as a question of whether states can use the knowledge that they now have of the cyber-world to improve their military capabilities—and yes, they can. The other point, at the risk of dampening down enthusiasm for all this, is that we are quite a small player in all of this. We are not really at the leading edge, when you look at the size of effort that goes on in the United States and, I imagine, other countries such as China. We just need a slight sense of proportion about that.

Q26 Mrs Moon: But it was a small State—Estonia—that faced a particular threat and experience, which woke people up.

Professor Sir David Omand: It woke people up, but it was actually only a denial-of-service attack.

Q27 Mrs Moon: As the Armed Forces are increasingly looking at network technology, are the

increased risks to those new network-enabled weapons systems bringing a new level of risk?
All witnesses: Yes.

Q28 Mrs Moon: Or is the level of risk greater than when we were using simpler weapons, if you see what I mean?
Professor Collins: When I was a professor at the Defence Academy in Shrivenham, I gave lectures on network-enabled vulnerability, which is exactly your point. Yes, it has to be thought about in a systematic way across the new development. Every new development that the MoD puts in should be thought about in terms of what it does, especially—I am sorry, that is not very articulate. When it is networked, what does that do with regard to enhanced vulnerability that had not been there before it was networked? You are absolutely right.

Q29 Mrs Moon: So we need to offset enhanced capability against enhanced—
Professor Collins: New benefits normally do have new risks.

Q30 John Glen: Do you think it is useful to describe cyber-space as a new domain? I think, from Sir David's comments, that he does not think it is, and I recognise that there is a present and a future. Obviously, if you get into that language, it has implications, in terms of how resources are employed and so on, particularly for the Armed Forces, in terms of acting in a different domain. I realise that there is a bit of a debate on this. It would be interesting to hear your three views, even with respect to the present and the future.
Professor Sir David Omand: My instinct is against thinking about cyber as a domain, because it is ubiquitous. If you are looking at land, sea and air and operations in those environments, they all involve activity that could be influenced by cyber, so it is not something to put in a compartment and say, "Within the Ministry of Defence, cyber is done by this little group in isolation". That said, obviously you need to have some focus of activity and some command and control, but I am just nervous about people thinking that because it is a separate domain, you are going to get separate activity. In the end, with cyber, it is real people who get hurt, real money that gets stolen and real intellectual property that gets pirated.

Q31 John Glen: You have cyber-war and cyber-weapons, do you not?
Chair: Maybe you do not have cyber-war.
Professor Sir David Omand: I think that the idea of cyber-war is very unlikely. Cyber-assisted war is very likely.
John Bassett: On balance, I can see some use for the concept of cyber as a domain at present, principally for the reasons that David has outlined—that it helps focus thinking on it. It is unclear to me whether in five years' time we will think of it as a domain or not. I would say, yes, very gently and cautiously, at this stage let's consider it a domain, but let's be willing to drop it quite quickly if it proves that that is not the best way of handling it—not a very robust form of conceptualisation, I am afraid.
Professor Collins: I do not think that it is new at all. There is a very interesting book, published some years ago, called "The Victorian Internet", which is worth reading, because it is the history of the telegraph in the mid-19th century. In particular, there is an interesting military story whereby the military discovered that a telegraph message could be sent to the Crimea in about a day and a half. It took them six weeks to get the reinforcements there, by which time, of course, everyone was prepared for the reinforcements to arrive. That was when they woke up to the fact that the telegraph travelled more quickly than ships—a very salutary story. The relevance of it is to do with time constants, and the rapidity and global range and reach of what we now call cyber-space compared with where it was maybe even 10 or 20 years ago.
The parameters have changed, the nature of how cyber stuff interacts with all the other physical and organisational stuff, and those things are different. That is where I think that the acceleration of the rate of use, the rate of range and the reach of cyber stuff has changed the nature of how it interacts with all the stuff that we have traditionally done, and I am not sure that we have really bottomed that at all yet, as to what the impact of that change of time constant is. "The Victorian Internet" describes that in terms of days and months; we are now talking seconds, and that is really rather different for us, compared with where we were even 10 years ago. It is not new, but it does have aspects that are different.

Q32 Mrs Moon: From what you are saying, we are always playing catch-up, so what are the priorities that you see now for the next Defence and Security Review? Are we able to project that forward, or are we always waiting for the technology to come along to know what we have to start building our security around? Do you know what it is now for the next four years?
John Bassett: On a personal basis, I think that it is all about the people. It is about ensuring that we have enough good people in the Ministry of Defence, other parts of Government, academia and industry, and I think that we do not have anything like enough at the moment. I think that growing and skilling the people is, for me, the single most important thing for us to do.
Professor Sir David Omand: Iain Lobban, the Director of GCHQ, last year introduced the idea of the 80:20 division—you can get 80% of the security that you need through good hygiene, looking after people and your information, patching your systems up and ensuring that everything is up-to-date. For the remaining 20%—the really dangerous attacks and the advanced, persistent attacks—you really have to get into the intelligence space, understand who is attacking you and how you are being attacked, and work with the security industry to fix that.
One of my priorities would be getting the relationships right between the Government's capability, particularly down at GCHQ but in defence as well; the security industry, which has a great deal of capability in this area; and their customers—the critical national infrastructure, the financial system,

the defence companies and so on—so that we make a real impact on stopping the theft of intellectual property. I think it is possible to do that.

Another priority—this is not a defence priority—would obviously be in relation to criminal activity for gain, trying to cut down on losses from cyber-attacks for criminal gain. Those would be the things that occur to me first.

Q33 Mrs Moon: I am intrigued by what you said about the interrelationship between Departments and the private sector, and the sort of communication between them. What about building that relationship in relation to research and development, and building sovereign capability? Is that relationship in place, or is that something you need to develop?

Professor Sir David Omand: It was highlighted in the National Strategy, and my assumption is that people are working away trying to develop it. I would not hazard a guess how far it is there yet, but I think people are trying things out, and new relationships are being developed. I know that a number of companies have been working very closely with GCHQ and being given much more information—highly classified information—about the kind of attacks that are going on to steal intellectual property. It seems that that sort of trusting relationship—circles of trust—is essential. The Government cannot do all this themselves, working directly with the thousands of different companies that are under attack. We have to mediate it through the industry.

Professor Collins: There is a joint programme that Research Councils UK and GCHQ are funding, which announced only last week new centres for academic excellence—I think six universities in this country, it was announced. It is exactly aimed at providing the bigger pool of expertise that we need, but it will take time.

Q34 Chair: We are just about to go into private session with those responsible for this within the Ministry of Defence. Is there anything you feel that we should know that you have not been asked questions about, or that would be the key question that we failed to ask? What would you answer to that?

Professor Sir David Omand: The question I would ask, I have to say—looking behind me at the people you are about to address it to—would really be about priority. The cyber-security domain was put up as one of the top four national security priorities. If we are going into defence, the question I would ask would be: does it have an equivalent priority within defence? Is it being taken sufficiently seriously? Are the organisation and the levers in place to enable those who are co-ordinating this work to make sure that every aspect of it is taken seriously? As I was saying at the beginning, we are dealing with an enormous range of potential threats, some of which may be at the more trivial end, but some of which are extremely serious. I hope that the Ministry of Defence is really up for this.

John Bassett: If I were you, I would ask what the metrics for success in this area are, particularly in the softer areas of cyber-security, as in the strategy. What does success look like? How do we determine whether we have succeeded? What are the metrics? It is not an easy thing to answer, but I think it is a good question to ask.

Chair: This is very helpful, because you are giving those who are just about to answer the questions the chance to work out what it is that they are going to say in response to these questions.

Professor Collins: Recent history shows that the Ministry of Defence has undertaken almost no operations without being part of an allied group. How does cyber-security work in the context of working with allies, some of whom we have worked with continuously for some time, and some of whom, as it were, we are meeting for this occasion, whatever that operation might consist of. How does that work out? Have we got existing protocols or established mechanisms by which we set up those alliances, and the cyber-security that needs to exist within it, quickly and effectively?

Professor Sir David Omand: The other thing that I would ask in a closed session is about the advantage that our long-standing relationship with the United States gives, in both military and intelligence terms, in getting a handle on some of these technological developments.

Chair: Thank you very much indeed for informing us and our session, and also our next session.

Examination of Witnesses

Witnesses: **Air Vice-Marshal Jonathan Rigby**, Director, Cyber, Intelligence and Information Integration, and **Major-General Jonathan Shaw**, Assistant Chief of Defence Staff (Global Issues), gave evidence.

Resolved, That the Committee should sit in private. The witnesses gave oral evidence. Asterisks denote that part of the oral evidence which, for security reasons, has not been reported at the request of the Ministry of Defence and with the agreement of the Committee.

Q35 Chair: Thank you very much for coming to inform us, in an entirely private session, about some of the questions that we have to ask. Would you mind giving a very brief summary of what you both do, please?

Major-General Shaw: Major-General Jonathan Shaw. For the past year and a bit—since its inception, in fact—I have been the head of the Defence cyber-security programme, which I may go into a bit more detail about, but which effectively means that I am responsible for the £90 million that came across from the Cabinet Office as part of the national cyber-security programme. This post was created in response to SDSR, and it was the MoD taking cyber seriously for the first time. I leave in about a week's time, and my colleague to my right will be the next head of the Defence cyber-security programme. I am handing over to him, so you have the past and the future.

Chair: Right. Thank you.

Air Vice-Marshal Rigby: I am John Rigby; I took up my post about three weeks ago. The post was originally intelligence capability, and it has grown, as part of the normalisation process for cyber, to include cyber-capability and elements of information operations. That is the role.

Q36 Chair: Okay. Thank you very much. Can you describe the chain of command in relation to the cyber issue? It is defence security within the MoD and within the armed forces. If you could stick within the Ministry of Defence part to start with, we will then broaden it out.

Major-General Shaw: I think it is best here to talk about the future rather than the past. The future is tentative and there are areas that I will highlight as being in discussion. What we are really talking about now is the creation of the Joint Forces Command, which took effect from 2 April. It instituted a new process, which has yet to bed in and yet to be finally decided upon.

In effect, the chain of command for cyber operations follows the chain of any other form of operation, in that if we were doing an integrated operation, there would be cyber elements within it. From that point of view, the command and control of actual cyber operations within the military domain are run as in any other operation, because the whole key about cyber is to look at the effects you are hoping to achieve and, if it were part of military effect, it would be merely one of the tool bags. It goes back to some of the discussion in the open session earlier, whereby cyber is not seen as something separate—a completely discrete stove-pipe—but merely another golf bag that the military commander has at his disposal.

Therefore, the cyber effect needs to be woven into the overall effect that is being achieved by the Joint Commander. That is very much the model we have and, therefore, the operational chain—if we are talking about delivering the operational effect—remains as it has always been, with Permanent Joint Headquarters and the Chief of Defence Staff, and those lines of operational authority. The confusion has perhaps arisen from the fact that the Joint Forces Command is there to generate capability to be used by defence on those operations, and there the chain of command is in flux, because hitherto we have had part of the cyber-defence bit being owned down at Corsham under one chain of command. There was also the targeting and information operation function in the main building, as well as various disparate bits. The whole point of the creation of my post was to bring all that together into one coherent package. The point of the creation of the Joint Forces Command is to provide one focus, which will be my successor here, who will be driving the development of capability across defence, so the various bits of force generation and cyber-capability will be developed in accordance with the plan at Joint Forces Command. That is the single service piece; it is the joint cyber unit at Cheltenham; it is the operations taking place at Corsham; ***

There are two chains of command: an operational chain of command that remains much what it was, and the capability development chain of command, which very much centres on the Joint Forces Command. The operational command and the capability development command both sit at Northwood within the structure of the Joint Forces Command. I do not know whether anyone wants to comment on that.

Air Vice-Marshal Rigby: I have just a couple of things to say. On reducing the cyber risk or seeking to achieve a cyber effect, that would come directly out of a contingency plan or the campaign plan. As we have just said, it would be another element of the military capability portfolio that one either needs to protect or use in a defensive role. We would then be working very squarely with GCHQ among others, but we would then actually ensure that our capability was delivered in order to achieve the commander's effect. The only other thing I would add is that the DOC is currently conducting an audit into the detailed command and control relationships between the different components of the cyber world. That is due to go to the Secretary of State at the end of May.

Q37 Chair: Who is conducting the audit?

Air Vice-Marshal Rigby: The director of operational capability is conducting an audit into progress thus far and recommendations for detailed command and control arrangements. I am squarely responsible, but it is on how we achieve unity, and it goes to the Secretary of State at the end of May.

Major-General Shaw: I think that it is worth commenting that the critical issue is something called *** which you may have heard about. Hitherto, it was

the mission to defend our network—pretty much the focus of MoD's effort in cyber-space and the protection of our own networks. It was called ***. It was run by the Chief of Defence Matériel. In many people's judgment—I am one of those who believe it—what we have learned over the past year about the nature of operating in cyber-space means that the idea that we can just have cyber-defence as one hived-off piece has been overtaken conceptually.

Actually, there is no such thing as pure cyber-defence. If you want to secure your networks, you have to manoeuvre in cyber-space. If you are going to manoeuvre in cyber-space, yes, you need some defensive elements, but you also need the ability to punch the enemy as well, if I can use that metaphor. ***

Certainly my recommendation, as it went to the Joint Forces Command, was for it as a standing operation, running our networks and defending them. That is very much how conceptual evolution is affecting our organisational structures. As I say, it is that decision that will go to the Secretary of State in the next few weeks, as per the DOC audit. I have not seen the DOC report, but I would hope that that is the answer it gives.

Chair: At 3.49 pm, there is likely to be a vote—perhaps more than one. Julian Brazier needs to go at some stage. I have more questions about the chain of command, but I wonder whether I can ask Julian Brazier to ask his question first.

Q38 Mr Brazier: Thank you very much. Following straight on from the answer that you have just given, what planning assumptions will inform the development of your future cyber-force? You have told us what it will look like structurally, but that is too general a word. What sources are you looking at? You have been given a significant amount of money, and you have thought a lot about structures. What is the bible on what the threat is out there? What are the assumptions?

Major-General Shaw: I think the first assumption that we would make is that we are aiming at a moving target and that, whatever we come up with now, we will have to test and adjust with reality, if not anticipate it. We have come up with various force levels, which are the basis of the DCOG—the Defence Cyber Operations Group. That is the programme of new line serial numbers for personnel operating inside Cheltenham, working with GCHQ in the Joint Cyber Unit, Cheltenham.

Q39 Mr Brazier: Uniformed people?

Major-General Shaw: Those are uniformed people working inside Cheltenham, helping them to come up with national capabilities. Here it is worth stepping back a stage and saying that the British response to the cyber threat—this is very much what you hoped for—is to create a national bucket of capability, from which everyone draws. As for what David Omand said, there is only thing I would disagree with: I do not believe that it would be nice to have separate stove-pipes of capability. I think that the UK is significantly advantaged by having one bucket of expertise. That one bucket of expertise is GCHQ. We are contributing personnel into it to ensure that in the development of cyber-capability there are military people there, both to add their expertise to that development and to give the military input on what sorts of effects we might be looking for in cyber-space.

Q40 Mr Brazier: Following directly on from that, I was encouraged to hear what you said about the manoeuvrist point ***. To what extent will you be looking to reservists and the private sector for skills for this? Obviously, you already have the specialist signals groups.

Major-General Shaw: Well, there are minimalist and maximalist options here. At the moment, General Brealey, who is heading up the study on behalf of Defence, is starting it small, with the unit you have just mentioned and with formed units and nice haircuts and people doing drill—what you might call conventional cyber-reservists. My vision on cyber is very much inspired more by the Estonian model, by thinking more broadly about the sort of people that UK Ltd needs as a reserve capability, because so much of our cyber-resilience, if we were to suffer an attack and needed reserve capability, is not about uniformed people as such.

If you go down to Corsham and look at the Joint Cyber Unit, Corsham, which handles our defensive aspects, you are hard pushed to tell who is a service person and who is a civilian, because cyber-capability breaks down all the barriers between civilian and military, and it breaks down the barriers between war and peace. It is ever-present and it is a capability. If we are facing a national crisis, we will need a national reserve more than we will need a military reserve. I can see where there may be cases where we need to send some military cyber operations overseas, and that will have to be service people, but the grander vision for reserves is to go for a national reserve that really will attract people with ponytails and earrings and will not force them to go through the same military strictures that we conventionally think of, so that we pull in the people with the requisite talent to get involved in the national effort. That will take a different sort of mindset and a different kind of approach.

Q41 Mr Brazier: A very quick point, if I may throw it in, because we will have to vote any second: the point that those in the specialist signals group made to me was that they really think that they are getting those sorts of people. They are getting a very wide variety, but in terms of sending teams abroad to do some of the quite exciting, chunky things they have done—normally a two-man team—they always like one of those two people to have had some military experience in another context. Simply putting a guy into a job who has not got any military experience—they are all cyber experts and they all do it for a living and that is brilliant—is actually less valuable in that, working on his own.

Chair: Are you asking a question here?

Mr Brazier: No, I am not. I am making a point.

Chair: ***

Air Vice-Marshal Rigby: ***

Chair: I am afraid that we are going to have to vote. We do not know how many times we will be voting. We will come back as soon as we can. We aim to get this evidence session over by 5 o'clock, if that is okay, come hell or high water. Thank you very much. We will be back soon.

Sitting suspended for Divisions in the House.

On resuming—

Q42 Chair: Julian Brazier was in the middle of asking you questions about, among other things, the Defence Cyber Operations Group and what planning assumptions will be used. We heard the phrase "cyber-hygiene" from David Omand before. What are you actually doing to instil cyber-hygiene across not only the Ministry of Defence, but the armed forces in general, and also the rest of Government? I suppose that may not be your responsibility.

Mrs Moon: And the Defence Committee.

Chair: And the Defence Committee.

Major-General Shaw: It isn't, you're right, but you have touched on a wider theme. The interconnectedness of us all means that there is a national issue about education on cyber-hygiene. As part of the training needs analysis work that we undertook as part of the defence cyber-security programme, one of the strands was personnel and training and skills needs. That broke down into an analysis of the specialists. We would need the top-end specialists with hybrid skills doing bits of this and the other stuff, and a sort of general level of awareness that everybody needs across the bottom end. That work has just reported at the end of March. Those plans are being put into place now across Defence. Just as the Government have issued the "Get Safe Online" document both in hard copy and online, so within the MoD we are stepping up our cyber-hygiene efforts to educate all personnel in the requirement for cyber-hygiene.

Air Vice-Marshal Rigby: There are two aspects. The first is counter-intelligence to make sure that if there were an insider threat—someone with malicious intent within the forces—we would need to get them and make sure that that threat did not materialise. We have recently taken on responsibility within defence intelligence for doing CI, and we are increasing the number of analysts set aside to make sure that our people are safe, so that they do not have the opportunity. ***

The other thing with GOSCC at Corsham is to ensure that the patches that we put on the systems and on the network are up to date, and they are very professional at doing that. You can never be there all the time, but as long as the gap between a threat being identified and a new patch going on the system is minimised, then your system—just like at home—is more protected than it would otherwise be. Those are two other aspects that are really important for hygiene.

Q43 Chair: Which brings up the question that Professor Collins raised about working with allies, and whether there are decent protocols in place, particularly working with the United States—something that Sir David Omand raised ***.

Major-General Shaw: Cyber is just another effect, or rather, to put it another way, it is merely the latest medium through which to achieve effect. Therefore, all the normal effects that we try to achieve, and all the normal relationships that we have, suddenly have a cyber dimension to them or cyber ways of achieving them. Hence everything that we have tried to do before and all our international relations now have a cyber-annexe on them.

That is easier in some areas than it is in others. For instance, our relationship with the United States is, inevitably, the most mature. The close relationship between GCHQ and the NSA has built on historical ties. The new kid on the block, but coming right into equal top place, is Australia with its Defence Signals Directorate, which is its GCHQ equivalent. Unlike in Britain, where our GCHQ does not sit in the MoD, their DSD sits within their MoD. That is their national centre of excellence. The primary relationship that we have internationally is between the United States, ourselves, and Australia—the three Departments of Defence. That memorandum of understanding between the three of us really opens the doors to closer co-operation between the three of us. The ambition now is to make that memorandum of understanding actually substantive in terms of operational co-operation.

Here we run up against one of the issues, which comes back to the point that we mentioned earlier about stove-pipes. Whereas Australia and Britain find it very easy to co-operate together—they have similarly fluid legal arrangements and one national centre of excellence, so agreements can be made fast ***

***We have good talks with France, but, again, we have hit problems that are familiar from other areas where we are working with France. *** What you will note about what I am saying, though, is that we are starting to talk now about bilateral relations, because we find that bilateral relationships are where you can make progress. The more people you have in the group, the harder it is to make progress. That absolutely is epitomised by the problems that we are facing in NATO, trying to get agreement on this. The NATO team is very much run by the Estonians, because they are the people who have been stung the most, so they have put the most effort into it. They are in what I would describe as post-attack mode, and they are determined that it should never happen. I sense that the rest of us are slightly, in national terms, rather hoping that it does not happen and not taking it quite as seriously as perhaps we should. In terms of creating unified NATO policy, I think that is a very slow boat indeed. That policy is coming along, like all NATO policy, at the speed of the slowest runner. There is, therefore, reluctance to sign up to very strong NATO-wide protocols, which is regrettable, but that is symptomatic of the problems you have with an alliance of that size.

Q44 Bob Stewart: Would we really want it—the NATO-wide protocol? Could we trust it?

Major-General Shaw: These are the questions, aren't they? None the less, the fact remains that NATO, if it is to operate as a unified alliance, needs to trust its systems. It needs to be able to trust all the people who

are buying into that system. Setting standards within NATO is proving very difficult. The question was mentioned in open forum about setting standards; setting standards and measures of effect in cyber-space is an extremely difficult task, which, frankly, Government have not answered yet. No Government really have, to my mind; I have never seen a satisfactory set of metrics for what success looks like in any concrete terms.

Air Vice-Marshal Rigby: Just to emphasise a couple of points, Commander JFC *** went to the States specifically to look at the cyber challenge, in the week that Commander JFC took up command. I hope that emphasises *** important it is to Commander JFC to get a grip of this and to move forward with the Americans.

Q45 Chair: Okay. Thanks. So when John Bassett said to ask what the metrics for success are, you would say, "There aren't any."

Major-General Shaw: Best effort, I am afraid. If you asked me what the risks were, I would say it is the potential for incoherence or uneven response across Government with regard to how much effort people put into their defences. Given that the nature of cyber is that it exploits the weakest link, there is a very real problem with the potential for there being an uneven response across Government. This issue has been given to the CIO of MoD to suggest some standards, and I know he is working on that topic. People are aware of the question and they have given it to John Taylor in the MoD to sort out, but I do not envy him his challenge.

Air Vice-Marshal Rigby: I think we could get some metrics, but they would not be end-benefit metrics, if you know what I mean. They would not say how good we were at cyber or how bad we are at cyber, but one would perhaps look towards how many trained personnel we have got towards a trained standard. We might look towards how many contingency plans we have that have got decent cyber-annexes, and how many options we have on the shelf in order to conduct an offensive cyber-attack. The metrics would not say whether we were good or bad, but they would give milestones towards us progressing the cyber-agenda.

Q46 Chair: So it would be an input agenda rather than an output process agenda.

Air Vice-Marshal Rigby: Yes, I think so. It is always the problem with things such as intelligence, because it is almost Rumsfeldian.

Chair: That is a new word I have not heard before, but I understand what you mean.

Air Vice-Marshal Rigby: You might want to look at the gap between malware being detected and your ability to put a patch in accordingly, even though that goes towards the information assurance thing. There are a lot of input measures that are of value, but output measures are going to be tending towards impossible to get, and we would just waste our time, I suggest, trying to find those.

Q47 Chair: Okay. Do you mind if we ask you all the other questions about a chain of command, the roles of the joint cyber units, and the relationships with the DCOG and the GOSCC in writing? That will save time now.

All witnesses: Yes.[1]

Chair: Now I want to move on to Madeleine Moon's question.

Q48 Mrs Moon: We have got lots of Government Departments, each responsible for different aspects of their departmental security. Are there rules of engagement that decide which cyber attacks the Ministry of Defence will respond to, or is it only an attack that affects the Ministry of Defence directly in its services? What are the principles on which you make that decision, and who makes it?

Major-General Shaw: The Ministry of Defence's remit is limited. Effectively, it is to look after its own systems and to prepare capabilities to be used in case of conflict under the law of armed conflict, so our remit is quite limited. In terms of protecting the national infrastructure, that resides with another Department. The CPNI looks after that. Our remit is quite simple, and it is quite clear when MoD would or would not be involved. The exception to that is, as with any national disaster, if the effect of the attack is such that central Government in their normal way decide that they want military assistance: the normal rules of MACA apply and the MoD might become involved. As I say, if the nation feels that it is under attack, cyber is merely the latest golf club in the golf bag of potential responses that UK Ltd might use. So standard procedures apply.

Q49 Mrs Moon: So it would not be altered by, say, the motivation of the attack, the nature of the attack, the target or the impact? If the whole national infrastructure, as you say, was taken out, the Ministry of Defence might be called in purely because of its personnel capacity, rather than because of a particular skills base?

Major-General Shaw: I think it depends on the nature of the attack and the proportionality. There are all sorts of issues. What you are implying is that the MoD would respond in some way and then the issues of proportionality, attribution and intent all come into play. Those are very real and particular problems with executing cyber-responses to an incident.

Q50 Chair: Is a cyber-attack considered to be an article 5 attack under NATO?

Major-General Shaw: I think that is a political judgment about the severity of the attack and how big it was.

Q51 Chair: So it could, potentially?

Major-General Shaw: I see no reason why it couldn't be.

Air Vice-Marshal Rigby: I do not believe that Estonia quoted article 5 when it was attacked by Russia, so I do not think there is a precedent for that.

Major-General Shaw: But potentially it could. The danger that that question exposes is that we get obsessed with the means by which the effects are delivered. The key thing about cyber is to note that it is a new domain through which to achieve an effect,

[1] Ev 44

and it is the effect that matters. Just as you can rob a bank with a pistol or through cyber, the critical thing is that the crime, the robbed bank, is the effect. Could a cyber-attack lead to an article 5? Of course, if the effect of that attack is so severe that it is judged to be an article 5 attack. So it is the effect that matters, not the means through which it is delivered.

Q52 Bob Stewart: To follow up that point, who in our country—it is not just the Ministry of Defence, it is all the other Departments, too—is actually sitting there 24 hours a day on the operations desk and saying, "We're under attack! This is something the National Security Council needs to know about now"? Where is that desk or that position?
Air Vice-Marshal Rigby: That is physically at Cheltenham—it is CSOC—but it is a pan-Government agency.

Q53 Bob Stewart: But there is some person, not just a panel?
Air Vice-Marshal Rigby: Correct.

Q54 Mr Donaldson: Gentlemen, what can you tell us about the nature and extent of the cyber-security threat to the MoD's assets, networks and interests?
Major-General Shaw: I'd answer in the same way that I have already indicated. Cyber is merely the latest means that people are using to achieve the same effects. As David Omand said: espionage, subversion, disruption and attack. All the traditional effects that people have tried to achieve against us they will now try to achieve through cyber-space. Those are ongoing.
***
Mr Donaldson: ***
Major-General Shaw: ***

Q55 Mr Donaldson: And those *** would you describe those as direct targeted attacks on MoD systems, rather than generic attacks?
Major-General Shaw: It's a combination of the two, I would say.

Q56 Mr Donaldson: So even within the *** only some of those would be direct targeted attacks.
Major-General Shaw: That's my judgment.
Air Vice-Marshal Rigby: I think another way to come at the problem is to recognise the vulnerability, both of the networks and of the systems—the air, land and maritime systems—because they are connected, they do have computers in them and, as soon as you connect to the internet, which you might need for operational reasons to get your operational agility going, you have a vulnerability. We don't wish to sweep the vulnerability under the carpet. We need to recognise what the vulnerability is and then protect against that vulnerability. Then the threat is an entirely different approach, which is why I think we need to be linked up to the intelligence agencies to be able to guard in the longer term, and in the short term, against those threats.

Q57 Mr Donaldson: Looking back over the past five or 10 years, how do you assess the change that has taken place in terms of the nature of the threat? How do you expect it to evolve over the next five to 10 years?
Major-General Shaw: The first thing to say is that over the past five to 10 years, our dependence on cyber-space for the business we do has become much greater. Cyber-technology, the digital technology, has become ever more ubiquitous. Hence, we are ever more vulnerable.
Plus, technical developments continue apace. They continue on both sides. On the offensive, there is the malicious software, the criminal gangs competing with each other, the individual locked away in his room at 2 am competing with his mate across the road. That sort of stuff is spinning off the people trying to attack. Equally, the defensive technology has spun off as well. That competition will grow and continue for ever.
Over the next five to 10 years, I think exactly the same is going to happen. I can only see us becoming ever more dependent on cyber-space and the competition between the offence and the defence will continue throughout. The critical response to that is not to abandon cyber-space because it is too dangerous, nor fling our hands up in horror because it is too difficult. All organisations and all people need to make a very severe and clear judgment on what is their vital information that they really want to lock away, and what level of risk they are prepared to take with all their information.
It is like household security. You have garden furniture out there that you take the risk that no one is going to nick. You have got stuff inside the house; you then have got your crown jewels that you lock away in your safe. You have equally got something that you probably lock away in the bank in the town. You have different levels of security because you have looked at your physical possessions and decided how you want to secure them.
Cyber is a distracting word. When I start my speeches on this I always say we are not talking about cyber, we are talking about living in a digital age. The digital age is all about information. We all have a duty—in defence as everywhere else—to prioritise our vital information and to give it the requisite security. That means that what you have is a graduated response, because you can't defend everything. You take risks on certain bits. That's how you cope with a penetrated system, ***. They live through it; they don't bother trying to secure it. They just accept that it is penetrated. We all do the same thing in our daily lives. I see this as part of getting used to living in a digital age, getting used to this sense of security, and making very clear commanders' judgments about what information is vital and how tightly you are going to protect it, and what bits we are just prepared to operate. As John was saying about using the internet, you need to use it but accept that it is vulnerable. That is just the way we will have to learn to go about it.

Q58 Mr Donaldson: Presumably that changes as the nature of the threat changes and we learn lessons.
Major-General Shaw: Absolutely. It is a very fluid environment and we have to remain very agile on this. One of the difficulties about the nature of the earlier

question, about what our planning assumptions are, is that that implies a sort of top-down, directive approach to what we need. The reality is that we are playing it on more "recce pull", if I can say. In a sense, we are all too old to play this game. We have to listen to the people at the coal face and the young kids who are doing this. They are going to be telling us the reality, and we will need very agile policy decision-makers to keep up with the reality of the threats facing us. If there is one risk that was mentioned earlier, it was about pace, and it is the fact that the threat is evolving probably faster, I would say, than our ability to make policy to catch up with it.

Q59 Mr Donaldson: With that evolving threat, looking ahead, with state and non-state actors, to what extent do you think they are developing the capacity to weaponise this kind of cyber-space cyber-activity? Is it premature or hyperbolic to talk about cyber-war?
Air Vice-Marshal Rigby: To answer your first question to a degree, standing here, looking back five years, we have seen cyber-attacks on a nation-to nation-basis, on an oligarchy-to-nation basis, and cyber-espionage—serious levels of those sorts of things. Ten years ago, we would not have been debating that sort of thing, so it is real.
We must recognise that cyber is essentially an asymmetric form of warfare. So it is far easier to go on the offensive than defend against all the threats that are out there. Thus, I think people will be developing things—bespoke military-grade, if you like, cyber-threats—but a lot of them do not need to. A lot of that capability is already out there on the internet, and it may well be that the vast volume of the threats coming our way is from people who pick stuff up on the internet, and that is the volume we need to defend against. That does not mean that there isn't going to be a Stuxnet-type thing with our name on it, but there is a volume-against-complexity thing that we are going to have to face. What is really interesting is the point Mrs Moon made about motivations, and I think what we need to look for over the next zero to 10 years is the motivation of people with these tools, and how they might choose to use them against critical national infrastructure.
Major-General Shaw: You asked the question about weaponising cyber-space. The language implies that there is something evil about this, but I would turn it on its head: given that we are going to have wars—they keep happening—and that our current ways of taking out enemy capability involve kinetic destruction, which involves collateral damage and civilian death, if there is a technical option that would allow us to achieve the same effect on a Government, with no loss of life, you could turn the argument on its head, saying that there is a moral argument about why we should develop these, because they are a more humane way of conducting competition between states. I just offer that thought.

Q60 Mr Donaldson: Okay. Is it just a moral argument at the moment, or are we beyond that?
Major-General Shaw: No, I think there is quite a good practical argument for doing it as well. However, I do not think we should underestimate—we were talking about Stuxnet earlier—the difficulty of creating these weapons or weaponising cyber-space. The intriguing shift that we shall see is that, whereas Stuxnet, as was described in the open forum earlier, was very much tailor-made to the target, it may be possible to create a rack of off-the-shelf options that you can apply, or it may be that all cyber-targets are going to be, almost by definition, bespoke. That is a very interesting technological development, which we are all considering at the moment.

Q61 Mrs Moon: Are we maintaining technologies that otherwise we would have thought of as redundant, in case we need to bring them back, in the event that we need to operate without cyber-capabilities? I am thinking of something like Morse code.
Major-General Shaw: I think the nation has moved beyond reversionary modes, and we need to face that fact.

Q62 Mrs Moon: But are there differences between the forces, in terms of how reliant they are on network infrastructure? Is the RAF, the Army or the Navy more vulnerable?
Air Vice-Marshal Rigby: I'm not sure. It depends on how modern the systems are that each of the services is operating. The Joint Strike Fighter is completely dependent on computer wizardry, but I imagine that the next generation of the Combat Vehicle will be equally dependent.
Practically—this is something that defence has to get its head round as it moves from fighting in Afghanistan towards contingency operations again—we have to go back. In the cold war we made sure that we could cope without our principal systems. We must have fall-back and contingency methods of operating, particularly in command and control. I think the Americans will be particularly stunned by this. Where they have complete situational awareness, they will have to learn and understand again how to operate without it.

Q63 Mrs Moon: Are we still teaching map-reading?
Air Vice-Marshal Rigby: Oh yes.
Major-General Shaw: Oh yes—at one of my schools.

Q64 John Glen: One of you used the analogy of different levels of security within a home. I want to push that a bit further. Clearly, there are relationships between what you have in the bank and what you have in the safe in the home, and what you have in the garden. The same is sort of true in terms of having an operational environment that can exist at a tier 1 level of risk that would be satisfactory, to the extent that if all environments were compromised, you would still have sufficient resources within a very tight core. Is that a sensible way in which to look at the necessary levels of completeness that you need?
Air Vice-Marshal Rigby: ***

Q65 Chair: What can you tell us about the offensive use of cyber? You have mentioned it, so it must exist.
Major-General Shaw: And clearly it does. You can do offensive cyber in many ways. The kinetic bomb is quite a useful cyber weapon in that if it destroys a

node, it takes down the communication network. You therefore achieve a cyber-effect, which comes back to what I said earlier about effects. Effects delivered via cyber-space is one of the areas in which we are trying to play catch-up. One of the big difficulties with it is that it depends very much on knowing your enemy. Even when you have worked out what target you want to attack, the lead time for preparing the target set can be quite long. Then it needs policy decisions about whether you wish to do what inevitably becomes more invasive technological intrusions, if you like, into other systems with a view to downstream activity. The pre-planning required for offensive cyber should not be underestimated.
***

Q66 Chair: Is there any deterrent value in cyber-capabilities?
Major-General Shaw: There may well be, but it is early days. The deterrent value of cyber is overstated at the moment, because there are huge problems with attribution. To take the simple example of Estonia, to all intents and purposes, the attack on Estonia came from California. It makes it extremely difficult. Until you attribute it, until you can work out a proportionate response and definite intent, it is a murky area. We should be hesitant to leap straight to nuclear deterrent, to theology, and apply it to the world of cyber.

Q67 Chair: That may not work any more, either. I gather that to all intents and purposes, the cyber-attack on Georgia came from the American state of Georgia, which is amusing.
Air Vice-Marshal Rigby: I think Estonia is a good example. It is, I think, the most connected state in Europe, and yet the attack did not stop Estonia from working. I think we have to recognise that, with that as a sign of what a big cyber-attack can do, perhaps it is not that great a deterrent.
Chair: Okay. We have no more than five minutes left.

Q68 John Glen: In terms of developing cyber-capabilities, how will that differ, from your perspective, from developing conventional military capabilities? Is there a cyber strand within defence lines of development, for example?
Air Vice-Marshal Rigby: ***In terms of information protection, that is a defence line of development and would be run through the usual defence methodologies and prioritised accordingly.
***

Q69 Chair: Is that a joint computer unit?
Air Vice-Marshal Rigby: Joint cyber-unit? No, it is beyond that. It is in the programme board structure that we are working with Cheltenham.
Major-General Shaw: Yes. It has to be a national response rather than an MoD response, because the tools are very similar. It is more about the application.
Air Vice-Marshal Rigby: The joint cyber-unit is far more about the *** as opposed to running the programme for capability development. When we normalise it in four years—all the money is coming on top of this money at the moment—we will have to work out how we conduct business then.

Q70 Chair: David Omand's question: what are the priorities for cyber-security within the Ministry of Defence and the Government as a whole? Do you think that those priorities are the right ones? Do you think that cyber is high up enough in the priorities of Government?
Major-General Shaw: Having cyber as one of the top four priorities is absolutely the right place for it. We shall see with PR12 whether it has a high enough priority within defence. We still do not know, as the results of that are still embargoed, but it hints at a wider risk that I think exists across Government: the difference in funding for each Department.
Whereas the national cyber-security programme of £650 million was money for new stuff, that was merely the tip of the iceberg. Far greater than that is the bill that every Department faces for looking after its own internal security of its existing systems. That money was for Departments to allocate, and one of the greatest risks I see in the entire national response to the cyber-threat is an unbalanced response, where there is new money for new stuff, but Departments, which are so strapped for cash, will not give sufficient priority to the security of legacy systems and new systems. That is a much bigger part of the iceberg underneath the water.
That challenge exists for the MoD as well. Certainly, last year, in PR11, we bid for new money from defence for the other part of the cyber equation. We got nothing. This year, we made a more modest and more realistic bid—we hope. It is still surviving and it is still there. I do not know if it has finally got over the line; we shall see. I think that illustrates the real challenge we face and the danger that there is an unbalanced response across Government on this one.

Q71 John Glen: Which inherently creates a new risk. If you have vulnerability in one Department that has chosen not to or is not able to achieve internal defence, you could create a bigger concern for the core, combined entity. Presumably, the combined entity must be assessing those risks across different Departments.
Major-General Shaw: Yes, you would hope so.
Chair: I think we will leave it there. Thank you very much indeed. That was very helpful and most interesting. We will, as is usual, give you the transcript of this for redaction before any publication takes place. We are most grateful.

Wednesday 16 May 2012

Members present:

Mr James Arbuthnot (Chair)

Mr Julian Brazier
Thomas Docherty
John Glen
Mr Dai Havard
Mrs Madeleine Moon
Penny Mordaunt
Sandra Osborne
Ms Gisela Stuart

Examination of Witnesses

Witnesses: **Nick Harvey MP**, Minister for the Armed Forces, **Air Commodore Tim Bishop**, Head of Global Operations Security Control Centre, and **John Taylor**, Chief Information Officer, Ministry of Defence, gave evidence.

Q72 Chair: Minister, I am checking to see whether we are allowed to begin even though it is 2.29. I think that we will just throw caution to the winds and begin. Welcome to the first inquiry into defence and cyber-security, which is part of the series of emerging threat inquiries that we are doing. We have already received some very helpful evidence from the Ministry of Defence and from industry. Would you be kind enough to introduce your team?
Nick Harvey: Thank you very much, Chairman. On my left I have Air Commodore Tim Bishop, who is Head of the MoD's Global Operations Security Control Centre, and on my right is John Taylor, who is the Ministry's Chief Information Officer.

Q73 Chair: Thank you. We will be taking evidence, in due course, from Francis Maude, the Cabinet Office Minister. Talking of which, how does the Ministry of Defence communicate with the Cabinet Office, the National Security Council and other Government Departments about cyber-security?
Nick Harvey: Thank you. I am aware also that you have seen Major General Jonathan Shaw and Air Vice-Marshal Jonathan Rigby in private session. You will understand that there are limitations on some of the things that you might want to explore with me in a public session, but if we run into any difficulty—
Chair: Alert us to it, please.
Nick Harvey: The co-ordination across Government is, as you say, through the Cabinet Office and the small full-time unit they have looking across Government at cyber-security issues. I am also on the ad hoc ministerial group that brings together different Government Departments for discussions across the cyber agenda. John Taylor is on an officials group. John, do you want to explain your role across Government?
John Taylor: In my role as CIO in the MoD, I also have a number of cross-cutting roles pan-Government. One of those roles is developing a cyber and information risk management regime, which is being developed on a pan-Government basis. I have set up a working group—essentially—to take that forward, which has interdepartmental representation. I am also doing work in the context of the Government's ICT Strategy on the Public Services Network, which is also concerned with cyber-defence. In that role, we are taking forward, on a pan-Government basis, a work strand which looks at what cyber facilities we build into that Public Services Network effort. In that context, we are working very closely, not only with the Cabinet Office, but with the likes of the DWP, HMRC and the Home Office. That is all brought together under what is known as "the Chief Information Officer Delivery Board", which is chaired by the Government CIO, so we get good interdepartmental working in that forum as well.
Nick Harvey: On a regular basis, we are essentially in a reporting relationship with the Cabinet Office on the Defence Cyber Programme, and we report to them monthly on the progress of that.

Q74 Chair: Would you not describe the Cabinet Office as a co-ordinating Department rather than an executive Department? The thing that concerns me is that it is quite hard to see from this diffuse and slightly vague organisation that I am hearing about who is actually in charge of doing something.
Nick Harvey: I think that an analogy might be drawn with the COBR principle. When there is some sort of an incident anywhere within Government, the Cabinet Office has this COBR capability that kicks in. In and of itself, it does not have a great organisational empire at its disposal, but it has a co-ordinating role among other Government Departments, which have the mechanical functions. In a sense, I think, in the cyber sphere, the small unit in the Cabinet Office operates somewhat similarly. The principal levers at their disposal actually reside in GCHQ. That is where the serious firepower would come from to deal with things in a practical sense. The small group in the Cabinet Office has, as you rightly say, a co-ordinating function and a policy function, but is not running, hands-on, a big Department or capability.

Q75 Chair: GCHQ is the responsibility of the Foreign Office?
Nick Harvey: GCHQ is principally the responsibility of the Foreign Office, but it has a cross-governmental role in this area.

Q76 Chair: So should we have a Foreign Office Minister in front of us?
Nick Harvey: You certainly could do, if you wanted to know more about that.

Q77 Chair: Is information sharing across Government enough for what the MoD needs? Are

there occasions when the MoD does not get what it needs from other Government Departments?

Nick Harvey: As well as the mechanism that I have described going through the Cabinet Office or indeed through GCHQ, we have some bilateral contacts with other Government Departments. Where relevant, we would flag up to them any concerns we had or anything we had discovered that was going on that we thought other Government Departments needed to know about. The point I am making is that there is joint Whitehall architecture but there are also direct Department-to-Department links as and when necessary.

Q78 Chair: But you cannot call to mind any particular instance in which there has been a failure to share information. Is that right?

John Taylor: I think that is generally true. In any process where information is being exchanged, glitches occur from time to time. That sometimes happens because quite a lot of the material that informs our response in cyberspace is highly classified. We are taking steps to build on the work we have done over the past couple of years in particular with GCHQ to improve those information flows. I think we are already seeing considerable benefit for that in our day-by-day, 24/7 cyber-defence operations. The Air Commodore might wish to comment on that in general terms.

We are still building that information-exchange capability, but it is moving forward quickly; it is getting better quickly. Certainly, I am not conscious of any major incident that has caused the MoD any particular problem in this space.

Air Commodore Bishop: Building on what John said, at the tactical level, the information exchange and sharing of information is very good. We also share, for want of a better word, our tradecraft: tactics, techniques and procedures, and the way we would address issues when they arise. We also share staff. We have some staff embedded at GCHQ, for instance, ensuring those ties are tight. They also exchange staff with me. We also do that with the cyber-security operating centre, which is the bit that sits above at the top level and directs what happens across other Government Departments, should we have instances down at the tactical level. At my level, it works very well. No instances spring to mind of when not having information has caused me and the MoD an issue.

Q79 Chair: In 2011, the Cyber-Security Strategy was produced. How are the different Government Departments getting on with achieving the goals of that Strategy? In relation to that bit for which the MoD is responsible, how are you doing?

Nick Harvey: In a sense, I and the Ministry, and perhaps to some extent John Taylor does, but the MoD is essentially responsible for our own piece of it. You might want to explore with Francis Maude, when you see him, his analysis of the other parts of Government, but we are responsible for delivering the Defence Cyber-Programme, which in the first instance is principally about protecting our own Defence networks against any cyber-attack or penetration. We also have responsibility for evolving the UK Government's capability if they thought it necessary to take any proactive, disruptive steps to deter anybody from attacking us.

So I believe that we are putting together our capabilities well. We are trying to ingrain in and throughout Defence a higher degree of awareness of the cyber-threat and to work into everybody's thinking the challenges and opportunities of the cyber domain, but this will clearly take time. So far, so good, but it is a programme that will take us through to 2015. In a fast-changing arena, we have to be as agile and as fleet of foot as we can.

Q80 Sandra Osborne: I would like to ask you about demarcating the role of the military. What principles have been developed for determining whether the response to a particular cyber-security incident will involve the Armed Forces?

Nick Harvey: In the event of some sort of cyber-attack against the Government, the co-ordinating role for a response will be exercised by the Cabinet Office. I previously drew the analogy with the COBR operating principles. Depending on the precise nature of the attack and which parts of Government networks were subject to the attack, a lead Government Department would be appointed. Other Government Departments would render any assistance that they could. Our principal responsibility is for Defence's own networks. We would be the lead Department in that event, but if there were an attack on another part of Government and we had any relevant expertise that we could contribute to their dealing with it, we would do that. Depending on the scale and severity of the attack, it might well be that Cobra would meet and bring together Ministers and/or officials from the relevant Departments to co-ordinate the Government's response. The principal standing responsibility is for our own networks.

Q81 Sandra Osborne: Can you say a bit about how the understanding of the military role has evolved? How does it compare with that of our allied nations?

Nick Harvey: I have talked to a number of allied nations, and the way cyber-defence is organised differs quite a bit from country to country. Some of our allied nations base most of their cyber-defence within their Ministries of Defence, but because GCHQ is genuinely a world-class capability, the British Government put the central function in GCHQ's hands. We work extremely closely with GCHQ. We have people permanently on site with them, but they are performing the central role that in some of our allied countries would be exercised somewhere within the defence arena.

Air Commodore Bishop: We would provide support in the way that we provide military aid to civil powers if we are asked. We have a lot of experience that we can bring to the table to provide help, and we have capabilities such as forensic capability, technical-support capability and computer emergency response team capability that can be used across a range of scenarios to allow us to deal with or recover from incidents. We are there if we are asked to help, but we are not necessarily leading the way there. We are

defending our own networks, which, in itself, is a fairly large task.

Q82 Sandra Osborne: As you say, you closely collaborate with GCHQ as a national centre of expertise in the field. What implications does this relationship have for command and control arrangements, accountability and defining rules of engagement in cyber-operations?

Nick Harvey: We have our own command and control arrangements within Defence which cover our aspects of this, but the command and control arrangements across Government are as described through GCHQ and, specifically, the Cabinet Office. I don't think we have experienced any problem with this. We don't feel any lack of ability to control those things which we need to control, nor do we feel that we have responsibility for things over which we don't have control. So my sense is that our current arrangements are working pretty well. That said, this is a fast-evolving area. We will constantly be looking at what we are doing and seeing whether there are ways that we ought to improve it. But at this time, I am comfortable with the arrangements that we have got.

John Taylor: Perhaps I could add to that, Minister. In terms of our own network defence, some two years ago we put in place a number of what we call network authorities: people who have assigned responsibility in the network space. Currently we have three. One is our network capability authority, which looks at future systems to make sure that they are, if you like, cyber-proofed. We have a network technical authority, which looks at systems that are going to come and use our networks to make sure that they are not going to cause any new vulnerabilities, and we have the network operating authority, which is the role that Air Commodore Bishop fulfils. We have set that up as an enduring operation within the Department that is working 24/7, 365 days a year under the express direction of the Chief of the Defence Staff.

Air Commodore Bishop: From my perspective, in terms of running the operational piece, if I provide my resource to support GCHQ or someone else, they are in a support role in support of the mission of whoever it is. If they provide resource to me, they are in a support role in support of my mission. So my C2 is very clear. If I transfer any of the resource from the MoD to help, the C2 is through the Department that is gaining the resource for however long they need, not going in and running it from a C2 perspective. It is a support arrangement change.

Q83 Sandra Osborne: How much of your role in relation to cyber-security efforts is focused on the Olympics?

Nick Harvey: We are playing a support role here to the Olympics organisers, and we have seconded some staff to them to ensure that they have enough resource to deal with the assessed threats, but we don't have corporately a lead responsibility for that. However, we play our part as part of the cross-Government effort.

Air Commodore Bishop: To expand on that, we have had a number of people working with the Olympics cyber co-ordination team for about 12 months now, developing the standard operation procedures they will follow, their tactics and techniques—

Mr Brazier: Could you speak up a little?

Air Commodore Bishop: We have been working with the Olympics cyber support co-ordination team for the last 12 months, helping them develop their operating procedures, tactics and techniques to address any instances that may come along during the Olympics period. I have people who during the games period will be embedded into that team. They will have a reach-back to the Joint Cyber Unit down at Corsham, where the whole unit can lend support as and when required. But we are very much in a supporting role using the experience that we have to help the Olympics co-ordination team be as well prepared as they can be.

Q84 Mr Brazier: Can I ask what questions the MoD is seeking answers to in the review that is going on at the moment by the Directorate of Operational Capability?

John Taylor: I can comment in the sense that this is very much work in progress. It came about primarily as a result of some of the transformational changes that Defence has already embarked on, most notably in this context, the formation of the Joint Forces Command, which is a new arm made up from our three single Services but very much focused on what we call joint enablers for war fighting operations. With that development, which came out of the work that Lord Levene completed last year, the Vice-Chief was very keen to look at how the responsibilities of the Joint Forces Command in cyberspace were going to be positioned within the constructs that we had previously.

It is clearly important, particularly in relation to the last question on command and control, that we are absolutely clear where the responsibility and the accountability lie. So having such a big organisational change, we felt that the principal question was to look at command and control governance in this space. Because of the operational nature of what the Joint Forces Command will be doing, we felt that the Directorate of Operational Capability was best placed to look at this.

Q85 Mr Brazier: Why is global operations security still separate from Joint Forces Command—or isn't it? Have I got that wrong?

Nick Harvey: Joint Forces Command and CJO are responsible for military operations, but the protection of our networks is still—I think rightly—vested in the same teams who actually plan and manage our networks, which, in a sense, comes under the Chief of Defence Matériel. Tim is accountable to the Chief of Defence Matériel for the defence of our networks. We are very keen to sustain the principle that those who plan and provide for our future networks are the same people who defend them in terms of their security. We think that there might be dangers if different teams were responsible for that. That is why it is not part of the Joint Forces Command.

Q86 Mr Brazier: Is there not a danger that it all becomes rather defensive? One of the key things that

emerged in recent writings is the importance of this being seen as another battle space, not just as a matter of security.

Nick Harvey: I entirely agree with that, which is why we are trying to ingrain this deeply into defence thinking right across the piece. That is why Joint Forces Command is responsible for this, and it is certainly the objective of the Defence Cyber-Security Programme that we will bring this into the mainstream of everything that Defence does. I agree with you; I think it is another domain in which all our activities take place. I do not think that there is a danger that we will view this only in a very narrow, defensive sense. I think you are just alighting on one bit of the organisational architecture that happens to be responsible for that element of it. It is intended to be something that everybody, right across Defence, embraces and makes part of their daily business.

Q87 Mr Brazier: Just to narrow it down a bit, Air Commodore Bishop referred earlier to Corsham. Can we hear a little bit about recruitment practices there to seek out and hire people, and what sort of people you are looking for?

Air Commodore Bishop: Absolutely. There is a mix now. We need some people with experience—normally older people, probably like me—and we need some younger people who have got the dexterity with the modern technology and who understand it because they have been brought up on it. The unit is constructed with a range of military and civil service personnel. They are split at the moment so it is about 40% civil service and 60% military, with a military element that can go forward into threat—theatres of operation—if we have to, where currently we would not send civil servants. We have got a range of services in the military part. We are looking at people with intelligence backgrounds, we are looking at people with technical backgrounds and we are looking at people with police backgrounds, because there was always a forensic and potential police issue around some of the stuff that we do.

Q88 Mr Brazier: May I ask you specifically about the very, very high-quality TA signals unit that you have, who are all part-time and have a very exciting range of civilian jobs, including in several of the areas you just mentioned? Their strength has always been that they have had a part-time commander with a real civilian job. There is a rumour going around that they may be broken up and put in as part-timers in the back of full-time units. Is there any truth in that rumour?

Air Commodore Bishop: It is not a rumour that I have heard. I could not comment further, because I genuinely have not heard that that is the case. However, the reservists of course have a large part to play, not only in defending but in operating the network. We defend the network so that we can operate at a time and place of our choosing; making sure that the network is there when we need it is what the job is all about—the defensive side is to make sure that that can happen. So "operate and defend" is where the reservist units with the skills that are there come in—they have a part to play in both. We need to make sure in going forward that we do not look at one in isolation from the other; we need to mix them.

Q89 Mr Brazier: Forgive me, but I put it to you that the key to keeping really good quality people who earn their living in a different way is for them to have a command structure that is led by people who earn their living in a different way. Otherwise, what happens is that gradually the structure actually sheds the part-time element, because key decisions get made between Monday and Friday, from which they have been excluded or whatever.

Air Commodore Bishop: We run a 24/7 operation, 365 days a year, so it is not a Monday-to-Friday, nine-to-five event here. There is a part to play for expertise that comes in on a part-time basis in support, along with a full-time capability that is providing that 24/7 cover. There is a balance to be struck. I think that the two can go hand in hand—one does not necessarily exclude the other.

Q90 Mr Brazier: Of course they go hand in hand, but my final point is that you have to have a command structure that recognises it. Perhaps it is odious to make comparisons between Services, but the most successful of the three Services in keeping high-quality air crew on the reserve list is the Navy, precisely because the head of the naval air reserve is always a guy with a real civilian job, so he makes sure that the Navy, when it is planning aviation things, takes account of the fact that you want to use people who earn their living in different ways. That is just a thought for when you come to design what is clearly a new and exciting expanded structure.

Nick Harvey: We certainly recognise and are very interested in developing the potential for reservists to contribute in this area, because if they are working in other relevant fields, they will be developing a very interesting range of skills that we might not be able to develop in our own organisation. Therefore, the potential for them to add value to what we do is absolutely understood, and we are very keen to develop that further.

John Taylor: May I add a comment from a capability development point of view? I think that we have recognised within Defence—very much so—that the skills in this area are premium ones. Certainly, in my own area—I run all our security accreditation work, in which these reservists play a big part—we are seeing new opportunities coming along in the cyber arena for these individuals, so we are very much taking a holistic approach to their training and development, whether they are reservists, full-time military or civilian, to get the blend of premium skills that we need to do our best in this space.

Q91 John Glen: If people do not want to be a full-time reservist and they are not in the military or the civil service, but they have the skills that you need, do you not find your structure and the absolute constraints around those three pots of skills quite difficult, because on the outside people obviously earn a lot more money doing the sorts of things that you need? Do you think, going forward, that this could be a real constraint for you in having the depth and

quality of skills? Slightly secondary to that, in terms of the culture within the Services and this being seen as not quite the same as a typical military career trajectory might have been, are you having difficulties getting the people who were recruited on a different basis to adopt such career paths?

John Taylor: In terms of the overall career paths, our view for the short term is that it is a sufficiently new and exciting space and, although there are large differentials between what individuals can get outside compared with what we can afford to pay, whether they are civil servants or military, we are benefiting from the attractiveness of the role, and that is a plus in the short term.

My own view is that we have to look more to the medium and longer term because as the whole agenda starts to expand, particularly when the economy picks up and demand out there starts to increase, we will be more challenged. That is why in terms of the approach to how we man the overall capability, we are almost being quite agnostic about the source of the individuals if they have the skills and the training needed to fulfil the role. For example, I have military staff who work in my systems accreditation area. At the moment, they see potential opportunities when they finish their military career of coming back in and capitalising on the training and investment we have put into them. We obviously are trying to encourage that as much as possible.

Air Commodore Bishop: I can add to that from the Joint Cyber Unit at Corsham in that we have people—almost on a waiting list—wanting to take over from those who are there. It is not long before they are coming to the end of a tour when the phone starts to ring and say, "When is a job available? Who do I need to speak to, to come and get it?" They want to come because of the variety of the work. One of the things that we have been very keen with them is that they know what they have to do. They are authorised to do it. We would term it as mission command, and they are allowed to do their job within their authority. We also offer them a lot of variety: it can be the 24/7 operations desk; it can be forensics; it can be computer emergency responses; it can be the technical security teams that they can move around and do. We also invest very heavily in their personal training. For instance, last year we spent £400,000 on personally training members of the Joint Cyber Unit.

Q92 John Glen: To what extent do you think that that could be a pathway to a lucrative career outside and that, in fact, you will do a brilliant job in the short term to satisfy that demand, but actually in the medium to long term you will have a bigger problem because the people will go off? I am not suggesting that it is something you can easily solve. I am trying to draw out whether it is something that needs to be examined for the medium and long term.

Air Commodore Bishop: Absolutely right. It would be naïve if we thought that, having got some of the best training in the world and then somebody offers a big fat pay cheque, people would not decide to go. We do lose some, but we don't lose very many. A lot of them stay because they do enjoy what they do, and they do have the authority to do the job they have been put in there to do. They are trusted. I have to trust them, especially the youngsters because they are the ones who will see—

Q93 John Glen: Early responsibility.

Air Commodore Bishop: Absolutely. They also feel proud of being part of something that is allowing defence to work. If we can make sure that we protect the networks so we can operate when we want to, they actually have a core part to play and do. They are tied to the output of what they do, which is good to see. But we do lose some.

Nick Harvey: It is possibly worth adding that contractors are very important to our whole effort. Another part of the work mix at Corsham is representatives on site in a centre from the major contractors who supply us and with whom we are dealing. That is just another element.

Q94 Ms Stuart: Cyber security is a priority. When we heard evidence from David Omand, he said that the cyber security domain was put up as one of the top four national security priorities. Can you tell me where it sits in terms of priorities within the MoD, and how can I tell that that is where it sits?

Nick Harvey: Cyber is a very high priority for the MoD. The threat to our national security posed by hostile action through cyber space was clearly recognised when it was made a Tier 1 threat in the National Security Strategy. It also reflects the funding allocation to the National Cyber-Security Programme. We take it very seriously in Defence. We think that it is an important part and parcel of our planning ahead and our developing of doctrine and concept. We are also making further investment ourselves, over and on top of those pan-Government funds. We have added another £30 million of funding this year and another £18 million last year. I expect that the Air Commodore will be able to describe what we have been doing with that funding and the sense of priority that he feels that he is creating.

Air Commodore Bishop: Absolutely. This is funding that is coming on top of the funding that exists already for operating and for the current defensive capabilities, so it is new money in that sense. For instance, the money that became available last year to meet some emerging needs as the threat changes was used to improve our analytical tools, to bolster our boundary protection on the edges of our networks in certain areas and, importantly, to improve our overall situational awareness of what "good" looks like and what has changed from what "good" was, because that is the indication that we get. That money has gone into improving our ability to respond much faster and in a much more agile and focused way, so that we are not having to think, "What does that look like and what does that mean?" Instead, we are thinking, "We understand that we need to take these actions to ensure that we can operate the network." It is real investment to improve the availability of our networks as we go forward.

Q95 Ms Stuart: As it stands, would you describe the cyber threats as containable, or are they still an issue of concern?

Nick Harvey: I think that it would be bold to say that. It is a very fast-changing threat. We recognise how serious it is and that is why we give it the priority that we give it. We think that we are doing reasonably well in keeping on top of it, but one really does not know how it will evolve in the future, so one has to be aware of sounding too cocky about it. It is something to which we take a very cautious approach.

Q96 Ms Stuart: Given that we heard earlier about the interconnection across Government, the investment in it and how it is a priority for the MoD, how does your prioritisation compare with other Departments? Are you content with the priority that they give it or not?
Nick Harvey: Each Department has to make its own judgment on the risk that it is prepared to accept to its own information and the systems that it uses to process that. In terms of my dealings with ministerial colleagues who come together in the ad hoc group, there is a wide and growing awareness of the threat and the priority that the Government attach to it. Other Departments have come a long way in the past 12 months or so. John probably has a better view across Government than I have.
John Taylor: I would certainly echo that. I think that if you had asked me that question 12 or 18 months ago, I would have said that the MoD was not quite where it wanted to be, but quite a number of other Departments were not even where the MoD was. Now, as the Minister described, because of the investment we have made and are making, we are getting closer to where we want to be.
I have noticed in my dealings with central civil Departments that—I hesitate to describe it as the scales falling away from the eyes, but I think that there has been quite a lot of that over the past 12 months. What has been the driver of that? It is two things, or two interrelated things. One is, if I can use the term, the austerity measures that we are all having to cope with. That is forcing us to look much harder at how we can co-ordinate and join up to have a more collective response rather than an individual Department response. One ad hoc metric that I might use is the number of Departments that are very interested in seeing Air Commodore Tim's operation down in Corsham. We are entertaining quite a few people across Government and, increasingly, internationally.
The second big driver is the digital-by-default stance that the Government has taken in putting more and more services online, and getting a much better understanding of the risks, be they risks to the availability of the services, risks to the information being carried by the services or, if you are talking about payments or tax collection, your financial loss as a result of cyber incidents. All those things have contributed to that very significant change in situational awareness.
If I may continue for a minute, the challenge going forward is to come up with practical, cost-effective ways to tackle those—ideally, on a pan-Government basis, where it is sensible to do that. I do not think that each Department will necessarily be able to put the level of investment in. Actually, it would be crazy to do that, because to a large extent, we are all contending with the same range of threats from the low end all the way up to the high end.

Q97 Ms Stuart: As a matter of interest, how often does the ad hoc group meet? What is the pattern?
Nick Harvey: I suppose roughly quarterly.

Q98 Mrs Moon: £90 million was set aside for the Defence Cyber-Security Programme. What will you achieve with that money?
Nick Harvey: You are quite right—that money was set aside, but as I have described, we are putting further money in on top of that. What we are hoping to achieve through the Defence Cyber-Security Programme, as part of the National Cyber-Security Programme, is to mainstream cyber into all of our departmental business. That requires funding of the sort that I have described in order to push it right through the system, but we want to make sure that in all future development of military concepts, the cyber element automatically becomes part and parcel of how we do things.
I have no doubt that we will continue to make the sort of investment that I have described from last year and this year in our future planning rounds. It is about trying to improve our own systems and legacy systems, because there are a lot of small networks in defence that belong to another era. We must to try to make sure that we can protect all of that at the same time as looking to the future. This is why the whole thing is coming under Joint Forces Command. We must try to plan for a future in which everyone at every level thinks—yes—about the air, sea and land domain, but also about the cyber domain and the part it will play in future activity. By 2015, I hope we will be well on the way to achieving that—that it will become a bread-and-butter part of our business. It will be up to an SDSR and a National Security Strategy in 2015 to assess how far we have got and how much more of an investment we will need to make in it from there forward.

Q99 Mrs Moon: Staying up to date with technology, the potential attacks on your technology and the risks associated with that—is it an expensive business?
Nick Harvey: Yes.

Q100 Mrs Moon: It is not like the old days, when you could buy a car and keep it for 10 years—the technology outstrips your capacity. In fact, the moment you buy it, it is almost out of date. How will you ensure that funds are available to maintain security for the networks and maintain the cutting-edge nature of the products that you are using?
Nick Harvey: By bringing the whole cyber concern into the mainstream of what we do, we will ingrain it into all budgetary work, and every time we are assembling budgets for any significant programme, this will be part and parcel of it.

Q101 Mrs Moon: Sorry Minister, but are you saying that you are going to have separately identified resources for cyber, security, and securing networks?

Nick Harvey: I am envisaging a time when this is so absolutely automatic to everything we do that all the programme budgets we devise to do anything will include ensuring that we have the necessary defences in place to guarantee and assure what we are doing. I don't know whether my colleagues have anything to add.

Air Commodore Bishop: Going forward, just building on what the Minister has said, as we procure future services to replace the legacy, we now know much more about the threat, so within those programmes, we can bake in a certain degree of security and protection for the products and services that we buy, which is the way we have always done this as we procured new capability. There will still be a requirement, if we are to stay ahead of the game, to have specialist cyber units with specialist capability that sit above and beyond what is baked into the normal operational capability that we have. If we do not, we will fall behind very quickly, as you say.

A lot of that is not about buying technology for protecting and defending the networks; you need some technology to do some monitoring. It is what you have on those monitoring devices—in terms of the latest information that you need to have against this threat—that actually makes the difference. It is not just about the kit; it is about the other lines of development that you need supporting the equipment to make sure that you can take a defence-in-depth approach to cyber-security.

Q102 Mrs Moon: My understanding was that you constantly needed to have patches and things in place to ensure that the latest form of threat is dealt with.

John Taylor: If I may respond to that, this has again been a problem that any large Department has had, particularly when they have had a multiplicity of different systems doing different parts of the business. One thing that has perhaps been an unintended benefit of some of the more enterprise-wide approaches we are taking to our networks, information technology and the applications we are using is that we can, as the Air Commodore said, bake in up front the means to provide the technical security, and we can be sure that it is there across the board. However, at the same time, in terms of keeping that up to date, patching, and so on, you only have to do it once, rather than 200 times if you have 200 systems, and hope that all 200 system administrators will do it. So, we are getting some benefit from the fact that we are having to take an enterprise approach, if only to drive down cost. I think as we move more into the pan-Government agenda, we can capitalise on that approach further.

Q103 Mrs Moon: Does Planning Round 12 have a defence and cyber-security programme fund within it?

John Taylor: It does.

Q104 Mrs Moon: Is there a clearly identified, constant stream of funds set aside to tackle this issue?

John Taylor: There is.

Mrs Moon: Thank you. I have to say that, as a cook, baking up front makes absolutely no sense at all. Obviously a man who does not cook came up with that idea.

Q105 Penny Mordaunt: Following on from the resources to look at the planning processes for cyber elements of the next SDSR, could you talk us through what activity is taking place on that, with particular reference to how you are managing to take account of the pace of change and rapid evolution of threats and behaviour in cyberspace, for both the short and long term?

Nick Harvey: Yes. Our operational planning now includes consideration of the cyber dimension to any future conflict or scenario that we think we might find ourselves involved in, so we are ensuring that the cyber element is worked into all future force development. The two joint cyber units—the one at Corsham and the one that is linked into GCHQ and the unique capabilities that it provides—are part of the Defence Cyber-Security Programme. We hope that, in time, we will train more and more of our people to have a greater capability in this area, and to view it as part and parcel of what they do.

In terms of considering the future character of conflict, we are also funding a programme of strategic studies at the Seaford House think-tank, which is part of the Defence Academy, to look at the implications of developments in cyberspace in terms of the environment in which our future security challenges will be managed. So, you are quite right. The pace of change has to be recognised. We have seen significant changes in the cyber-environment, even in the 18 months since we conducted the Strategic Defence and Security Review. We cannot afford to let the grass grow under our feet, but we are really giving this an emphasis and an importance that it has not had before.

Air Commodore Bishop: Also, we can learn a lot—we do—and we share with industry colleagues. Although the aim of an attack against industry may be different from the aim of an attack against us, the techniques that are used to prosecute the attacks are very similar. So, they are having to deal with the same kind of thing that we are dealing with, but from a different perspective of the attacker in relation to industry.

The sharing of information between industry and us, and of techniques that we use to counter attacks, is a very useful way of making sure that we stay ahead of the game. It is not always about buying technology; sometimes it is about sharing information with each other and being open and honest, saying, "This is what we've seen. This is what we need to do." That is just as useful as the technology that needs to be there.

Nick Harvey: In terms of the relationship that we have with industry, during the Afghan conflicts the increasing usage of urgent operational requirements has shown how there can be a swift and agile response to a changing need. The relationships with industry that the Air Commodore describes are vitally important, and when necessity brings it upon us we will make sure that we can react very quickly, cutting through some of the normal processes in order to respond to a rapidly changing threat.

Air Commodore Bishop: To add to that, we talked about command and control earlier, and John

mentioned the Network Operating Authority. I have the authority vested in me, without recourse higher than me, to direct contractors to break all the contracting rules that we have in place if we have to do something very quickly to defend the network. I can direct them and tell them to go.

Q106 Penny Mordaunt: When you consider the whole horizon, scanning across the whole national security picture, would you say that that is as advanced and well resourced as it needs to be to help you to plan for the future?

Nick Harvey: I think it is adequately resourced. I acknowledge that it is going to have to make considerable further advance. To be honest, it is still somewhat in its infancy and at an early stage. The new priority that the National Security Strategy has given to this, and the National Programme, and the additional funding that has been put in place, recognise that there is work to be done if we are going to stay ahead in this area. We have been describing, during the course of this hearing, some of the means by which we are going about that, but there is a long way to go—I would not that deny for a minute.

John Taylor: There is a piece of work that I am currently leading, again in the pan-Government space, to give effect to the role of the Government's Senior Information Risk Owner. Currently, that role is held by Mr Watmore in the Cabinet Office. Only now that we have this much more cohesive pan-Government approach both to cyber and ICT have we put proposals to him, only six weeks ago, for how we could give him some machinery to enable that more consistent approach to information and cyber-risks across Government. You will see that coming into being over the next six to nine months.

Q107 Ms Stuart: You have got cyber-security successes, but nothing happens, and you will ask for increasing amounts of money to make sure that nothing happens. I have a twofold question. What metrics are you going to use to show that you have succeeded in nothing happening, and you lose interest because there was not anybody out there who did not attack you? What metrics do you think we should use in order to assess that you guys have been successful and still deserve the money that you have been asking for?

Nick Harvey: That is a very good question, and very well put. Because the threat is so fast-changing, it does make it difficult to measure the effectiveness of our defences. Any adversary is going to be looking for the weak point in our defences. It will look, as we were just saying, beyond our own infrastructure to that of contractors and others we rely on. It is almost trying to prove a negative. Perhaps John Taylor can say a few words about the modelling that we think is the best way of doing this.

John Taylor: This is probably the most difficult set of questions to answer. We have been putting quite a bit of intellectual effort into it, but we are not there yet. The first one I would cite, which relates to some work that we have been quite successful in in the Ministry of Defence, is on what we call maturity modelling. Inherent in that is the fact that you cannot look at just one piece: the technology, the people or the process. You have to look at them in the round. When we look at the cyber defence system, we are not just looking at the technology and the capabilities that we have there; we are looking at the people and their training, the organisational culture, the levels of awareness, skills and processes. We have done that in the information assurance space. It takes quite a bit of effort, but it does give you some quantifiable assessment of where the organisation is in terms of its ability to manage in the cyber environment. The difficulty comes when you try to relate that to the level of investment that you have put in. I think that is one of the challenges that we have still to overcome.

The second approach that we are exploring is putting ourselves in the position of someone who wants to attack us. Let us consider what information he or she might have available on our vulnerabilities. Let us then use our operational analysis expertise to try and get a better understanding of we look like to somebody outside. It is a bit like looking in the mirror. Sometimes you do not like what you see. On the other hand, it gives you that different perspective, a scenario-based perspective, and we can look at that from all the way across the various threats that we are contemplating.

More broadly, we are doing some work on metrics to give us positive evidence that we are as safe as we need to be. That involves looking at metrics in the business infrastructure space, making sure that we understand what assets we have and that we have processes that review information risk on a regular basis. We then need to look in the technology space, making sure that our information is backed up, that we have up-to-date antivirus software—all the hygiene things that you need to do. Then there is the people space—for example, is our security vetting process working properly? We do have to have concerns about the insider threat. I will not go into any more detail on that.

Q108 Ms Stuart: In that case, I hope you did not hear how David Cameron answered the question today about why Coulson was allowed to look at papers without having been security cleared.

John Taylor: Well, there we are—a good example. Then, of course, we have the physical environment: are we controlling access and so on? I think we are already quite mature in quite a lot of these things in the defence context. My challenge in the pan-Government context is perhaps to get some other Departments to pick up some of those things. We are going to be giving them some encouragement to take them up. That will, I think, give us a more consistent approach on a pan-Government basis.

Q109 Ms Stuart: I can see that from your point of view you look in the mirror and you get yourself to a stage where you like what you see, but how do you suggest that we as a Committee test whether you have been successful?

John Taylor: That is a very good question. I think one of the metrics that might be interesting—I am probably being a bit bold here—and that you might explore is this.

Ms Stuart: He's looking worried!
John Taylor: This is when my Minister might give me a kick under the table. We are looking at this from the point of view of the ratio of how much we are putting into protecting our systems and the information and how much we are investing in the systems themselves. In terms of that kind of metric, if a Department comes in and tells you that it is spending £1 billion on IT and nothing on protection, I would be very worried. I think if we came in and said we were spending £1 billion on IT and half of it was on protection, you would be worried, too. I have already narrowed down the problem space a bit. What I am really suggesting is that we need to develop some benchmarks in this space for what "good" looks like, and there are a number of ways we can do that, along the lines I have described.

Q110 John Glen: How will we avoid the situation in which any relative benchmark from the commercial, business world would be justified by you as not being reasonably comparative, because of the nature of what you do? How do we establish a credible way of doing this? Are there international comparisons? Are there best practices in other jurisdictions that would be relevant here?
John Taylor: There are certainly emerging standards in this space, but I would hesitate to describe them as mature. When we look to the commercial community, I see quite a variable space. The International Standards Organisation is starting to develop good guidance that sets the bar for the sort of hygiene levels we should have. When I look at other jurisdictions, other environments, the challenge is how attractive we are as a target compared with these other areas. That is why we are having conversations on this with our colleagues in the US, who are quite concerned about this issue, both in the defence context and in the national defence context.
Nick Harvey: It does rather depend on your attitude to risk. Commercial companies will want to protect, for commercial reasons, what they do, but in a sense it would not amount to a national catastrophe if some of that got out, whereas if you are dealing in some aspects of our national security, you have to have a more risk-averse approach than some elements of industry might feel they could get away with.

Q111 Thomas Docherty: I want to go back to one of the things that Mr Taylor mentioned. Clearly, our Armed Forces are more reliant on network technologies now than perhaps we were five or 10 years ago. How is the MoD specifically planning to mitigate the risks that that poses?
Nick Harvey: Belt and braces and backups—sort of defence in depth, I suppose you would say. By working with intelligence and security agencies to assess the threat to our systems. By putting in place, as far as we can, technical measures to protect ourselves, restrict access and protect key data from compromise. By carefully segregating the most sensitive systems, carefully patrolling the links and gateways between different elements of systems and ensuring elements are completely autonomous. It is almost a sense of replicating in the cyber domain some of the approaches we would take to security in the physical space. Tim, is there anything that you want to say about that?
Air Commodore Bishop: No, I think that sums up the way we go about doing the business, and then we are into the tactical detail of how you do each one, but the Minister has covered everything.

Q112 Thomas Docherty: In response to a question from Ms Stewart, you talked about a hierarchy of risk. There is obviously a hierarchy of protection. I would imagine that there are some things that are more important to protect than other things. Has the MoD decided its priorities for what needs to be protected? Can you speak to that?
Air Commodore Bishop: Absolutely. It is about the way our protections are designed, they are in layers depending on the sensitivity of the information. The most sensitive information that we hold on our very secure systems does not have direct connections to the internet. The ones where we need to do a lot of business, for instance when we need to do a lot of work with industry, will have connections to the internet, and we will ensure that we can manage those connections and allow only the data through that we wish to go through. There is a lot of separation from our very close-hold information from the systems that genuinely work down at the internet-type level. That is how we go about doing it.
John Taylor: The other process that we have in place is that we have a fairly mature risk-balance methodology working within the Department. What do I mean by that? This is about when we identify a risk with a particular system or capability. We have a formal process for assessing that risk from the point of view of both an operational benefit and the information risk that might be inherent in operating a system in a particular way.
Whereas in the past judgments like that were taken on a somewhat more ad hoc basis, we now require projects and programmes to do a formal risk assessment looking at the benefit from operating in a particular way to the risk to the information or the people who might be using the capability. That is one of the processes that, in my role as the senior information risk owner for the MoD, we police quite systematically. So much so that I have probably taken upwards of 60 or 70 risk balance decisions on behalf of those programmes over the past two to three years. That has given us a very useful set of case law that we use to inform our risk appetite going forward. That very much complements the sort of thing that we are doing in the technical space.

Q113 Thomas Docherty: Following on from that point about the industrial interaction, it is a long-standing tradition that we have required our contractors and suppliers to take physical precautions to protect their estate and their interaction with the MoD. Can I press you to say something about what cyber-security measures you require the industrial supply chain to take?
John Taylor: This is an area that we are giving increasing attention to. I am not convinced we have got this quite right yet. As you rightly say, we are very

dependent on those suppliers. Having, if you like, got our own house in reasonable order, we are now starting to work particularly with our key suppliers to help them raise their game in this space. I am clearly not going to talk about any individual supplier but I think we are getting an understanding of what that landscape looks like.

Nick Harvey: It is also something that is being looked at on a pan-Government basis as well. The Department for Business, Innovation and Skills and GCHQ are working together to try to evolve a kite-marking system for suppliers to central Government.

Q114 Thomas Docherty: You will understand, I suspect, my slight concern at the very honest answer that we are not there yet. How concerned should we be? How long will it take us to get to where we feel comfortable?

Nick Harvey: We have very good relationships with key industrial partners. We share information with them. There is a mutual recognition of and understanding of the problem and a determination and will to help each other improve our defences. I think that the ingredients are there to get us to where we need to be, but it is a big task. As we have already commented a couple of times, there is an ever-changing, fast-evolving threat. You have to be very sure of yourself to say that you have cracked the problem. I think John Taylor is acknowledging that there is more to do.

John Taylor: There is also, if you like, a kind of institutional behavioural issue here. If you are sitting in a company that has suffered a cyber-attack that has done some damage, either through information or financial loss, the instinctive reaction is to want to keep that quiet. It is bit like the banks. We all know that they lose so many millions a year through fraudulent activity but it is never really talked about. Where we have got to now, at least from our engagement particularly with the big defence contractors, is recognition that they should not be shy in coming forward. We are seeing more of that now, particularly in some of the interactions that Air Commodore Tim's team has with companies. They can also reach out to us for help if they have a particular problem. Although I cannot talk about specific instances, there are certainly at least two cases where I have been directly involved when someone senior from a defence contractor has come to the MoD and said, "We have a problem; can you give us some help?" We are using some of our skills to help those companies raise their game. In direct response to your question whether you should be really concerned, I think it is something I would keep a very close eye on.

Q115 Thomas Docherty: You will be aware that we had your ministerial colleague in yesterday to discuss procurement. Off the shelf came up for debate. I also assume you will have seen Professor Omand's comments about striking a balance between off-the-shelf procurement and cyber-security. Minister, what is the MoD's approach to setting that balance between efficiency of purchasing and security? Is there a potential risk from off the shelf in the cyber realm?

Nick Harvey: There is certainly a potential risk; there has to be. It is always a question of balancing risk with the other factors you are going to consider. Obviously, price is one of those, but there is also speed and efficiency of delivery, how urgently necessary the piece of kit is, and the extent to which you have any known concerns about the product that the supplier is potentially going to supply to you. If it has any components that you have a concern about, you have quite a complex risk balance to perform. It is quite difficult to give you a generalised answer, but these are the components that you would weigh in any given situation.

Air Commodore Bishop: We use commercial off-the-shelf products in our cyber-defence systems.

Nick Harvey: There is no reason why you wouldn't.

Q116 Chair: No reason? If those commercial off-the-shelf products are made in China, does that give you any cause for concern?

Air Commodore Bishop: We are looking for a product that does a specific job for us, and if a product is available that can do that job in the way we wish to use it, there is no reason why we wouldn't use the product in that way. We would, of course, take advice from the National Technical Authority for Information Assurance on whether the product would allow us to do what we are trying to achieve.

Q117 Chair: You would not really know what was in it, would you?

John Taylor: In terms of our approach to this, it is, as the Minister said, very much about looking at the sourcing risks that you may be taking. There can be a number of factors in an assessment of sourcing risk. Clearly, if it were a piece of equipment that had an inherent IT capability for defensive purposes, we would look at the sourcing of that very carefully.

Q118 Thomas Docherty: Do we buy any of our equipment from the far east? Any of our IT or technology at product level? Do we know?

John Taylor: I think, in terms of end products, the answer would be no. I can let the Committee have a note, if I may, on a particular sourcing decision that we took on IT equipment some years ago.

Q119 Chair: That would be helpful, but we also need an answer in relation to the component parts of end products.

John Taylor: I will certainly try to give you as much as I can on the components, as well as the end unit.

Thomas Docherty: From the thoughtful look on the Minister's face—he always looks thoughtful, to be fair—can I assume that this is not something on which you have regularly had long discussions within the Ministry of Defence?

Nick Harvey: It is an issue we are aware of. What you are putting to us is not new, as is witnessed by the fact that a decision was taken on this area some years ago, but it is difficult to give you an answer that covers every scenario.

John Taylor: I would also add that, in this space, the question of sovereignty in terms of capability is very much uppermost in our mind. Again, in my note I can

give you an example of where there is a very active debate on that issue going on in a particular programme. I am afraid that due to the sensitivity, I cannot share that with you publicly, but I am very happy to give you a note on it.

Q120 Chair: That would be helpful. We have been talking about vulnerabilities, and there is a vulnerability inherent in relying on computer networks, but there is another vulnerability that we need to consider, which is our new reliance on just-in-time procurement. The Libyan exercise last year showed the extent to which industry was able to ramp up production and, thankfully, provide us at the last moment with some really sophisticated equipment that we needed. If industry itself were taken down by a cyber-attack, those defences would no longer be available to us. I wonder about the extent to which that has been factored into your relationships with industry.

John Taylor: That is very much at the heart of the concerns that I expressed earlier about not having quite got there yet in terms of having a complete, end-to-end view of cyber-vulnerabilities in our supply chain.

Q121 Chair: You need that, don't you?

John Taylor: That is what we need, because although our military colleagues are very self-sustaining, increasingly as we are acquiring these capabilities on a service-provisioned basis, there is the question of what happens if there is an outage due to cyber at the wrong moment. I characterise it in terms of our own internal networks. If you have a problem in the network—not necessarily because of a cyber-attack, but because of a fault—at 7 o'clock on a Friday evening, just before the Minister's box closes, that can be quite career limiting. I think we could be in a similar place from a war-fighting point of view as well.

Q122 Chair: Minister, in 2010 you made a speech—well, you probably made rather a lot of speeches, but in this particular one you said cyberspace was "a new domain" that "should be subject to the same strategic and tactical thought as a conventional military operation." In many respects, of course, it needs to be subject to completely different strategic and tactical thought, but I think you meant the same amount or seriousness of strategic and tactical thought. There are differences, however, and I wonder whether you would like to share with us your views about what those differences can be in relation to the cyber-domain.

Nick Harvey: I do very much view cyber as another domain for warfare. The US Department of Defense has evolved its thinking along those lines, and we are doing so in the UK Ministry of Defence. To treat cyber as another domain is not to try simply to make it separate from the land, sea and air domains—quite the reverse. The way we look at it is that we have potential adversaries who would seek to do us harm in whatever domain they felt able to.

I think that treating cyber as a domain sends a signal, if you like. It says to our commanders that they have to have their wits about them and recognise the threat—and also, possibly, the opportunity—presented by the cyber-domain. It is not just some technical specialism for which a bunch of experts can be unearthed from some remote MoD section; it is something that should be part of the equation and the military planning at all times.

I am convinced that increasingly this is the way everybody in defence in the UK and elsewhere will come to work this into their thinking. I suppose increasingly the defensive and offensive elements to this will come together and will be worked up into doctrine. It is helpful to think of cyber as a further domain, but everything that we plan for the future needs to have an understanding and a recognition of this in it. To that extent, it is part and parcel, and not separate, but I think it is quite a helpful way of viewing it to think of it as an additional domain.

Q123 Chair: Okay. I want to ask questions first about law, and secondly about deterrents. First, law: do you think the same legal principles apply to cyber-attacks and conventional attacks? You said in that speech that "the established laws governing the use of force and the conduct of hostilities are equally applicable to cyberspace as they are to traditional domains." I just wonder whether everyone agrees with you—and do you agree with you?

Nick Harvey: I certainly hold that view today, as I did in 2010. For me, the law of armed conflict applies as much to cyberspace as it does to any other domain of operation. The principles of proportionality, discrimination and humanity apply to actions that we might take in this domain, as they do elsewhere. We should focus on the intent and the consequences, rather than the means of delivering the effect. Similarly, I suppose, when you are thinking of Article 5 of the Atlantic Treaty, that could apply to an attack in cyberspace, just as it might be invoked for a conventional attack. Whether it would be appropriate—

Q124 Chair: Is that internationally accepted?

Nick Harvey: Who is to say? There are countries, as the Committee is probably aware, who would like, as we see it, to bog the international community down in some slow and doubtless long process of trying to negotiate new treaties and bring about new laws to apply in this domain. We do not believe that those are necessary, because we think that the application of existing law and norms of behaviour will serve us perfectly well. As I say, it is really a question of focusing on the intent and the consequences, rather than on the means by which you bring those about. I think this is what the Foreign Secretary had in mind when he invited people from around the world to London for a conference to discuss these very matters. I think it would be a mistake for the international community to feel that it needs to reinvent a legal code for this domain; it would distract us from trying to work together to evolve norms, which should derive from existing law.

Q125 Chair: Norms and rules of engagement. Will you be involved in that?

Nick Harvey: At this stage we have not sought to develop specific rules of engagement for cyber, but as our understanding of cyber-operations, their potential, their capabilities and the associated norms of behaviour develop and evolve, I could envisage us coming back to that and possibly devising specific rules of engagement at some point in the future.

Q126 Chair: By the time you have done that, won't it be far too late?
Nick Harvey: Well, that would be my concern about reinventing law here. By the time we had got 200 members of the United Nations to agree to some new law, the technology would have left it all far behind. That is why we are far better adapting existing machinery to this new domain, and for the time being we conduct ourselves in this domain as we would in another. If, as we learn more, we need to devise extra rules of engagement, then we will do that.

Q127 Chair: Getting back to Article 5, is it your view that the cyber-attack on Estonia would or could have given rise to an Article 5 declaration?
Nick Harvey: It is an interesting point. I cannot see in principle any reason why one would say with any certainty that it would not. Potentially, yes.
Chair: The vagueness of that answer—
Nick Harvey: Well, it is a hypothetical question.

Q128 Chair: It was not hypothetical, actually, because it did happen.
Nick Harvey: But the request wasn't made.

Q129 Chair: The request wasn't made, possibly because no one was sure what the answer could be. Does that not lead you to wonder whether it might have been helpful at least to have had discussions about whether that Article needed to be clarified?
Nick Harvey: Yes, I believe that discussion would be helpful. As I said, my starting point is that Article 5 could apply to an attack through cyberspace as it might to any other form of attack, but you immediately pulled me up, asking whether that was universally accepted, in which case there would be merit in having discussion with our fellow signatories.
John Taylor: I am no expert in the law on conflict, but I think I understand proportionality. I recall that the Estonian incident was about websites being taken down. The challenge we have is making judgments on proportionality. If the debate were centred on that, it might bring some clarity in this space.

Q130 Chair: Moving briefly on to deterrence, but still staying for a moment on Estonia, do you think deterrence works in the cyber-field?
Nick Harvey: I don't see why it would not. Perhaps as we go forward and there are more cyber-attacks, or attributable cyber-attacks, and people gain a greater understanding of others' capabilities, that will, perforce, begin to play into the psychology and logic of deterrence.[1]

Q131 Chair: But surely the point about cyber-attacks is that they are not attributable. Do you know who did the Estonian attack?
Nick Harvey: No, but we have a pretty good idea—
Chair: That was several years ago now.
Nick Harvey: We have a pretty good idea where attacks on our networks come from.

Q132 Chair: Yes, but it is quite difficult to prove it, isn't it?
Nick Harvey: Not necessarily.

Q133 Chair: Four years after the attack on Estonia, if we cannot be certain who carried it out, even though we have a pretty good idea, those people who carried it out could be forgiven for thinking that deterrence did not really work, couldn't they?
Nick Harvey: Why? Simply because of the apparent inability to attribute it?

Q134 Chair: Yes. Changing the subject slightly, if you had an electromagnetic pulse attack—we have done a report on that recently—it would be quite difficult to attribute that, wouldn't it? That would, or could, take down the entire network, couldn't it?
Nick Harvey: Yes. John might be better able to speak on this than I am, but in terms of cyber-attacks on networks, we can in many cases tell pretty much exactly where they have come from—not in all cases, by any means.
John Taylor: Perhaps I can try to answer your question in relation to an exercise that I took part in, which was co-ordinated by the Cabinet Office last year. It was a cyber-attack purported to have come from a particular country. It was directed at our UK networks and was particularly targeted at the oil industry. That was the context. Certainly in the exercise, one of the immediate challenges, given the time scale—the very quick impact that such an attack can have—was a question mark over the alleged attribution of where it had come from. There was some doubt, but the sense was that after a relatively short period—two or three days—the sort of capabilities we have could have increased the confidence in that.
That does raise questions, particularly about a challenge that I discussed with General Shaw before he left: how do you position what I would call "active defence" in this space? That is something that we will just have to keep working at.
Chair: Getting back to law for a moment: Dai Havard on the International Criminal Court.

Q135 Mr Havard: During the conflicts in Iraq we had, for example, British soldiers running an internment camp. They were protected in law in a number of different ways, partly because it was all done under the auspices of a UN resolution. So, in terms of things such as claims in the International Criminal Court they gained a form of protection. If rules of engagement are going to be developed for cyber, in an offensive or other role, what work is being done to look at where individuals would find themselves placed in terms of protection, particularly under the International Criminal Court?

[1] Ev 46

The Americans are not a signatory to the International Criminal Court, for example, so if they were working in an alliance, they might find themselves in a very different legal position from other allied forces that they were working with. Is anyone doing any work in this area, to clarify the legal protection for individuals we were asking to work on our behalf in these environments?

Nick Harvey: We would apply exactly the same legal principles that we do in conventional conflicts—actions that we were conducting here. So you are quite right in pointing to events in Iraq. In Afghanistan, we operate under a different legal framework from our American allies, so we are not unused to having our people work alongside them but in a different legal set-up.

In terms of the cyber domain, it would be our starting point that we were applying the same legal principles here that we would apply elsewhere. Yes, you make a good point. I can well envisage circumstances in which people doing things on our behalf were operating within a different legal framework from international colleagues. To be honest, that already happens, but the way we advise and look after our people is to apply the law as it exists to what they are doing in this domain.

Q136 Sandra Osborne: Across Government as a whole, is the capacity for research and development in cyber-security adequate to meet the needs of the MoD?

Nick Harvey: The MoD works with others to promote and stimulate science and research and development. We are currently providing £80 million a year for research in the related areas of cyber and influence. For Defence, that is done through the Cyber and Influence Science and Technology Centre, which is part of the Porton Down Defence Science and Technology Laboratory.

The centre team up here work, as you have heard, with other Departments. We work with research councils to ensure that there is a co-ordinated programme of research here, and we invest, as John has told you, in pan-Government work. We are part and parcel of programmes that have placed work out in a number of universities. There is a lot of activity co-ordinated with other Departments—with the Cabinet Office and GCHQ—developing cyber-centres of excellence. Is there enough? Well, I don't know. Is there ever enough? There is certainly a lot going on.

Q137 Sandra Osborne: Could research be enhanced by greater involvement with organisations within academia and industry?

Nick Harvey: Well, we do. Certainly, as I have mentioned, when placing these contracts in universities, we will place our research work with whomever we think to be the best-placed supplier. That might well be academia and it might well, in other instances, be part of the private sector. We have a Centre for Defence Enterprise which does its best to place innovative research work in academia and in industry, and it is that expertise and approach that we use when placing work in this relatively new field.

Q138 Sandra Osborne: How much of a constraint is it in relation to fears about giving access to classified information and involving outsiders in the field of research?

John Taylor: That is always something that we have to be conscious of, particularly in terms of the background information that we get from GCHQ. I point to some of the work that we have done under the Information Assurance Technical Programme, which, from last year's figure, the MoD put around £8 million to £8.5 million into, along with contributions from other Departments. We have found that that is manageable, because it tends to be not large groups of people who are doing the work, so we can make arrangements for individuals proposed to do that work to be appropriately security cleared and to ensure that they handle the information accordingly. I would not have said that that was a major impediment to engagement with these other institutions.

Q139 Chair: Minister, I am going to end with a completely unfair question, which is also about research and development. Yesterday, when we had the Minister responsible for defence equipment and supply in front of us, I asked him whether he might agree that 1.2% of the Ministry of Defence budget being spent on research and development was far too low, and he did agree. Would you agree?

Nick Harvey: Yes, I would certainly agree. I feel altogether more comfortable about doing so if he already said that.

Chair: So that is two down, five Ministers to go. Thank you very much. That was very helpful and we are most grateful to all of you for your evidence.

Wednesday 27 June 2012

Members present:

Mr James Arbuthnot (Chair)

Mr Julian Brazier
John Glen
Mr Dai Havard
Mrs Madeleine Moon
Penny Mordaunt
Ms Gisela Stuart

Examination of Witnesses

Witnesses: **Rt Hon Francis Maude MP,** Minister for the Cabinet Office, and **James Quinault**, Director, Office of Cyber Security and Information Assurance, Cabinet Office.

Q140 Chair: Minister and Mr Quinault, you are both most welcome to this inquiry of the Defence Committee into defence and cyber-security. Mr Quinault, you have been in front of us before, so I will not ask the Minister to introduce his team—that is not necessary. By the way, we hope to finish the sitting by 4.30 pm—we are aiming at 4 pm—so brevity on all sides will make that more likely.
Minister, how would you characterise the Government's general approach to cyber-security and to dealing with the cyber-security threat?
Mr Maude: We started, at the very outset of the coalition Government being formed, by raising the level of concern about cyber-security. The security and defence review rated it as one of the four Tier 1 threats. In what is understood to have been an incredibly tight financial settlement generally, this was one of the few areas to which additional funds were apportioned, as a recognition that it was a growing threat. There was a high degree of continuity with the approach of the previous Government, with, I suppose, two variations. The first was a raising of the level of concern and the issue's profile, and the deploying of more financial resource into it. The second would be a recognition that this has to be dealt with not just by the Government; it is a whole-of-economy threat. The Government do not sort it out on their own, nor the public sector on its own; this has to be done holistically.

Q141 Chair: From all you say, this is one of the most important threats that we face.
Mr Maude: Yes.

Q142 Chair: Are you in charge of it?
Mr Maude: I am not in charge of all of it, any more than any one threat that is very diverse in the way it presents itself can be dealt with in one part of the Government. I have responsibility for co-ordinating the Government's approach to it.
Chair: This very important threat.
Mr Maude: Yes, absolutely, but—

Q143 Chair: So how much of your time do you spend on it?
Mr Maude: I would say 25% to 30% of my time, at a guess.

Q144 Chair: You are in the Cabinet Office. What executive authority do you have in the Cabinet Office for dealing with cyber-security?
Mr Maude: The executive authority. Well, in what aspect, because—

Q145 Chair: The Cabinet Office is a co-ordinating office, isn't it?
Mr Maude: Yes, but it has certain executive functions as well, so there are some parts of the cyber-security programme for which we have direct responsibility—the identity assurance programme, for example. Responsibility for the Government's ICT strategy sits in the Cabinet Office. The Government CIO reports to me. In respect of the whole approach to the public sector network, for example, while responsibility for delivering it across Government sits with the CIO in the Ministry of Defence, for these purposes he reports to me. But this is very variegated in the way the cyber-threat appears and what needs to be done to counter it, so responsibility, very properly, is spread across the Government. I doubt whether there is a single part of the Government that does not have some kind of responsibility for this. The co-ordination of responsibility in the Cabinet Office is a recognition of that.

Q146 Chair: But it used to be the case that we had a Minister in charge of cyber-security as such. Lord West was one of them; Lady Neville-Jones was another. That is no longer the case, is it?
Mr Maude: No, but that was by no means their sole responsibility in either case. They were both Minister for security, with a whole lot of responsibilities that were much wider than just cyber.

Q147 Chair: What are your other responsibilities?
Mr Maude: Many and various. I sometimes think I am "Minister for everything else".

Q148 Chair: Isn't that a bit of a worry?
Mr Maude: Probably—it may be a worry to others.

Q149 Chair: It's a bit of a worry to us, I think.
Mr Maude: Okay, I hear that. Should there be a Minister whose sole responsibility is cyber-security? Possibly, but it would not be a Minister with seniority and authority to get things done. The fact that it is only a part—albeit quite a significant part—of my responsibilities does not mean that it suffers from a lack of attention. You could have it as 100% of the responsibilities of a rather junior Minister in one Department, which would mean that the focus and the span of authority were rather narrow, or you could

have it as one of the responsibilities of a senior Minister such as myself, where my ability to operate across Government is reasonably well established.

Q150 Chair: In May last year, therefore, the lines of authority—the responsibility for cyber-security—transferred from the Home Office to the Cabinet Office.
Mr Maude: Well, it transferred from a Home Office Minister. The office of cyber-security already existed in the Cabinet Office. It reported—and I think this was before James arrived there—
James Quinault *indicated assent.*
Mr Maude: The co-ordinating function sat in the Cabinet Office, but ministerially it reported to Pauline Neville-Jones. I think that was probably the case before the election, but James will know more about that.
James Quinault: Yes, that is correct.

Q151 Chair: It sounds like a diffuse muddle.
Mr Maude: I do not think it is a muddle. It is quite diffuse, and it may not be particularly tidy, but a lot of things are not tidy in life. It is not a muddle; we have quite clear lines of authority. The National Security Council sets this as a Tier 1 threat. The Foreign Secretary chairs a ministerial group that draws together Ministers with responsibility for particular aspects of the cyber-security strategy, which obviously I sit on. I chair the programme board—rather unusually for a Minister—but I am always quite interested in how the money gets spent, and in ensuring that it is spent to good effect and that we do not duplicate and reinvent the wheel, which can very easily happen with a programme such as this where new money is made available. It may not be particularly tidy, but we are getting quite a lot done in rather an effective way.

Q152 Chair: The Intelligence and Security Committee has said that it is concerned that there is a large number of Government agencies with overlapping interests in cyber-security. You may say that that is life—that's the way that life is—but what have you done to minimise the muddle I told you that I feared that we might be in?
Mr Maude: Did it say that there were overlapping responsibilities? I would be concerned if there were fewer agencies.

Q153 Chair: I think overlapping interests.
Mr Maude: I would be concerned if that were not the case. I would be concerned if there were only a few Departments that had any interest in this, and if they rigidly stuck to concerning themselves only with what lay within their narrowly drawn boundaries. This is very far-reaching, and it is changing all the time. One of the challenges is that we do not know what threat we will be facing next month, let alone in a year's time. When I took responsibility for the programme a little more than 12 months ago, one of the things I did was to say that rather than lay out now the plans for spending all this money over the whole of the CSR period, because we do not know what we are going to be facing, we actually need to hold some of it back. The thing we know we are going to need in government and in the law enforcement authorities is more capability, particularly in GCHQ, where quite a large chunk of the money will get spent. We need to have a real centre of excellence and expertise, which is the case—it is world-renowned for the quality of its expertise. My concern is that we need to hold back, because we need to be able to operate in an agile and fleet-of-foot way to respond to new and changing threats as events unfold.

Q154 Chair: Minister, my concern is obvious from my line of questioning. We have seen you in the past few months giving statements and answering questions on a whole range of things from the civil service to all sorts of other issues. A few months ago, I wrote a letter to the Prime Minister asking for a meeting between this Committee and him about our Report on the threat from electromagnetic pulses. That meeting is now going to go ahead. You were kind enough to answer a few weeks ago to say that the Cabinet Office would respond to our Report shortly. What concerns me about that is that you did not give any impression of being aware that the Cabinet Office—your office—had already responded to our Report. That made me less convinced by your expression of interest in our Report in the letter.
Mr Maude: I can't comment on the background to the Cabinet Office's previous response to your Report.

Q155 Ms Stuart: Who would sign off a letter from the Cabinet Office to this Committee in response to a Defence Committee Report?
Mr Maude: There are a variety of Ministers in the Cabinet Office. I do not know which particular part—It would not have been myself.

Q156 Ms Stuart: If cyber-security is your responsibility within the Cabinet Office, who else would sign that off?
Mr Maude: I do not recollect who would have signed that off.
James Quinault: This was not a report on cyber-security, as I understand it, but on electromagnetic pulses.

Q157 Chair: It was on the threat from electromagnetic pulses, which could take out our entire electronic infrastructure. Well, you sounded interested in your letter to me.
Mr Maude: I—
Chair: Perhaps you might like to read our Report—and your response.
Mr Maude: I am aware of it.
Chair: I am grateful.

Q158 Ms Stuart: Might we have an explanation of who signed it off, and if it was not you, why not? What other authorities are there in the Cabinet Office that allow another Minister to sign off a letter about a report of that nature? That would help us to understand how this all works.
Mr Maude: I will get you a detailed answer to that.

Q159 Chair: You will accept, I think, that it rather highlights our concern that we are not sure that anybody is in charge of this.
Mr Maude: In charge of what? In charge of electromagnetic pulses?

Q160 Chair: Well, A, that and, B, cyber-security in general. I have the impression that you are very busy doing other things.
Mr Maude: I am quite busy, yes.

Q161 Mrs Moon: Chair, I would like to go back to one of the Minister's earlier responses. I was not clear whether we were talking about a muddle or a model. It does seem to be more of a muddle than a model that we have been talking about.
Chair: My pronunciation has always been poor. Shall we come back to Gisela Stuart?
Ms Stuart: Do you want me to proceed? I thought Madeleine was asking questions.
Chair: I think that Madeleine has made her observation.
Mrs Moon: I was merely making an observation. I thought the Minister and the Chair were talking at odds. I thought one was talking about a model and the other about a muddle. It will be interesting to see what *Hansard* makes of it.
Mr Maude: I am sure it can clarify.

Q162 Ms Stuart: I have to confess that about 30 years ago I used to attend lessons in English as a foreign language. I was beginning to wonder whether I ought to go back to those. I still don't understand what you were trying to tell us. Could you try again for my benefit and simplicity?
You tried to start to say that the National Security Council establishes a tier of authority, and there is a clear chain of authority. I am not clear where the responsibility goes. Will you set out for me in simple language that I can understand: national security, National Security Adviser, deputies, the functions of the Office of Cyber Security and Information Assurance. How does all that hang together? Who instructs whom? How often do those people talk to each other?
Mr Maude: As throughout our system of Government, there are political appointments who are called Ministers and there are civil servants. The line of authority in civil service terms is the National Security Adviser and then the deputy National Security Adviser, to whom James Quinault reports. The line of ministerial responsibility is that I am asked by the Prime Minister to take responsibility for the cyber-security programme overall. I do that not because I have direct ministerial responsibility for most of it—although I do for some relatively small parts of it. I chair the programme board that oversees the programme.

Q163 Ms Stuart: Can you then instruct other Departments?
Mr Maude: We allocated the resources through the programme.

Q164 Ms Stuart: That is permissive, but can you instruct?
Mr Maude: Just to be clear, the way our system works is that we work through collective decision taking. I do not have the ability to instruct Philip Hammond or his Department. He has the ability to do that and he would be understandably affronted if I were to seek to do that. If there is a sense that the Ministry of Defence—or any other part of Government—is not doing what is needed to be done, the way that gets dealt with is through the collective process.
Ms Stuart: You describe something that is permissive and a line of authority, but, at some stage, someone must take—
Mr Maude: I do not think that I used the phrase "permissive."

Q165 Ms Stuart: But by allocating money, you enable Departments to do things. Specify a bit more clearly to me how if everything is so interconnected between every Department, you allocate the money but they are actually not doing what they should be doing. That then jeopardises the whole system. Who has the authority to say, "You are not stepping up to the plate and doing what you need to do"?
Mr Maude: That would be done through the programme board, where we—

Q166 Ms Stuart: Which you chair?
Mr Maude: Yes, absolutely. We expect—both I and my officials in James's team, but also other parts of Government—to hold each other to account for how the money is being spent.

Q167 Ms Stuart: But to be clear, if you, as the chair of the programme board, find a Department that has been given allocated resources to fulfil a function relating to cyber-security but it does not do it, you would be the person who has the authority to instruct them to do so?
Mr Maude: We would certainly have the authority to withhold further funding and address the failure, but I do not have the authority to instruct—nor would I expect to—officials in other Departments. That is a universal principle of the way our Government works.

Q168 Ms Stuart: How often does the NSC discuss cyber-security?
Mr Maude: Not very often.

Q169 Ms Stuart: What is that? Three times a year, 10 times a year?
James Quinault: It comes up as part of other agenda items. There is a plan to have a dedicated session on this in the autumn.

Q170 Ms Stuart: Twice a year, once a year?
Mr Maude: Once or twice a year.
James Quinault: As a subject in itself, maybe twice or three times a year.

Q171 Ms Stuart: So the most important security threat gets discussed twice a year.
Mr Maude: No one has ever said that this is the most—it is one of the four Tier 1 threats.

Q172 Chair: Mr Quinault, you said that there is a plan to have one of these meetings in the autumn.
James Quinault: A dedicated session on cyber.
Mr Maude: Solely on that.

Q173 Chair: Has there been one in the past?
James Quinault: There have been large parts of meetings devoted to cyber earlier on, at a stage when the programme was still in gestation.

Q174 Chair: But not a dedicated one.
James Quinault: No. But there is another ministerial group solely devoted to this topic, which meets more frequently.
Mr Maude: The ministerial group that the Foreign Secretary chairs meets every six weeks or so.
James Quinault: Also, as a programme in its delivery phase, the important thing now is to be chasing delivery on those agreed actions under the strategy. That is what is done by the programme board that the Minister chairs.

Q175 Mr Havard: Can I just press you? National Security Adviser and National Security Council—I understand that. On the Office of Cyber Security and Information Assurance, can I get some of the language clear because we have got the Strategic Defence and Security Review? The "defence and security" bit can often cause an issue because they are different, but they are interrelated and they are the same. That title is about cyber-security—electronic pulse, for example, is about cyber-security—but then there is "information assurance". There are two related things here. Are you doing information assurance for Government and does that include the Ministry of Defence? We are trying to discover where the Ministry of Defence's involvement starts and finishes in all of this. Like defence and security, some of it is not really proper for the Ministry of Defence, even though it might take it on. It might be that others need to sharpen up and take on their bit. We are trying to find whether these delineations are for purpose. Could you unpack some of that for me on cyber-security and, separately or related, on information assurance?
James Quinault: Yes. It makes for a rather long and inelegant title, but I think my predecessors thought that it was important to have "information assurance" in there, in that there are aspects of that, which are not to do with the protection of computer networks, that can simply be about losing information—leaving it on the train or misplacing discs.

Q176 Mr Havard: Don't go there, we know that story.
James Quinault: Indeed. There is that aspect to it as well.
Yes, the office has overall oversight of activity on that right across Government, including the Ministry of Defence, but the Ministry of Defence is very active in this area on its own account for good reason. The day-to-day lead on issues of information assurance in the MoD is, very properly, with it.

Q177 Mr Havard: Right, what I am trying to get to is—Bob Gates, the previous DOD Secretary in America, had a simple way of describing this: he talked about .mil, .gov, .org, and .com. So .mil can protect itself, .gov is not very good at it, .org is less good at it, and some bits are spectacularly good and others are rubbish. Then there is .com and people objecting to the fact that you are spying on their computer, so you might be able to do it, but will you be allowed to do it? Where does the military fit in? You are supposed to sit over all of this, presumably, and the business opportunities that come out of it. Yours is a very broad canvas.
James Quinault: Yes. As the Americans would say, this is absolutely not just a .mil or .gov issue. It goes right across the economy, as the Minister was saying.

Q178 Mr Havard: Where does DIS sit in that?
James Quinault: The Defence Intelligence Service? They are absolutely part of this. As I understand it, they also report to Sir Stuart Peach, the Joint Forces Commander, who is also the cyber and information assurance leader for this in the MoD. They are absolutely involved.

Q179 Mr Havard: Is he getting some of this money?
James Quinault: Just to go back, we see this absolutely as not just a Government and military issue. It touches everything in life, not just everything in Government, which is precisely why the approach to it has to be one of co-ordinating activity, rather than directing it all from the centre. If you want to reach business, the business Department needs to be mainstreaming this into its other communications with business.
Mr Havard: My colleague is going to ask you questions about that.
James Quinault: It has to lead on that. That cannot be done from the Cabinet Office.

Q180 Mrs Moon: Will you say a bit more about what you see as the role of the Ministry of Defence in national cyber-security and who defines that role? Does it define it itself, bring it to you and ask for permission—"Yes, that's fine, you do that" or "No, we would like you to do a bit of that."? Who decides what its role is and what is it?
Mr Maude: Its role, I would say, is to ensure that cyber is actually in the mainstream of what it does in strategy, doctrine, training and operations, and to help to build a good sovereign capability to defend our interests in cyberspace. It needs to work really closely with GCHQ. It is the centre of expertise in this territory and should remain so. We should be absolutely at pains to ensure that we do not replicate small pockets of expertise in different places. There is a great tendency for that to happen in Government and we have been at pains to ensure that it does not happen. Of course, it has a serious job to do, which is protecting its own networks and equipment. That is what I think Mr Havard has just been asking about. No one else can do it. We are not going to try and second-guess that. That is its obvious responsibility. The cyber-security programme does not pay for that. That ought to be business as usual for the MoD, which does not at all suggest that it is trivial. It is not; it is incredibly important.

Q181 Mr Brazier: We have focused so far on policy development, systems development and standing arrangements. This afternoon, let us suppose, there is a major cyber-attack on the UK. Who takes the lead, and on whose authority?
Mr Maude: The place where that would appear, first, is in the Cyber-Security Operations Centre, which is at Cheltenham. That is where the knowledge would be; the first intimations would be gathered together there. It depends on the scale and the nature of it. If it is deemed essential—if it is of a scale that it cannot be dealt with just by the Cyber Security Operations Centre at Cheltenham—then it would come up to the Cabinet Office.
If it was of sufficient scale, it could lead to COBR being convened at different levels, depending on the scale, with different Departments, potentially, in the lead, depending on what it was. If it was an attack on the energy infrastructure, for example, unless it was at a level where the Prime Minister would want to chair it, you would ordinarily expect the Energy Secretary to chair COBR. Similarly, if it was an attack on transport infrastructure, the Transport Secretary would, and so on.

Q182 Mr Brazier: Let's suppose for a moment that there was the kind of attack that Georgia suffered from. I am just talking in cyber terms, not about other things. Suddenly, all the Government websites come under attack, all the information movements come under attack, and the City of London. It is a massive viral attack right across all the dots, to follow up Mr Havard's point. COBR then convenes, presumably under the Prime Minister's chairmanship, because it is across—
Mr Maude: Yes, I would expect that.

Q183 Mr Brazier: Where does the chain of command go after COBR?
Mr Maude: How do you mean, "after COBR"?

Q184 Mr Brazier: Or below COBR.
Mr Maude: When COBR sits, you first of all assess what the hell is going on and establish what needs to be done in real time. Actions emerge in real time—you sit there and they appear on a screen as the discussion proceeds—and are taken up by whichever Department or bit of Government is appropriate, which will be allocated at the time.

Q185 Mr Brazier: So COBR would decide between the competing views of different Departments?
Mr Maude: Yes, totally. And immediately, in absolutely real time.

Q186 Mr Brazier: Within all this, the Cyber Security Operations Centre is clearly crucial to it all. Has its role changed since it came under the direction of GCHQ rather than the Cabinet Office? Do you think its role has changed or not?
Mr Maude: I would say it is probably changing every day, because the whole thing is changing. James may want to comment on that.
James Quinault: No, the role it performs of monitoring and triaging incidents and making sure there is a single version of the truth for Government to act on remains the same. I think the decision to change its reporting line was made for administrative reasons. It is based in Cheltenham, and many of its staff are from there. It made sense for their reporting line for administrative purposes to go through that route, but their responsibilities and accountability remain exactly the same.

Q187 Mr Brazier: Forgive me for taking a parallel, but given that the Cabinet Office is there in the centre and COBR is there with you and the rest, a parallel example is a very good initiative the Committees visited: the National Maritime Information Centre, which looks at potential maritime threats. Some of us were rather surprised that that has moved away from the Cabinet Office to the Home Office. In the same way, I am just trying to get the logic of something that so obviously needs co-ordinating from the centre and will so obviously be vital to COBR if there is a particular concern. It is a little puzzling that these vital assets seem to be moving away from the Cabinet Office.
Mr Maude: These things are not fixed for all time. In Government, as in all big, complex, dispersed organisations, there is no perfect structure that says, "All of this must be done in the centre, and everything else dispersed." That will always slightly be in flux in any organisation. If you look at any big multinational company, you will see that that will vary. Is there a perfect answer for all time? No. Will all of this work perfectly every time? No, nor is there a way of preparing for every possible eventuality.
James Quinault: If I may comment, these arrangements have been exercised and practised many times in the past few months as we run up to the Olympics, including some exercises involving the Minister himself. We consider them fit for purpose.
Mr Maude: Yes, we do test. It is not just that it looks like it works in theory.

Q188 John Glen: One of the issues must surely be that, if something goes horrendously wrong, it is difficult to attribute who is behind it and what the intent is. Could you address the issue of how that complicates matters? From this Committee's perspective, one of the things we are concerned about is at what point it would be discerned as a hostile act by a party and when the military lead would be assigned. It seems to me that you could presume that that happens in all circumstances, or you could wait. How do you see that as a complicating factor in terms of the attribution and the intent, and discerning that?
Mr Maude: Attribution is very difficult in this field, not only in the field of cyber-attack. Obviously, this is a subject that it would be easier to pursue in private session. You are quite right that this is a significant complicating factor. Proof is not always easy. Attackers are quite good at doing a false attribution.

Q189 John Glen: I suppose that what we are seeking is an assurance that there is a clear protocol of giving lead responsibility to some part of Government, and that that aggravating factor of how to attribute does not delay the appropriate response.

Mr Maude: In every set of circumstances, there is a judgment. It will rarely be the case that there is absolute proof. There are judgments to be made—difficult, complex and delicate judgments.

Q190 John Glen: I think from what you have said so far that those judgments will be made collectively under your headship of executive responsibility.
Mr Maude: If something looked like it could be a sovereign attack, that would clearly be for the Prime Minister.

Q191 Chair: Minister, you may want to tell us things that ought not to come out in public session, so we will consider either moving into private session at the end of this, or writing to you, depending on how things go during the rest of the afternoon.
Mr Maude: Sure.

Q192 Mrs Moon: Minister, could you tell us who, across Government, decides what investments should be made in understanding and anticipating the evolving cyber-threat? Do you make that decision, or is it down to individual Departments?
Mr Maude: The way allocation of money within the programme works is that different bits of Government bid for money.

Q193 Mrs Moon: Who decides who gets it? Who decides on the bids?
Mr Maude: Ultimately, I do, but obviously with appropriate consultation and discussion. My earliest decision was to say that we are not going to commit it all. The perfectly understandable Whitehall preference is, generally, "Here's money—let's work out how we're going to spend it," but I said that we are not going to do that in this case. There are things we know we are going to need, and that is investing in people and capability. That is focused predominantly, but not exclusively, on GCHQ. We need to retain flexibility.

Q194 Mrs Moon: Are we spending enough on this task?
Mr Maude: Could you spend more? Absolutely. Is this a perfectly judged and precise science? No, it isn't. As I say, we do not know what the threat will look like in two years' time. We need to be as prepared as we can be. You want to pitch this at the point where what we are doing in terms of the rising graph of protection against money spent starts to flatten off, where you could spend more and it would get better, but not that much better when there is a hell of a lot of competing claims for the money. So, could more be spent? Yes.
Without wanting to sound remotely complacent, which I am not—and touching wood at every available opportunity—Britain is generally regarded as being in a reasonably good place on this front. There was a study, but I can't remember who did it—
James Quinault: Booz Allen Hamilton.
Mr Maude: It said that the two countries that were ahead of the game on cyber-security were the United States and ourselves. I recollect that it put us ahead of the United States. But as I said, there is not a flicker of complacency about that.
Chair: Who was that?
James Quinault: It was Booz Allen Hamilton.[1]

Q195 Mrs Moon: You said that we don't know what is coming at us two years' ahead. How much time and money are we spending to scan the horizon and to keep up with the latest threats? This is not something that has even been static.
Mr Maude: No.
Mrs Moon: There is a risk. With Government, we are very good at setting up things that we expect to sit there for the next 50 years. This is not an area where we can do that. Are you confident that we have and will retain the capacity to horizon-scan and adapt rapidly and effectively?
Mr Maude: I am, actually—again, not to be remotely complacent about that. In our civil service reform done last week, we explicitly said that horizon-scanning needs to be strengthened generally for the Government. I would say that our ability to scan the horizon is reasonably good. There is a lot going into it, but I will let James talk a bit more about that.
James Quinault: If your question was a detailed one about how much and where we are spending money on this, intelligence and anticipation of the threat is a thread in a lot of the programme allocations. Understanding where the threat is going to go next and how best to deter that and defend against it is a big part of the investment in GCHQ. I obviously cannot say in a public session how much, but it is a big feature of that.
It is also a strand of the money going to law enforcement and SOCA to understand the ecology of cybercrime, a strand of the money going to the police e-crime unit, and strand in the work done by BIS and Government ICT to understand the market of this: where that might go and what new challenges that might throw up, for example in the move to do much more computing through mobile, what difference that would make to the threat, how that migrates and how therefore our responses need to migrate to follow it.

Q196 Mrs Moon: So you are not making a distinction, say, between cybercrime and national security? You see them as a whole, as a package?
Mr Maude: They overlap a lot.
Mrs Moon: We appreciate that.
Mr Maude: In terms of technologies, they obviously completely overlap. In addition to what James has said, I should like to point out that BIS has a scheme to recognise the academic centres of excellence in this area. It has awarded the status to the first eight UK universities earlier this year. I think David Willetts is hoping to announce another round in the autumn of this year. Again, we are looking to build up the centres, where there is real expertise, and to tap into that. We might say a little bit also about the work that we are doing with the private sector to develop the kind of information sharing and the ability to react in a much more cohesive way.
Chair: We will be coming on to that in a moment.

[1] Note by witness: Economist Intelligence Unit report sponsored by Booz Allen Hamilton

Q197 Mrs Moon: Do different Departments have different assessments and rankings in terms of the risk that cyber-attacks pose to them? For example, is the Ministry of Defence and the Foreign Office perhaps the most important Departments, but Education is at less risk? Is the spend differentiated between Departments? How do you work out which Departments need a greater focus?

Mr Maude: It is just different in different places: BIS, for example, will have a range of activities. One will be what I have just talked about with the university building up the centres and supporting those centres of expertise and excellent. Another, which is hugely important, will be building up awareness in business. It is generally the rule that businesses that are explicitly and overtly internet businesses take this really seriously and tend to be pretty good at it, but the most physical business that there is will depend one way or another on the internet.

The range of different degrees of preparedness in the business world is enormous. You will have seen the Director General of the Security Service yesterday talking about working with a particular company that has been very vulnerable. So BIS has a big task working with the business world to encourage them to be better prepared and to defend themselves better. Other Departments will have a different role. The MoD's role obviously will be very specific.

The Government Digital Service, which reports to me, has developed the identity assurance programme, which we intend to be something that does not just enable people to verify their identity for Government purposes, but actually to create a federated model where people can have a way of their choice to verify their identity to be able to transact on the internet with anyone, and not through a centralised system, but with a whole lot of different providers of identity services based on common standards. That sits with us. That is something that will be of benefit not only to Government as we move towards the digital provision of services online, but it will make it easier for people to transact online in other ways.

I have bank accounts with two different parts of the same bank. I have two different widgets from the same bank to enable me to assure my identity to do banking online, which is absurd. We should all have from the provider of our choice—not, emphatically, from the Government—an ability to assure our identity more widely. That is being done, as it were, from my teams in the Cabinet Office.

Q198 Mrs Moon: How much oversight does the Office of Cyber Security and Information Assurance have on individual Departments' spend? If you think BIS is not spending enough, can you tell them that they need to spend a bit more and that they are not focusing enough? We talked about collective decision making, but how much are you there also to make sure, as a sort of internal watchdog, that people are doing their jobs and to chivvy them if they are not?

Mr Maude: I see that very much as my job and the job of James's team in the office. That is what we do at the programme board

I am trying to move us away from "Are you spending the money?" to "What are we achieving?" It is quite difficult to measure what the outcomes are. Some of the bids were to hire people in particular places to do particular things, and one of the things we have been really concerned to do is to make sure that different Departments, different parts of the public sector, aren't bidding against each other to get what is a fairly scarce resource—people with high degrees of expertise. So we do this in a much more holistic and collaborative way, and don't duplicate. That is a huge part of what we are doing.

It is very much holding different parts of Government's feet to the fire, to make sure they are delivering on the strategy. It is no good having a strategy and a programme if it just exists on paper.

Q199 Mrs Moon: Are your salaries equivalent to private sector salaries?

Mr Maude: I hope not.

Q200 Mrs Moon: How do you know you are getting the best?

Mr Maude: Well, it is absolutely the right question. We won't always get the best. I think GCHQ operates in a very specific market—and this is an issue for them, which we are alert to. Across government we will not always be competitive in salary terms. People will generally not come and work for government just because the money is better. We need to make it attractive, but actually particularly in this area the attraction of coming and working in this field in government is that you have the chance to make a difference, on a big scale; and by and large people do respond to that sense of being able to operate on a big canvas and make a difference to the big picture.

Q201 Penny Mordaunt: Minister, can I ask you how effectively you think information on cyber-threats is shared across government?

Mr Maude: Pretty well, I would say. We are not aware of any particular problems in that respect. There have been problems between Governments. Things can sometimes be slow, but we are working very actively in the international field. I would say we are the leaders in the international field at promoting co-operation, particularly within law enforcement agencies. We hosted the London conference last November and will be active lead participants in the Budapest conference this October. We were certainly in the lead in drafting the Budapest convention. So I don't think particularly there is a problem on information sharing—[2]

James Quinault: On an operational level, I am not aware of problems of sharing information about threats between Government agencies. Did you have a particular thing in mind? At the moment, while we would always like to know more, what we do know is very quickly and appropriately shared. The issues are more about sharing between Governments or between Government and the private sector, where the programme is making strenuous efforts to get better information sharing at that level.

[2] Note by witness: We were certainly one of the leaders in helping to draft the Budapest Convention

Q202 Penny Mordaunt: So things like classification of information; those sorts of issues.
James Quinault: Yes, that is an issue.
Mr Maude: Yes, and we are aiming to simplify; what we tend to do is we have an over-complicated hierarchy of classifications, which we are aiming to simplify, but also—and this is a matter of culture and behaviour more than protocol—to limit and constrain the tendency there is to over-classify documents and other information. There aren't very many examples of things like the milk rota in one part of my Department being a restricted document, and somebody being given a security breach because the milk rota was left on their desk overnight; but this is not as streamlined as it might be.
James Quinault: It is not an obstacle to the sharing of cyber-threat information. It is a problem for some of the business generally. We all have different classifications. We have different classifications, again, between Government and the police. Simplifying that would make for speedier, more sensible conduct of business more generally, but it is not specifically a problem on cyber.
Chair: If you think that the Cabinet Office is a problem, you should see the Ministry of Defence.

Q203 Penny Mordaunt: Are any other barriers of that nature causing things not to be as speedy as they might?
James Quinault: As I say, not within Government, we don't think.
Mr Maude: And the steps we have taken to accelerate the rolling out of the public sector network, which is essentially about mandatory open standards on things like security and interoperability, will make that easier. It is not fully rolled out, but it is being rolled out. It is much cheaper than what it replaces, and much more efficient and effective.

Q204 Mr Havard: Is that sort of stuff being done through what was the WHISPER programme, and so on? There were different ways of trying, first of all, to collect people together so that they could have the discussion about common understanding, or have those been overtaken by events? Various aspects of the efficiency of the process were being researched, and the Royal College of Defence Studies was doing some stuff. Lots of people were doing things. Are you saying that a formal process is now in place that has overtaken those things?
Mr Maude: For what?

Q205 Mr Havard: Well, the WHISPER programme—the Whitehall information programme, or whatever—was trying, at the very start, to get the various agencies together that needed to come into the same room to have that conversation you have just described. It was at a very low level at the start, and it has obviously moved on significantly. You are talking about the local authorities being involved, for example, and the devolved agencies. There are all those aspects of government, not all of which are in Whitehall, in a physical sense.
Mr Maude: The public sector network is very deliberately for the whole public sector and offers considerable savings.

Q206 Mr Havard: Does that include government, if you see what I mean? Is it the public sector in its broadest definition?
Mr Maude: The wider public sector. Absolutely, and my recollection is that the first entities to take up the public sector network were two big county councils.

Q207 Mr Havard: Does that include agencies as well?
Mr Maude: Absolutely.

Q208 Mr Havard: And sponsored bodies of the National Assembly et al?
Mr Maude: Yes, totally.
James Quinault: One of the goals of the security classification review is to get to something that is more easily shared with agencies outside government, with whom we deal on some things.

Q209 Penny Mordaunt: Is any information on cyber-threats and related issues not shared routinely between Departments? Do you think there is a problem there?
Mr Maude: That would depend on the level of security needed. If it is highly sensitive, it would be on a very restricted basis, but I do not see any constraint, I would say.
James Quinault: I am not aware of any constraint to sharing information on, as it were, the warning, the alert, or the thing that the Department needs to act upon in order to protect itself. Obviously, we are much more careful in sharing the information from which that is derived, which may be very sensitive. There is a problem in that sometimes the warning that you wish to give people comes from a very sensitive source, and sanitising it, so that it is still useful to the recipient but does not reveal where it has come from or compromise some of your equities, can be a difficult thing to do. But it is being done. I am not aware of any case where a warning that could have helped a Department to protect itself was held back.
Mr Maude: But there are particular difficulties or sensitivities in the sharing of information with the business world, and within the business world, where it is incredibly important that information is shared, so that the knowledge of threats, in quite a specific way and very quickly, can be disseminated. The real task is to find ways of desensitising and anonymising information. For understandable reasons, businesses tend to be quite diffident about sharing widely.

Q210 Penny Mordaunt: The last question I wanted to ask you is that presumably, sharing information will make better collective Government decision making, as well as improving decisions within Departments. What evidence do you have that that is happening, if it is?
Mr Maude: Without wanting to spend all our time in meetings discussing things, we do have sessions where decisions are taken on the basis of shared knowledge. That is essential.

Q211 Ms Stuart: Following on from what you said about Government and private sector involvement and this clash between national security needs and confidential commercial interests, how are you progressing with developing protocols that would allow for that kind of sharing so that both sides know exactly what is possible and what is required?
Mr Maude: We are making some progress. We are working to develop a sort of information-sharing hub with what we have described as nodes, where different sectors can share knowledge. Some of these can exist in incipient form. James can perhaps talk a bit more about the detail of that. In terms of the protocols, this is a kind of work in progress.
James Quinault: That is what the hubs and nodes are all about—finding ways of sharing information, pooling information on situational awareness between Government and industry and between different firms so that we all get a better picture and can protect ourselves better.

Q212 Ms Stuart: I know that you thought that you were making good progress in that you gave a speech on 4 May when you said that there is now really tangible progress being made. So you have made the tangible progress, but may I press you a bit more as to where you are with the protocols? You may even want to give me one or two examples of how you know that there is tangible progress.
James Quinault: One instance would be that the hub and node thing is already broadening out between the pilot sectors that we started with. We began with five—finance, energy, defence, telecoms and pharma. We have now added transport to that list. We are broadening out as we go. Colleagues of mine spent most of last week with industry partners talking about how we can collectively build up to the next stage. The pilot has identified that we probably need slightly different delivery vehicles for different bits of this. So for the high-threat club, as it were, defence and security firms, perhaps telecoms and some parts of the critical national infrastructure, we would probably need something with some infrastructure behind it, so that people can share very highly classified information in real-time, fast, with one another. For the rest, where it is more about warnings and alerts coming out from the centre and where the idea is to get as many people as possible joining, we would probably want something that is much less classified, much easier to reach and where the circles that people want to join are decided by them rather than being policed from the centre. It is something much more like a social network to be honest. Work is going on now to bring those things forward. We are making progress and the programme can point to places where firms would say that the information that they have shared through this process has definitely helped them to protect themselves from what otherwise would have been a significant loss.

Q213 Ms Stuart: Are you already making, or are you intending to make, the requirement for information sharing part of your public sector contract when you contract with the private sector?
Mr Maude: With suppliers? I guess that where it is in the defence and security field, it is already part of the arrangements.
James Quinault: Yes, the MoD is looking now at whether it should be tightening up and increasing the standards asked for, particularly from List X companies. There are already requirements, but they do not include, for example, mandated auditability and that kind of thing.

Q214 Ms Stuart: That is just the MoD. I am not clear whose responsibility that bit is. Is it the MoD or the Centre for the Protection of National Infrastructure?
James Quinault: For defence and security companies, as the contractors of the MoD, it is principally an MoD responsibility, but the CPNI and ourselves are involved with the MoD in thinking about that, because it obviously has implications beyond the defence sector.

Q215 Ms Stuart: Are there then MoD and general public sector requirements?
Mr Maude: I am assuming that it is the case, but I will check.
Ms Stuart: It would be helpful.
Mr Maude: I will definitely check. I would assume that that is built in, but we should absolutely check.

Q216 Chair: Do I take it from what you said that the issue of the supply chain for the MoD and perhaps for other Government Departments and whether those small and medium-sized enterprises are properly protected from cyber- attack themselves is an issue which your Department would tend to consider was the responsibility of those other Departments to deal with? So managing the defence supply chain would be an issue for the Ministry of Defence, would it?
Mr Maude: Yes, definitely. Where suppliers are providing cross-cutting services, which they frequently do through the Government Procurement Service, we would expect to be in the lead on that. I think James will say that we are chairing work on that across government.
James Quinault: So our view would be that the MoD has to be in the lead on thinking about its relations with its own defence suppliers, which is completely appropriate, but we are involved in thinking with them about what may need to be done to those relationships to deal with cyber-issues.

Q217 Chair: I am pleased to hear that, because the Ministry of Defence think they have not got this quite right yet. Are you working with them to help them to get it quite right?
James Quinault: Yes, and with other Government Departments for whom this is an issue, too

Q218 Chair: If the MoD hasn't got it quite right, other Departments—for example, those Departments dealing with the finances of the country—will have got it less right, won't they?
James Quinault: It is also not just a question of getting it right once and for all. Just as the market you are dealing with moves on, so, too, do your responses

and policies. You are talking here about telecoms, which doesn't stay still. So the Government's thinking about this has to move with the nature of the beast.

Q219 Chair: Who is gingering all of this up?
James Quinault: The Cabinet Office leads collective work on this, but, as I said at the beginning, it is then for the Ministry of Defence, let us say, to think about how it plugs that into its relationships with its suppliers; it is not for the Cabinet Office to run all of that from the centre.

Q220 John Glen: Minister, can I ask about your level of contentment with what the MoD have reported back to you on the progress they have made on their cyber-security programme and the components that they are in the lead for?
Mr Maude: The parts that they are responsible for are the Global Operations Security Control Centre at Corsham, which I visited two or three months ago and which is incredibly impressive and state of the art. They have set up the Joint Cyber Unit at Cheltenham in GCHQ, which seems to me to be working pretty well. We are not reinventing the wheel in different places. MoD and GCHQ have properly grasped that we need a single integrated capability in this territory, which absolutely should be based in GCHQ.
I would say, but you will have investigated this yourselves, that the MoD have a good sense of the importance of cyber for military thinking in the future. It is built into, I understand, the concept of the responsibilities of the new Joint Forces Command. I think they have got, as far as I am aware, decent plans for rolling out training on cyber across their personnel. There is a scarcity of key skills in this area. That is universal, which is one of the reasons why one of my obsessions in this area is avoiding duplication. These are scarce resources in the economy generally, so we need to make sure that we are not replicating functions in different places. That is a challenge in the law enforcement area, which is very dispersed. Some of it is central Government and some of it is wider public sector, so it is not all within our control.

Q221 John Glen: Obviously, as you have explained in your answers to the earlier questions, there is a degree of autonomy within different Departments, but I think you probably also agree that there is an issue on the need for consistency and for you to have a level of assurance that each Department is dealing with cyber-security in a responsible and adequate way. Are you confident that you have that level of consistency? One of the things that has come up is concern about metrics for measuring it. If we return to this in 18 months to two years, what would we look for to see consistency?
Mr Maude: Am I totally happy that it is consistent? No, I wouldn't say that, that would be very complacent. But am I aware of any particular failings, in terms of progress? I think it took a little time to establish the necessary degree of collaboration in the law-enforcement world—I do not know that we are completely there but we are in a better place. We have been quite insistent on that.
The metrics is really difficult, and it is the kind of question I have asked a number of times. One of things that I did in the latter part of last year was to bring on to the programme board a very experienced senior non-exec from the business world, who had run one of the big technology businesses, to help with that and to provide the challenge and so on. It is very easy, when you have an early stage programme, to say yes we are spending the money, hiring people and doing all this, but what are we actually achieving? In terms of metrics, it is difficult. In terms of the outcomes, can you measure how many cyber-attacks do not happen that would have happened had we been less successful? It is hard.

Q222 John Glen: But presumably there are known information networks across Government Departments that you can identify as critical and needing to be treated and protected in a consistent way? Have you identified specific things as well? It is a separate question.
Mr Maude: I see what you mean, yes. Is our own infrastructure—our own vulnerabilities—protected to a reasonably consistent level? I think so, but do you want to add anything, James?
James Quinault: Yes, to the extent that consistency is appropriate. One of the ways of making this easier for yourself is by trying to decide what information assets most need to be protected and to make sure that you are only protecting them to a proportionate level, otherwise your walls are too long and they are bound to be breached somewhere. We do have metrics on that, we do know how many attacks have been thwarted, but what you do not always know of course is what has got through. But we do have metrics.
I think the Minister was talking about metrics for the programme as a whole: how do we tell that the investments being made through various Departments are producing the goods? There are, absolutely, metrics in terms of the outputs that we expect from each element of the programme—we know what the money is supposed to be buying and whether we are getting it—but what is less clear, as the Minister said, is whether overall that is making the dent in the outcome that we want to see, with the overall problem. The problem there is that we do not have a baseline, we do not know how big the problem is that we are trying to shrink. We are working on that, but if we had waited to solve it before we cracked on, we would be further behind the curve than we are.

Q223 John Glen: I understand the difficulty with the issue and with resolving it, but from our perspective—not that you are doing things from our perspective—of scrutiny, if we come back to this in two years, what do you suggest we should be looking for to demonstrate that progress has been made between now and in two years' time, for example?
James Quinault: You will need to do what we are deciding we need to do, which is to try and make a great big pile of all the pieces of data that bear on that question and then form a subjective view about whether you think things are getting better or worse—taken from infection rates, as revealed by security vendors or reports, or data on numbers of attacks

mounted from Britain—and just piling it all up and deciding whether you think that means that the problem is getting bigger or smaller. That is what we think we are probably going to have to do, but the hunt is still on.

Mr Maude: Finally on that, this is an internationally competitive environment. One of things that we explicitly say in the strategy—the first objective—is to make the UK one of the most secure places in the world to do business in cyberspace. I think we kind of are there at the moment, and acknowledged to be. Keeping there is very important, because the attackers and the fraudsters—whatever—will go for the places and the entities that are most vulnerable.

Q224 Chair: Which is partly a problem of the skills we have in the sector. You have mentioned that before.

Q225 Mr Brazier: I have some questions about people, Minister. Commenting to this Committee, Professor Brian Collins—as you know, he is an expert in the field—said:

"Perhaps as a codicil to that…there is an assumption that there will be continuity of stewardship of the strategy over a period of many years."

I appreciate that you are not answerable for MoD but it slightly concerned us that when we had got a National Security Strategy and then a SDSR that put the spotlight very firmly on MoD as having a very large role in this, they immediately appointed a man as the project manager who was known to be leaving the Army a year later. In fact, he performed very well in front of this Committee almost hours before he left the Army a week or two ago. Is there going to be some continuity in this field of key individuals, or not?

Mr Maude: Ideally. It is a general plea, actually, that we need greater continuity generally. One of the benefits of a coalition is that you get greater continuity among Ministers because reshuffles are more difficult. Not more difficult—more complicated. But when we were developing the civil service reform plan, one of the pleas among Ministers was to rotate civil servants less frequently and keep them in post longer. That is a general plea.

Q226 Mr Brazier: General Shaw was clearly well enthused and briefed on the subject, but it just seemed a great shame to have somebody in his last year in the Army leading the charge, and leaving.

A wider point. What is the Government's long-term strategy for competing with the private sector to recruit and retain the brightest talent in cyber-security? You were asked a bit about that earlier, so I will go on into the supplementary. Is there a danger that highly trained people no longer employed by the Government could one day use their skills in service to those attacking UK interests? Having taken people through some of these very sensitive areas, to what extent are you able to keep tabs on them if they leave?

Mr Maude: To the greatest extent we can. How do we compete? As I say, it is not just money. By and large, brilliant people do not go and work at GCHQ for the money; they do it because it is fascinating and it is very big-picture, serious stuff. We need to home-grow more talent and not expect to recruit everyone at the level of talent and expertise that we need, but to develop it more, which is something I believe we should be better at generally in the civil service.

So far as keeping tabs on people afterwards, would you like to say a word about that, James?

James Quinault: Keeping tabs on—?

Q227 Mr Brazier: The possibility that they may go and work for someone who is—

Mr Maude: Hostile. Senior people, when they leave Government, are subject to rules on business appointments and need consent.

Q228 Mr Brazier: And you are satisfied with the vetting process at the beginning? I mean, there were always stories about terrorists in Ireland getting training from the Army. That is something you could not prevent in principle. There is always the occasional story on that. This is an area that you are satisfied you have a pretty strict vetting process for people who start in it, not just at GCHQ but more widely?

Mr Maude: I don't suppose it is infallible, but I think it is pretty damn good.

Q229 Mr Brazier: What issues arise with the engagement of staff from private sector partners to work on Government cyber-security, for example potential conflicts of interest if staff feel they are being pressured to divulge threat information from their employers, or difficulties with security clearance for staff who work internationally? What sort of issues arise when you are dealing with the private sector in collaboration?

James Quinault: There are sometimes issues, and necessarily, because for the reasons you gave, we need to make sure that we are not harbouring a cuckoo in the nest. That said, there is a pressure from the other side to make sure that these rules are not inadvertently cutting us off from sources of talent. So we think hard and carefully about what levels of security clearance are proportionate and, where we can, we try to find ways of separating out the problem that we want people to work with us on from the information about where it has come from—its background and so on—which they do not need to know, and which is the really sensitive stuff.

We would get on very much better in this field if we could find ways of doing that on a regular basis, disassociating the problem we want help with from the rest of the sensitive stuff, and laying that out there for people to work on publicly. If we could do more frequently what the big vendors do, in advertising some of their difficulties and vulnerabilities and asking people to come up with solutions, we would be getting on a lot faster and would get a lot of talent for free. So we are keen to do that. The last thing one wants to do in this area is narrow it down to a small set of vendors to deal with, because that is not the way to breed innovation and the sort of quick response that you need.

Q230 Mr Brazier: That is a rather interesting point. You are saying that part of the key to it is finding, in cyber terms, ways of separating the product from the source.
James Quinault: Separating out the thing on which you want to bring innovation and skills to bear from the reason why you are worried about it, if you like. There is an obvious problem with advertising a vulnerability to the world at large, but if you can find a way of keeping that dark while asking people about the particular technical issue on which you want help, you can do that much more easily, and thereby draw on a much wider set of expertise, rather than having to go back and back to a small set of vendors who have passed over a barrier to entry in terms of security clearance. It would be great to get the widest possible set of firms and interested people working on these problems, instead of having to deal with a small group of defence companies all the time.
Mr Brazier: That is very helpful.
Chair: The final issue is international direction.

Q231 Ms Stuart: Minister, I gather that, like many of us, you have finally visited Estonia, for obvious reasons, not least because they have had direct experience. As a result of that, I gather that we now have someone in the embassy in Tallinn who will focus specifically on co-ordination on cyber, and act as a permanent point of liaison with the Cyber Defence Centre of Excellence. Why did we not just join the NATO group, which is part of the centre of excellence, in the first place? Would that not have cut out the middleman?
Mr Maude: The centre of excellence there, which I visited, was not operational.

Q232 Ms Stuart: I seem to remember visiting one some years ago that was operational.
Mr Maude: It is not an operation centre, it's a know-how and research centre.
James Quinault: It is operational in the sense that it is working. It is not operational in the sense that it is not the place from which cyber-defence of NATO would be commanded.
Mr Maude: Absolutely. That is what I meant.

Q233 Ms Stuart: But we could still have joined it, rather than appointing a liaison officer to talk to it, or am I misunderstanding something?
James Quinault: The officer concerned will have other responsibilities besides liaising with the centre. They will also, for example, help the Government to tap into what Estonia is doing on putting public services online. There is a lot of other stuff going on in Estonia.

Q234 Ms Stuart: But it is already a paperless Government, or has aspirations of being one.
James Quinault: Yes. This liaison person will help us to tap into that, as well as liaising with the centre. It is not everything they do. It would indeed be peculiar to have a liaison officer to the centre but not to join it, if that was all they did. In fact, they have other jobs as well.

Q235 Ms Stuart: May I press you just a little more? Why are we not part of the NATO centre, if what is going on there is so interesting and important?
Mr Maude: It is interesting, but it is not the only thing going on in Estonia from which there is much to learn. Estonia, which famously was the victim of a massive cyber-attack, is, at the same time, the most digital Government in the world, and has not been one whit deterred by the cyber-attack from going down that path. There is a huge amount of knowledge, generally, in Estonia, and some really interesting businesses in that field—small start-ups in the field in Tallinn. One of the things we were doing was looking to build links between those sorts of businesses and businesses in Britain. We are good at this stuff—not only Tech City; I visited Malvern recently, where there is a particular cluster of businesses in this field.

Q236 Ms Stuart: May I press you a little more? Estonia is barely larger than Birmingham and you have been to the place in Malvern. What did you learn other than that interesting small businesses could work together and that it would be very interesting if they did that?
Mr Maude: Enormous amounts about moving to digital Government and provision of public services online and the possibilities. We talked to them about how they contract with suppliers. They contract on a much shorter-term basis. They do not do what we do and have typically done in this country in government, which is to embark on massively long and huge IT contracts with one oligopoly of major suppliers. They looked at us in bewilderment when we described some of the things.

Q237 Ms Stuart: But they are that much smaller, so it would be quite different. I want to press you a little on an earlier question on protocols in terms of procurement and sharing. Do they have protocols in place that would require information-sharing in terms of cyber-security, and unless they did that, would the Government not sign contracts with them? Is that the kind of thing you have learned from what they are doing?
Mr Maude: Do you mean with their suppliers?
Ms Stuart: Yes.
Mr Maude: I do not know whether we particularly focused on that. Of all the Governments in the world, they are the most focused on this.

Q238 Ms Stuart: I have seen them sat around their Cabinet table with their laptops and not a single piece of paper, but what did you come away with that made you say, "Hey, that's really interesting what they are doing. Why don't we do it here"?
Mr Maude: The single insight I took from it is that we in this country allow ourselves to be excessively transfixed with security and prevent ourselves from doing really interesting things that drive productivity and better services for our citizens, because of what are sometimes inflated concerns about security. One of the concerns—any civil servant will tell you—about the frustrations of operating in the civil service is that there is IT that is incredibly difficult to use, because somebody has inserted into it security

constraints. A senior civil servant in my Department who is not dealing with anything particularly sensitive told me that before he can start work every morning it takes 15 minutes for his computer to fire up. The effect of that on productivity, and the frustration for people, is huge.

As I have said, Estonia has very intense concerns about security—no one more so. They paid a big price to learn the lessons that, actually, everyone else has learned, but they are still doing this stuff and they are doing it very aggressively and pursuing it vigorously. The particular insight I drew from it is that we should push ahead with creating digital services here, aggressively and at pace, with proper concern for security, but the security should not be a block on making progress on digitalisation.

Q239 Ms Stuart: Other than Estonia, are there any other countries where you felt, as you looked around, "They are really quite good and ahead of things. We could learn from them"?

Mr Maude: The States is very good. In February, I was in the States and visited the National Security Agency. Again, what was fascinating there was to find that they operate on a very short-term basis, similar to Estonia—although the United States is not small like Estonia—and they use a lot of small suppliers. If you go to Silicon Valley, you will find a number of really small companies with 80 or 90 employees, newly set up in 2008 or 2009, which are doing business with the National Security Agency. They are open-source, cloud-based suppliers, and they are doing incredibly sensitive, difficult stuff. The point is that to do the stuff well, we need to be tapping into the new wave of suppliers and developers. There are possibilities now, and those on the other side of the argument, if you like, are developing all the same things. We need to be as alert and agile as they are.

Q240 Chair: Will you forgive me for hammering into the ground one question that I still do not feel I have really got to the bottom of? Why is it that we are not joining the Cyber Defence Centre of Excellence? Would it be wrong for me to paraphrase what you have said as the Estonians are well ahead of the game; they are doing very interesting stuff; it is extremely helpful; we need the liaison officer; but we are even better and we do not think that is how we should be spending our money? Is that it?

Mr Maude: Just to be clear, the centre of excellence is a NATO institution. It happens to be based in Tallinn, but it is not the sole repository of Estonian knowledge and expertise. The reason for having someone based there whose sole role will be cyber but who will not be solely interacting with the centre is that it would be quite limiting just to be involved with that.

Q241 Chair: Just to be involved with that, yes. Have you been inspired to add anything to what you have just said?

Mr Maude: No, not really. That is the way I put it to them, because they raised the same question with me, as you would expect.

Chair: Thank you very much, Minister. It is just past 4 o'clock, and given the number of other things you have to do, I think we ought to release you. Thank you both for a very helpful evidence session.

Written evidence

Written evidence from the Ministry of Defence

Q1. *The nature and extent of the cyber-security threat to Ministry of Defence and Armed Forces systems, operations and capabilities*

1.1 The Government's 2010 National Security Strategy identified cyber attacks on the UK as a "Tier 1" threat—one of our highest priorities for action. These attacks are already occurring and cover a broad spectrum of actors and sophistication, seeking to carry out any number of effects.

> *Criminals* across the globe are already exploiting cyberspace to target the UK in a variety of ways. Some crimes exist solely in the digital world, in particular those that target computer networks and online services, but there are also the more traditional crimes such as fraud—now occurring on an industrial scale. Identity theft and fraud online now dwarf their offline equivalents. As businesses and government services move more of their operations online, the scope of potential targets will continue to grow.
>
> *State actors* who have traditionally used other means for the gathering of intelligence from the UK with the aim of spying on or compromising our government, military, industrial and economic assets are naturally turning to cyberspace to conduct this activity as more and more information is put into electronic format.
>
> *Terrorists* have previously been using cyberspace to spread propaganda, radicalise potential supporters, raise funds, communicate and plan. While it can be assumed that they will continue to favour high-profile physical attacks, the threat that terrorist groups might use cyberspace to facilitate or to mount attacks against the UK is growing, especially if terrorists believe that our national infrastructure may be vulnerable.
>
> *"Hacktivists"* and politically-motivated activist groups operating in cyberspace pose a real and present threat to the UK. Attacks on public and private sector websites and online services in the UK are becoming more common, aimed at causing disruption, reputational and financial damage, and gaining publicity.

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

1.3 Within the Ministry of Defence (MoD) there are technical, organisational, procedural and physical measures in place to protect against and mitigate the impact of cyber attacks. We have refrained from public comment on the specific detail of cyber security incidents or threat assessments as this information could be useful to potential adversaries.

Q2. *The implications of the 2011 UK Cyber Security Strategy for the Ministry of Defence, including:*
(a) *the MoD's role in cross-governmental cyber-security policy and practice, including the protection of critical national infrastructure;*
(b) *the relationship of MoD's actions and planning to the National Security Council, the Cabinet Office and GCHQ*

2.1 The 2011 UK Cyber Security Strategy sets out the Government's vision for cyber security by 2015, and what the National Cyber Security Programme (NCSP) will aim to achieve to realise that vision.

2.2 The MoD contributed throughout the drafting of the UK Cyber Security Strategy, and continues to work closely with the Office of Cyber Security and Information Assurance (OCSIA) on cyber issues. The development of any MoD policy on cyber will be in line with those guiding principals set out in the UK Cyber Security Strategy and, where appropriate, co-ordinated with OCSIA and Other Government Departments (OGDs) to ensure that departmental policy is harmonious and works with wider Government policy. As such, the MoD has no responsibility, policy or otherwise, for the protection of Critical National Infrastructure; this remains the preserve of Centre for Protection of National Infrastructure (CPNI).

2.3 The 2011 UK Cyber Security Strategy contains a number of objectives, for which lead departments have been allocated. Under objective 2 *"Making the UK more resilient to cyber attack and better able to protect our interests in cyberspace"* the MoD has been given the lead on *"Ensuring that the UK has the capability to protect our interests in cyberspace [by] improving our ability to detect threats in cyberspace [and] expanding our capability to deter and disrupt attacks on the UK"*. Minister for the Armed Forces will act as a focal point for delivery of this objective, and governance arrangements for cross OGD work are in the process of being formulated.

2.4 Cyber was highlighted in the 2010 National Security by the National Security Council, and again within the Strategic Defence and Security Review. The MoD has therefore taken the recommendations of both these reports and formulated Defence Strategic Direction 2011 (DSD11), which is used by the MoD for planning and policy formulation. In this way the MoD works closely with the National Security Council and the Cabinet Office to ensure that it meets the priorities set out by Government in the defence of the nation.

2.5 GCHQ and MoD work together as part of the NCSP. As the Director of GCHQ recently highlighted, a key role for GCHQ is supporting the military in Afghanistan and we will continue to benefit from a close working relationship, including the theme of Cyber.

Q3. *How the Ministry of Defence and the Armed Forces are managing and planning responses to threats in the cyber domain; including:*
(a) *skills, capacity and expertise within the MoD and the Armed Forces, including in research and development;*
(b) *how MoD and National Cyber Security Programme resources are being used to address cyber-security*

3.1 In the MoD, investment in ensuring military networks and equipment are protected against cyber attack has been underway for a number of years. The funding of cyber defence of key networks and systems remains a departmental commitment, and the funding for this is allocated from the Defence budget. The funding allocated from the NCSP, comprising £90 million, will be used by the Defence Cyber Security Programme (DCSP) to improve the broader transformation as to how the MoD approaches cyber operations. The new Joint Forces Command will take the lead in the development and integration of defence cyber capabilities from April 2012.

3.2 The DCSP is divided into four major workstreams lead at 2* level within Defence:

(a) *Mainstreaming Cyber*—which seeks to establish cyber operations as part of the mainstream of departmental planning and operations; backed by appropriate training, education and awareness.

(b) *Defence Cyber Operations Group (DCOG)*—which considers the role, structure and organisation of the DCOG; together with the specialist skills and training required for personnel within the group.

(c) *Cyber Capability*—which builds the necessary capabilities to undertake cyber operations.

(d) *Cyber Future Force*—which designs the cyber component of the Future Force 2020 providing the longer term vision backed by a programme of experimentation and development.

These workstreams are supported by *cross cutting activities* including programme governance and management, cross OGD working, and engagement with Allies.

3.3 As a major part of the DCSP, the creation of the new DCOG to bring together cyber capabilities from across defence. The DCOG will provide Defence with a significantly more focused approach to cyber, ensuring that it is at the heart of Defence operations, and is fully mainstreamed into all operational, procurement, and policy planning.

3.4 The DCOG will include a Joint Cyber Unit (JCU) hosted by GCHQ at Cheltenham whose role will be to develop new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace. We will also consider the future contribution of reservists in bringing in specialist cyber knowledge and skills.

3.5 Our Global Operations and Security Control Centre (GOSCC) acts as a focus for the cyber defence of our networks. Based at Corsham, it operates 24hrs a day, every day of the year to monitor our networks, detect attacks and take the appropriate actions required. In the event of a Cyber incident, the GOSCC provides an immediate response and functions as incident command and co-ordination, including a forensic analysis function to give possible indications of future vulnerabilities, attack vectors, and as best as can be done—attribution of source. The GOSCC monitors over 200,000 devices across our networks and provides constant analysis of our operating systems and applications to look for vulnerabilities that can then be addressed before they are attacked. A second JCU has been established and embedded within the GOSCC. It will develop and use a range of new techniques, including proactive measures, to disrupt threats to our information security.

3.6 To ensure that we have the right people and skills to undertake this work, we will grow a cadre of dedicated cyber experts to support our own and allied cyber operations and secure our vital networks by bringing together existing expertise from across Defence, including the Armed Forces (both regular and reserves), and our Cyber and Influence Science & Technology Centre (our focus for Research & Development on Cyber matters). The Chief Information Officer (CIO) is working to assist the DCOG in developing skills, framework, training and evaluation.

3.7 We will also build on the work that has been, and continues to be undertaken in the MoD Information Strategy (MODIS). Defence is committed to building and maintaining a robust Information Assurance (IA) regime that allows information risks to be understood and managed across the department; driving through behavioural change. The Defence Board has directed that the Communications-Electronics Security Group (CESG)'s Information Assurance Maturity Model (IAMM) Level 3 should be achieved and maintained across the department by the end of 2012 and a programme is in place to deliver this.

20 February 2012

Supplementary written evidence from the Ministry of Defence

1. *What are the respective remits of the Defence Cyber Operations Group and the Global Operations and Security Control Centre? How do they relate to each other? What are the other important relationships for each of the DCOG and the GOSCC?*

The UK *Defence Cyber Operations Group* (DCOG), due to be fully operational by March 2015, is a federation of cyber units across defence—working closely together to deliver a defence capability. It will mainstream cyber security throughout the MoD and ensure the coherent integration of cyber activities across the spectrum of defence operations. This will give MoD a significantly more focussed approach to cyber, by ensuring the resilience of our vital networks and by placing cyber at the heart of defence operations, doctrine and training. The establishment of the DCOG is a four year project and it is currently on track to deliver the appropriate personnel across all four years.

ISS' *Global Operations and Security Control Centre (GOSCC)* delivers and assures information and communication services for UK Armed Forces around the clock. Around 200 people work in the GOSCC, a mix of military, MoD civilian and contractor personnel from major industry partners involved in supporting the Defence Network, including Fujitsu, BT DFTS, Cassidian, EADS, Babcock and Paradigm. Their role is to deliver, manage and defend the Defence Network and provide worldwide assured communications for the MoD around the clock, 365 days a year.

2. *What will change as the Joint Forces Command assumes leadership for defence cyber capabilities?*

As Commander of JFC, Air Chief Marshal Peach will lead on the development of cyber capabilities across Defence—as well as ensuring that they are fully integrated into planning and operations. He will also champion the development of Cyber skills and training across Defence, ensuring that we manage our scarce cyber resource to best effect. Culture and language are also included as part of the wider influence sphere.

The Chief Information Officer (CIO), Mr John Taylor, and COMJFC will operate together closely in a "supporting" and "supported" relationship to achieve a Single Information Enterprise across Defence. The CIO will retain control over how the cyber risk to MoD's Information and Networks is mitigated and managed.

Cyber policy will remain in Head Office.

3. *What are the distinct roles of the Joint Cyber Units hosted at Corsham and at GCHQ?*

The Joint Cyber Unit (Corsham) is established and aims to proactively and reactively defend MoD networks 24/7 against cyber attack to enable agile exploitation of MoD information capabilities across all areas of the Department's operations.

The Joint Cyber Unit (Cheltenham) hosted by GCHQ will reach full operational capability by 2015 and will have the role of developing new tactics, techniques and plans to deliver military effects, including enhanced security, through operations in cyberspace.

4. *Where else in MoD are particular responsibilities for cyber-security located (for example, research and development, securing the supply chain)?*

The formulation of the DCOG will facilitate the concentration of all MoD cyber expertise within MoD coming together under one structure. The only current exception to this is the GOSCC, which will remain under the DE&S Top Level Budget for the time being. Research and Development is conducted at the DSTL site at Porton Down.

5. *How will the DCOG provide support to commanders across the Services? What sort of support is needed, and what are the urgent priorities?*

The DCOG will ensure coherence across Defence planning for cyber operations and ensuring that commanders have situational awareness of the impact of cyberspace on their operations, and able to use cyber tools and techniques to assist them in conducting successful operations.

To do this the DCOG will achieve the following by 2015:

- Cyber operations fully integrated into Defence, and all staff know how they form part of the essential defence of our networks during their everyday work and interactions;
- Clear policy, doctrinal and legal basis surrounding the use of cyber tools and techniques, including the proportionate enemy use of cyberspace;
- Cyber included in all planning and operations, with commanders and planners able to see exactly where cyber fits into their operations and the impacts of cyber;
- Commanders/staff understand the cyber domain;

— Recognised career structure attracting motivated personnel and retaining them after investing in their development;

— Greater situational awareness of our networks;

— Suite of cyber capabilities developed in concert with GCHQ;

— Robust structures for intelligence support with GCHQ;

— Agile procurement and rapid pull through of R&D;

— Cyber security and resilience factored into all MoD equipment; and

— Links established with key Allies.

6. *What is the vision for how cyber skills will be developed and deployed throughout the Armed Forces? Will these skills be integrated, or remain in a separate strand?*

Cyber skills will be embedded across Defence by 2015 and mainstreamed into every relevant training intervention at the appropriate level of detail. Content will be driven by the training need identified in our Training Needs Analysis by target audience. Specialist training will be provided to those specific roles within the Defence Cyber Operations Group, and wider targeting and Cyber planning roles; their skills will be recorded against a cyber competency framework on our HR systems. External frameworks used across Industry and Government will be used wherever possible (eg SFIA for IT and IISP for Information Assurance) to ensure coherence with partners.

At the same time, all Defence personnel will receive varying degrees of cyber education and awareness according to their role. For those in operational command roles this will include the impact of cyberspace as a domain of operations and its integration within operations. This training will be embedded with other command and staff training.

We are also working with Other Government Departments (OGDs) to understand where Defence may be well placed to provide pan-departmental training. This is being conducted in tandem with the Cabinet Office.

7. *What impact will be apparent from the Defence Cyber Security Programme over the period before the next SDSR? What will have changed within the MoD and the Armed Forces?*

By the next SDSR, the DCSP will push forward the development of tools and techniques that will allow greater situational awareness of our networks, however this can never fully guarantee that any network will be 100% safe and secure. We will also be looking to ensure that cyber security and resilience is factored into all MoD equipment. We will have created a culture of cyber awareness within the MoD that will equip all staff with the necessary level of cyber hygiene to defend themselves, both at home and at work, from the most common threats emerging from cyberspace. It is estimated that 80% of the threat we face can be mitigated by equipping users with the knowledge and right behaviours to stay safe.

We will also have in place a clear procurement route and greater agility when it comes to cyber R&D. This is essential if we are to keep up with the ever accelerating pace of change within cyber. This is not just true of our equipment, but also of our people. To that end, the DCSP will put in place a recognised career structure attracting motivated personnel and retaining them after investing in their development.

Finally we will develop a suite of cyber capabilities developed in concert with GCHQ, supported by clear policy, doctrinal and legal basis surrounding the use of cyber tools and techniques, including the proportionate enemy use of cyberspace. All commanders and operational planners will be educated in cyber to understand the cyber domain, its impact and where it fits into their operations. Cyber will also be included in all planning and operations.

8. *What is the MoD contribution to the overall UK Cyber Security Strategy?*

The MoD has a close and productive working relationship with the Cabinet Office, and has played a major role in the development of both the UK National Cyber Security Strategy and programme. We have worked together to share best working practice, in particular on programme documentation. The Department reports to the Cabinet Office on the progress of the DCSP on a monthly and quarterly basis, and sends representatives to the National Cyber Security Programme Strategic Investment Board and Cyber Delivery Group meetings.

9 May 2012

Further written evidence from the Ministry of Defence

ISSUE—QUESTION ONE

1. *How does the difficulty of definitively attributing actions in cyberspace affect the value of cyber defence as a deterrent?*

KEY POINTS

2. HCDC Chair is invited to note that:

(a) In general, deterrents are improved as lessons are learnt from breaches of those deterrents—this is the case within cyberspace;

(b) definitive attribution is not always a requirement to establish an effective deterrent;

(c) whilst conventional deterrents can mitigate the risk of attack, they do not always prevent an attack;

(d) Cyber deterrents are effective even if definitive attribution is not achievable; and

(e) as a greater understanding of others' Cyber capabilities is gained, the psychology and logic of Cyber deterrence can also be evolved.

DETAIL

Overview

3. The MOD defends its Cyber networks to maintain Information Superiority by operating freely within cyberspace. Existing Cyber defence techniques provide both a deterrent to potential adversaries as well as a defence against determined hacktivist or state-sponsored actors. The ability to detect an attack is key to ensuring that the Department's cyberspace remains secure and complementing this with the tools, techniques and procedures to neutralise any cyber incident ensures that Cyber defence, within the MOD, remains an effective deterrent.

4. The ability to definitively attribute an attack would be an advantage; however, what is more important, with regard to defending the Department's cyberspace, is having the capabilities to identify the "command and control" server of an attack along with the country, or region, which is hosting that server. This knowledge enables the decision-makers to facilitate processes, both technical and diplomatic, to deactivate the threat. Definitive attribution is therefore not a requirement for cyber defence to be an effective deterrent; this position is supported in the following paragraphs.

Cyber deterrents and definitive attribution

5. Due to the ability of perpetrators to operate with a large degree of anonymity within cyberspace, the process for definitively attributing responsibility for Cyber attacks is recognised to be both challenging and time consuming. Authoritative attribution of Cyber attacks to an individual, or group, would need to be achieved though an analysis of intelligence acquired from a number of sources. These sources would range from highly complex Cyber forensics tools to non-technical traditional intelligence gathering methods. However, this situation is not unique to the ubiquitous electronic information environment bounded by the term "cyberspace" as similarities can be drawn from historic events where definitive attribution was not a necessary requirement for decision-makers to associate culpability and decide on a proportionate response. Furthermore, the requirement for definitive attribution of an act of aggression, or Cyber Attack, is not always necessary, as knowledge of "where" rather than "who" an attack has emanated from is sufficient to instigate defensive deterrent measures.

Conventional deterrents

6. Deterrents against conventional/traditional acts of aggression, including a nuclear capability, are effective for a number of tried and tested reasons. These include an ability to definitively identify an aggressor and a legal platform, and willingness, to instigate defensive measures. However, there are many examples where acts of aggression have not been definitively attributable to a specific perpetrator although the responsibility for the act has been publically linked to a country, or group of individuals operating on behalf of a country. In these situations, the usefulness of conventional deterrents has not been questioned but instead they have been reviewed for effectiveness. Deterrents are bolstered to ensure that existing defensive processes are able to further mitigate the chances of future successful attacks. In general, deterrents are improved as lessons are learnt from breaches of those deterrents—this is the case within cyberspace.

Conventional deterrents—Definitive attribution

7. The mistaken NATO bombing of the Chinese Embassy in Belgrade in 1999 instigated a series of attacks against US interests in various countries. Following the bombing, Chinese civilians, some in organised groups, attacked the American embassy in Beijing, and in other locations. The deterrent response by the USA was to engage with those assumed to be attributable (ie, the Chinese government) for a diplomatic solution and not to target the specific perpetrators (ie, those who were definitively attributable). On this occasion the diplomatic

approach successfully deterred further attacks and the status quo was regained. This highlights that the important factor was knowing "where" the attacks were believed to be instigated from and not "who" was responsible for the specific acts of aggression. Definitive attribution is not always a requirement to establish an effective deterrent.

Conventional deterrents—Terror attacks

8. The 1988 Lockerbie bombing, which killed 270 people and instigated a significant international incident, was immediately attributed to Libya. The definitive evidence to identify exactly who was responsible was not available until many years later and it took until 2003 for Libya to accept responsibility for the bombing. Despite the lack of definitive attribution many sanctions were imposed on Libya as a direct result of this bombing. The main deterrents against the bombing of aircraft, ie, airport security and the threat of criminal prosecution, were significantly strengthened and internationally communicated. Despite these improved deterrents and warnings of repercussions to protect civilian air travel, the perpetrators of the 9/11 attacks on the USA were not put off or prevented. Following 9/11, the next stage of deterrents was instigated which included a significant renewal and reinforcement of airport security processes and direct action against the organisation, and not the individual, to which the attacks had been attributed. Whilst conventional deterrents can mitigate the risk of attack, they do not always prevent an attack.

Cyber deterrents—Case study

9. From mid-December 2009 to early January 2010, the Aurora virus attacked a number of US commercial companies, one of which was Google. Whilst Aurora has not been definitely attributed, a number of organisations, including Google, publicly stated that Aurora was a Chinese state sponsored attack. In response to the attack, Google neutralised the threat through Cyber defence techniques and then threatened to remove its presence and services from China as a deterrent. No definitive attribution was ever established. In February 2010 the Chinese government identified and shut down a large hacker training site located within China, arresting a number of individuals. Whilst cause and effect has not been definitively attributed to either the Chinese government or Google's deterrent actions, this does demonstrate that Cyber deterrents are effective even if definitive attribution is not achievable.

Cyber deterrents—The future

10. The proliferation of inter-connected information networks, and MOD's reliance on them, will command an evolution of the deterrent techniques adopted, and the defensive measure employed, within the Cyber domain. As a greater understanding of others' Cyber capabilities is gained, the psychology and logic of Cyber deterrence can also be evolved. The ability to definitively attribute a Cyber attack does not need to be achieved for Cyber to be an effective deterrent. Attributing a Cyber attack to the country, or state, from which it emanated would provide the diplomatic leverage necessary to maintain, and enhance, the effectiveness of Cyber as a deterrent. The Cyber domain is now considered alongside the land, maritime and air domains and countries, or states, will potentially be responsible for protecting their Cyber boundaries in the same way they police their land, maritime and air domains.

Summary

11. The difficulty of definitively attributing acts of aggression against the UK's interests is not new. The examples given show that for deterrents to be effective, definitive attribution is not always necessary. The examples also demonstrate that for deterrents to remain effective they must evolve to meet the new and innovative techniques of potential aggressors. As such the MOD are adopting a series of cyber defence measures which taken together aim to raise the cost of attacks, and to create an environment which is not permissive for the attackers—this can range from law enforcement action (Budapest convention), through development of international norms, to improved security and intelligence.

Issue—Question Two

1. *The Minister referred to a programme of strategic studies being carried out by the Defence Academy "to look at the implications of developments in cyberspace in terms of the environment in which our future security challenges will be managed." We would be grateful for more information about this programme of studies and how it is expected to inform planning for the next Strategic Defence and Security Review?*

Key Points

2. The HCDC Chair is invited to note that:

(a) the Seaford House Cyber Inquiry, led by the Royal College of Defence Studies (RCDS), was initiated in December 2011;

(b) the first report on the Cyber Environment will be published in July 2012; and

(c) the final report will be issued in February 2013 and provide an evidence base to facilitate SDSR 2015 strategic thinking for Cyber.

DETAIL

3. In December 2011, the Defence Academy—RCDS (Seaford House)—initiated an Inquiry to set a broader strategic context for Cyber. By using multiple sources and methods to generate a fresh perception, and to surface critical insights, which may potentially reframe the basis of current thinking into Cyber. The Seaford House Cyber Inquiry is led by Ms Sue Ambler Edwards (RCDS—Head of Strategic Planning) with Mr Hardin Tibbs in support. Work began in February 2012 and will generate an unclassified report for Government and public application in February 2013. Findings which are not appropriate for public consumption will be filtered through the MOD.

4. The Inquiry will report quarterly to the Review Board which consists of senior "Cyber" leaders from within the MOD, Cabinet Office and Foreign and Commonwealth Office. Monthly meetings are conducted with a stakeholder Reference Group drawn from the MOD, Other Government Departments (OGDs), Industry, Academia and the Science community. The Inquiry will generate an outline report on the Cyber Environment in July 2012 before moving on to examining the implications for MOD and OGDs in preparation for the final report in February 2013.

5. The Inquiry will conduct an in-depth exploration and analysis of emergent social, technological and economic factors that will define the Cyber arena over the next three to eight years (2015 to 2020). Global stability and security implications for the UK Government and MoD will be assessed as an input to SDSR 2015. The Inquiry is a qualitative sense-making exercise using a hybrid of "soft-systems" and "futures thinking" approaches. It draws on participation by a wide range of stakeholders, to capture and reflect multiple perspectives and worldviews, and will incorporate current social and complexity science findings about the impact of information and networks on communities, identity and power. Subject Matter Experts (SME) will be consulted, tasked with research elements, and involved in concept development workshops. The Inquiry is a cross-disciplinary, integrative, strategic study.

6. The Inquiry will check for overlooked asymmetric threats, generate an awareness of flashpoints and identify sources of Cyber options that are available to MOD and OGDs. It will give greater confidence for the Department and OGDs in setting strategic direction for Cyber. Importantly, within MOD it will provide an evidence base that will be incorporated into Cyber Doctrine and Strategic Balance of Investment decisions which will input into SDSR 2015.

July 2012

Further written evidence from the Ministry of Defence

THE GLOBAL OPERATIONS SECURITY CONTROL CENTRE (GOSCC)

BACKGROUND

1. The Defence Equipment and Support Organisation through its Information Systems and Services (ISS) Operating Centre is engaged in the provision of managed, integrated, highly reliable and protected information and communications services (ICS) to Defence. ICS is an essential enabler to the MOD in its role as a Department of State and in conducting operations successfully. The GOSCC is the focus for the operation and defence of the MOD's ICS—referred to as the "Operate and Defend" mission.

THE GOSCC

2. The GOSCC which has been in existence for over 10 years now occupies a new purpose built facility (opened in Nov 10), near Bath, at MOD Corsham. The GOSCC allows us to exercise service management over the capabilities provided by a range of ISS programmes, each of which was individually designed to deliver best value for money for Defence, by the outsourcing of various elements of ICS delivery: in each case, the major contracts that the programmes generated delegate elements of responsibility for the provision of secure and assured services to commercial delivery partners, encouraging the delivery partners to establish their commercial Network Operating Centre (NOC) or Security Operating Centre (SOC), physically within the confines of the GOSCC. Thus, today, the GOSCC comprises of a juxtaposition of a number of bespoke contracted operating centres within an overarching MOD led ICS service management regime. In practice, the complexity of modern ICS and the interrelationship between the different elements that need to work together to provide a true "end-to-end" service, means that MOD staff within the GOSCC act as *de facto* Service Integrators of the "MOD networks" (the term used to refer to the interconnected MOD ICS).

3. From the GOSCC, global operations utilising more than 500,000 configurable IT assets are monitored and managed in real-time, this includes fixed locations worldwide as well as the dynamically re-configured and mobile asset in operational theatres. The GOSCC is manned by military, civil service and cleared contracted personnel who provide 24/7/365(6) watch-keeping responsibility to "Operate and Defend" the MOD networks.

THE "OPERATE AND DEFEND" MISSION

4. Given the current and increasing threat to the MOD networks and the information stored within them, it is essential that the networks are adequately defended. However, it is also important to ensure that information

can flow quickly and freely around the networks in order to optimise the ability of MOD personnel to conduct operations and business successfully. Therefore, there is a tension between the "Operate and Defend" requirements because, in general, networks that are optimised to support business needs are potentially more vulnerable to cyber attack. For example, users would benefit significantly if they were able to exploit directly the internet as a communications bearer, but there are very real security issues that restrict such an approach. Consequently, those who "Operate" the network and those who "Defend" the network need to strike an appropriate balance between enabling users to conduct their business to best effect whilst minimising the chances of sustaining successful, and potentially serious attacks on the networks and the information they hold which would in turn have significant consequences for the business. This balance has to be achieved in the design and upgrade of both networks and defensive capabilities, as well as in their operation in real time. The optimal balance changes with the developing threat (which can happen quickly) and thus success in this endeavour is highly dependent upon a thorough knowledge of the topology of the networks and a very good understanding of business needs.

5. The co-location of contracted NOC and SOC functions, and the consequent availability of network management data has led to the establishment of the Joint Cyber Unit (JCU) Corsham, resident within as a fundamental part of the GOSCC operations, to monitor and defend the MOD networks from attack. Thus the "Operate and Defend" mission of the MOD networks has been brought together, within the GOSCC, under the command of the ISS Head of Service Operations (Hd Svc Ops).

GOSCC Daily Business

6. The GOSCC undertakes the following activities:

(a) *Coordination with other defensive cyber operations.* Potential attacks against the MOD networks can originate from external or internal sources. A "Defence in Depth" approach is in place to impede the majority of external threats. However, the fast-paced nature of adversary activity in Cyberspace means it is impossible to monitor against all likely threats in all scenarios. Therefore, JCU(Corsham) co-ordinates its activities as an intelligence led process, with key liaison and engagement with trusted partners, agencies and corporate bodies.

(b) *Real time monitoring and active defence of the MOD networks.* A "Defend" watch-keeping team maintains continual watch against known cyber threats and are authorised to take defensive action, in real-time, against these threats. Escalation procedures are in place and when the consequences of delay outweigh the operational or business impact, immediate actions are taken.

(c) *Understand what is legitimate MOD network activity and what is an attack.* It is not possible to defend a network adequately unless the defender understands the network topology and "Operate" activity. Whilst modern tools can give both the operator and the defender a good understanding of the topology, the defender can easily misread normal and routine operator/network activity (such as planned outages, software upgrades, major data replication activity, outages due to hardware and software failures) as potential attacks on the network. Consequently an "Operate" team maintains a 24/7 management overview of network activity to ensure optimum availability of services to the customers/users of the MOD networks.

(d) *Impact on MOD operations by protecting MOD networks—disrupting contractor performance.* It is sometimes necessary to direct the contractors who provide many of Defence's network services to carry out unplanned work that could degrade network performance (eg the application of vital security patches during peak usage times). Such action will often impact on the contractor's key performance indicators, resulting in financial penalties. Since the contractors work in support of Hd Svc Ops, disputes that arise over these issues can be resolved quickly and amiably.

Best Practice

7. The current "Operate and Defend" mission has been in use within ISS for several years and works very well. The US and NATO both centralise Operate and Defend at the lowest possible level and commercial organisations are moving in this direction. Considerable international interest has been shown in the way the UK delivers the "Operate and Defend" mission as other countries/organisations develop their own "National GOSCC" capabilities.

June 2012

Printed in the United Kingdom by The Stationery Office Limited
01/2013 023459 19585