Written evidence

Written evidence from Dave Clemente, Researcher, International Security Programme, Royal Institute of International Affairs, Chatham House

This evidence focuses on three aspects of cyber security which are of relevance to this inquiry: (a) division of authorities, (b) development of skills and expertise, and (c) measuring success or failure. While the current fiscal environment is constrained, the Government has identified cyber security as an area of particular interest. Additional investment may be necessary in some areas, while gains through efficiency and cooperation will suffice in other areas.

1. Regarding the role of the UK MoD and Armed Forces in national cyber security, their primary responsibility must be to protect their own information and the networks that hold this information.

2. In a conflict situation it may be necessary for the military and wider Government to operate in a degraded or insecure cyber environment. This requires acceptance that total control of "UK cyberspace"—however defined—is impossible. As the late Prof Philip Taylor (University of Leeds) noted, "full spectrum dominance is impossible in the global information environment."[1] This was meant in the context of military psychological operations, but it holds equally true when attempting to secure highly inter-dependent computer networks and information systems.

3. Protection of critical national infrastructure (CNI) is an area of significant importance and one that is becoming more difficult to analyse as inter-dependency increases between CNI sectors. The 2011 UK Cyber Security Strategy notes the status of the Centre for Protection of National Infrastructure (CPNI), but the centre has a light-touch role that focuses on delivering advice and building partnerships and relationships between the public and private sectors.[2]

4. The role of the UK military in protecting CNI remains poorly defined, but the UK is not exceptional in this respect. The debate over appropriate authorities for protecting CNI has been going on for some time in the US. The US Senate recently held hearings on proposed legislation—the "Cybersecurity Act of 2012"—which included discussion of the roles of the military and the intelligence community in protecting critical infrastructure.[3] As the responsibilities of the UK National Cyber Security Programme become clearer, it may become increasingly necessary and appropriate for the Government to engage the public regarding the role of the Armed Forces and the intelligence community in protecting critical infrastructure.

5. Cross-government communication and cooperation remains essential to more effective national cyber security. At the moment there are few clear lines of authority across the public and private sectors for carrying out protective measures in cyberspace. In most domains it is possible to ascertain who is attacking and why, and the answers to these questions determines which entity serves as protector. This is rarely the case in cyberspace, which creates a high level of ambiguity about who protects (military, law enforcement, lawyers, etc).[4]

6. The UK 2011 Cyber Security Strategy allocated the majority of National Cyber Security Programme investment (73%) to the Single Intelligence Account (59%) and MoD (14%). While the military and the security services are essential components of protecting the UK in cyberspace, they may not be the most appropriate organizations to deal with problems that are causing some the most immediate pain (eg cyber crime/fraud/identity theft, malware, etc).

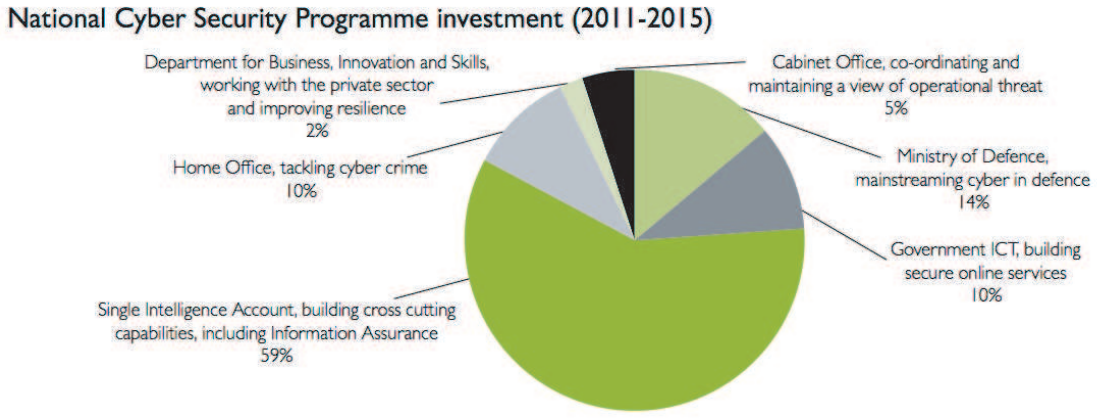
---

[1] Jason Vest, "Missed Perceptions", *Government Executive*, 1 December 2005, http://www.govexec.com/magazine/features/2005/12/missed-perceptions/20710/

[2] UK Cabinet Office, *The UK Cyber Security Strategy Protecting and promoting the UK in a digital world* (London: Cabinet Office 2011) https://update.cabinetoffice.gov.uk/resource-library/cyber-security-strategy, p. 28.

[3] Kim Zetter, "McCain: Cybersecurity Bill Ineffective Without NSA Monitoring the Net", *Wired*, 16 February 2012, http://www.wired.com/threatlevel/2012/02/cybersecurity-act-of-2012/

[4] Todd Bishop, "Q&A: The latest from Microsoft security guru Scott Charney", *TechFlash*, 15 Feb 2011, http://www.techflash.com/seattle/2011/02/qa-microsofts-scott-charney.html



7. Future government cyber investment may wish to devote additional attention to areas such as public awareness of basic/intermediate cyber security measures, as well as to early education in various aspects of information technologies (eg programming). Informed policy-making in these areas is increasingly necessary for the development of a highly skilled work force and is essential to remain competitive in the 21st Century.

8. The development of cyber skills, capacity and expertise are essential to adapt and innovate. The UK retains superb institutional memory from its involvement in the evolution of the internet and cyberspace more broadly. The people involved (often eminent academics) are irreplaceable, and their insight can be used more extensively to benefit the next generation of HMG policy-makers.

9. There are gains to be made from encouraging and rewarding cyber skills and expertise within the military bureaucracy. Some sensitive tasks cannot be contracted to foreign nationals, and it will be necessary to develop UK talent as well as implement processes that value and promote skilled individuals.

10. 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. In evidence given to the UK Parliamentary Intelligence and Security Committee in 2011, the Director of GCHQ noted that "I need some real internet whizzes in order to do cyber and I am not even sure they are even on the contractor market, so I need to work on that. They will be working for Microsoft or Google or Amazon […]. I can offer them a fantastic mission, but I can't compete with their salaries. But I probably have to do better than I am doing at the moment, or else my internet whizzes are not going to stay."[5]

11. Improvement in all these areas is highly dependent on accurate measurement. What metrics will the UK Government use to (a) judge success or failure in cyber security, (b) set benchmarks that can assist with these judgements and (c) preserve the institutional memory within government necessary to innovate and improve in cyber security?

"Security investment in the absence of security metrics will only result in overspending or underprotecting. No game play improves without a means of keeping score; decisions about developing, implementing and terminating cyber security programs are no exception. In fact, improving cyber security metrics programs is a meaningful goal in its own right. […] The cyber security problem cannot be solved absent a succinct mission goal. Reactive actions, however good, cannot drive policy. At the highest level of abstraction, the mission goal of cyber security is to:

— move from a culture of fear,

— to a culture of awareness; and

[5] Tom Jowitt, "GCHQ Boss Complains Of Cyber Brain Drain", *TechWeek europe*, 14 July 2011, http://www.techweekeurope.co.uk/news/news-security/gchq-boss-complains-of-cyber-brain-drain-34212

[6] Daniel E. Geer, Jr, "How Government Can Access Innovative Technology", in Kristin M. Lord and Travis Sharp ed. *America's Cyber Future: Security and Prosperity in the Information Age, Volume II* (Center for a New American Security, May 2011) http://www.cnas.org/cyber, p. 186.

[7] Daniel E. Geer, Jr, "Cybersecurity and National Policy", *Harvard National Security Journal* Volume 1, April 7, 2010, http://harvardnsj.org/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf

— to a culture of measurement."[8,9]

20 February 2012

Written evidence from Intellect

Intellect is the trade association for the IT, telecoms and electronics industries. Its members account for over 80% of these markets and include blue-chip multinationals as well as early stage technology companies. Our diverse cyber security portfolio reflects the fact that the technology industry has a critical role to play in the drive to online security, including providing agile solutions to cyber threats, supplying intelligence on attacks on information systems and in protecting itself, as part of the national infrastructure, from these attacks.

Intellect members commented that they do not believe they have sufficient detailed knowledge of MoD's current cyber security capabilities and future requirements, nor adequate knowledge of how the Department and the Armed Forces are managing and responding to the cyber threat. However, following a consultation with a number of member companies Intellect have highlight below the issues most salient to the technology industry:

— **Cyber Threat:** Whilst the MoD is clearly aware of the cyber threat, our members feel there is an issue in communicating the particular nature and extent of the threat it faces to industry and critically its supply chain, who, in many instances, provide and operate MoD systems. Due to sensitivity regarding classification levels, Intellect members have found that MoD threat briefings to industry have a tendency to be very high level. This can prevent business from coherently understanding the cyber threat, and consequently make it difficult for them to make informed investment decisions.

— **Co-ordination and awareness:** Intellect believes that coherent cross-departmental MoD support for industry-focused information assurance standards which are designed as a minimum baseline would help to protect the supply chain and reinforce the wider critical national infrastructure. Our members are also keen to see greater clarification of the roles and responsibilities within the MoD. The Department has a key role to play in co-ordinating and disseminating information and a responsibility to inspire and direct industry investment in cyber through more transparency and greater cooperation with commercial partners.

— **Current military capability:** The perception of industry is that the MoD does not appear to have the sufficient skills available for modern cyber-based warfare. Although our members do recognise effort is being made in this area, there may be scope for an enhanced military-industry partnership to address this capability gap.

— **Future skills:** The Cyber Security Challenge, initiatives undertaken at various universities and the Territorial Army's Land Information Assurance Group are all valuable initiatives. However, with the loss of skills to the private sector and the low uptake of Computer Sciences by British students at university level, a greater scale of investment in education both within academia and government is necessary to ensure the MoD has sufficient future capability.

  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.

— **Critical National Infrastructure:** Industry has greater "pace and scale" than MoD and other government departments in terms of the ability to use resources to develop and scale cyber products and services, and this is not always recognised by government. Partnership and coordination with industry is essential and perhaps more work is required to identify the size, composition, strengths, threats and weaknesses in UK CNI.

20 February 2012

---

[8] Daniel E. Geer, Jr, "How Government Can Access Innovative Technology", in Kristin M. Lord and Travis Sharp ed. *America's Cyber Future: Security and Prosperity in the Information Age, Volume II* (Center for a New American Security, May 2011) http://www.cnas.org/cyber, p. 186.

[9] Daniel E. Geer, Jr, "Cybersecurity and National Policy", *Harvard National Security Journal* Volume 1, April 7, 2010, http://harvardnsj.org/wp-content/uploads/2011/01/Volume-1_Geer_Final-Corrected-Version.pdf

Written evidence from Trend Micro

DEVELOPING THREATS FACING UK DEFENCE

- Industry is discovering that it has been targeted for several years by attacks with a level of sophistication and stealth previously thought to be reserved for nation-on-nation.
- The real world and cyber world are joining, which can catch even the most security savvy person out—real world contact gives credibility to an online approach.
- The twin pressures of Consumerisation and Virtualisation are stretching traditional defences.
- The latest commercial systems can help in ultra-secure environments by filtering noise—classifying/removing "known bad" which makes it easier to spot the ultra-stealthy unknown.
- Techniques/products also exist for further segmenting networks and identifying internal attacks. The single ultra-strong perimeter is dead—perimeter fractalisation is here.
- Many commercial vendors still believe they can offer adequate protection by doing what they have always done just a little better. They are fundamentally wrong and are adding to the severity of the problem.
- The savvy organisation now assumes compromise, and works to minimise the impact of that by earlier detection and better containment.

1. Sleeper agents and long term under cover intelligence gathering are the lifeblood of spy novels but, as is rapidly becoming apparent, exist also within the cyber-attack space. Often masked by the daily noise of mass random attacks (looking to harvest passwords, credit card numbers and banking details for financial gain) there is growing use of what has been coined by the media as Advanced Persistent Threats.

2. Much of the malware used for these attacks is in fact anything but "advanced". Often it is several years old and incapable of breaching a company perimeter. However, using advanced social engineering techniques, increasingly linked to real world contact, to gain control of a machine within the company perimeter, the attacker can gain a platform to launch their attack from within. Now with all the guards facing outwards towards the perceived threat of the open internet, the adversary can used tried and tested techniques (available off the shelf for a few hundred bucks if you know where to look) to roam freely within the internal assets of an organisation over a long period.

3. Virtualisation and Cloud computing are removing barriers between systems in the name of efficiency. All too few organisations implement the necessary security to provide virtual separation within those environments to return them to near physical security standards. It can be done, at least to EAL4+, but only with the right software and techniques.

4. Consumerisation is seeing smart devices walking in and out of the workplace, connecting to multiple networks, and providing a bridge between them that didn't previously exist. Devices with cameras, microphones etc that could be remotely controlled/activated introduce a new security dimension.

5. Of course in highly secure establishments such devices are banned, and proper network separation is still maintained. But increasingly the adversary is working back up the supply chain to compromise assets before they are shipped, or compromise products used as part of the security infrastructure itself. The RSA takedown is probably the most public example of this, where the commonly held belief is that RSA were merely a security supplier to more interesting (defence industry) targets. By remaining dormant over a long period such attacks may escape detection until the damage is done.

So can anything be done to stop them?

6. We must remove our reliance on a single perimeter, however strong. But we should not abandon that perimeter. Though leaders Jericho forum talk about de-Perimeterisation to indicate that the age of the perimeter is dead—they couldn't be more wrong. The perimeter remains vital to filter noise. The earlier (further from the vital core systems) that any attack can be blocked the better. We need now not one perimeter but multiple repeating perimeters tightening around key groups, individual servers, particular applications and data. It's like a fractal—a mathematical shape that however much you zoom in looks identical, with ever repeating copies of itself on a smaller scale. Each one strips noise by blocking stuff that shouldn't be heading that way.

7. On the inner layers anything you block also becomes vital intelligence—because that threat must have come from inside the organisation. Track back and clean, or honey pot and try to discover more about the adversary.

8. Ultimately you may get to a point where only a smart human, focused on the task, can spot something happening. But you make that person's job a whole lot easier by removing the haystack and just leaving the needle on the bare ground.

9. Then plan for compromise. Don't just watch for stuff coming in (Outside-in security) but also stuff going out. Build a second series of layers watching and guarding Inside-out. Encrypt data and switch the problem away from "how do you stop the wrong folks gaining access" to "how to you ensure the right folks do have access". Watch for data flowing out, particularly encrypted data. Where is it going to, does that make sense, is it authorised?

10. The answer to defence of ultra-secure systems isn't exclusively off the shelf security. But without learning from the latest industry best practice we will focus on re-inventing what already exists rather than the value add required exclusively for such secure systems.

17 February 2012

Written evidence from Russ Bubley

— "Cyber" is already a broad term, and is subject to further creep.

— (Almost?) No system is secure.

— Solutions must not significantly degrade the user experience.

— Unanticipated change will continue.

1 The term "Cyber" itself is unclear to most, and seems to be used by the media to refer to anything remotely connected to technology. With the increasing convergence of internet and voice communications (VoIP), as well as delivery of entertainment over the internet (eg BBC iPlayer, YouTube, etc.), "Cyber" could soon include most of our communications and media. Cyber-security has a similarly elastic definition.

2 This subject is often talked about only in terms of technical jargon. Very few of the issues are actually that complicated; the technical details can distract not illuminate.

3 Cyber-security issues tend to fall into several broad categories, in terms of impact:

— Information leakage.

— Misuse of computing resources.

— Disruption to use of resources by intended users.

5 Cyber-security issues can be brought into effect by a variety of methods, but it can be helpful not to confound the impact of a security breach and the methods used to conduct that breach.

Information Leakage

6 Casual leakage. With the growth of social media people unwittingly give away more information than they intend to. By studying all of the information made available by an incautious or apathetic user, a detailed profile of a person could be built up: what family they have, what they like to do in their spare time, how frequently (and where) they holiday, their politics, plus details of their ongoing relationships in both a private and professional context. Anecdotally, this sort of information has formed the backdrop to social engineering attempts at blackmail ("Your daughter was injured on a bus to Veracruz…") as well as giving potential kidnappers plenty of data both to select targets and ask for ransom from.

7 Accidental leakage. We read time and again of data compromises from people moving data off of a secure system onto an insecure one. Laptops that get stolen. Unencrypted memory sticks and CDs that wind up lost. E-mails sent to personal e-mail addresses.

8 Geolocation—where you are. Again, mainly from social media, but also from apps on mobile phones that encourage it, people disclose—both wittingly and unwittingly—where they are. There are many reasons why this could matter depending on the individual: personal privacy, implications for physical security, but also locations allow for inferences relating to the individual's work to be made.

9 Theft of data—quite a broad area, and would include for example, the goals of espionage, identity theft, blackmail, and as we have seen recently, to sell newspapers.

Misuse of Computing Resources

10 "Botnets"—Taking over large numbers of computers (typically home computers), so that they can be used to further a secondary goal. Examples of these goals are:

— Sending spam.

— Conducting a DDOS attack (see below, paragraph 14).

— Using computational power to solve a complex problem, eg breaking encryption.

11 Website defacement—This is where a hacker changes a website to show different information. While historically this has often been done purely for fun by hackers, more recently it has been a goal of "hacktivists", who have replaced the usual content of websites with political or religious messages. A more insidious version of defacement is to spread propaganda, where defacements may not be obvious without close reading of the text on a website.

12 Unauthorised use—depending on the capabilities of the system, any of these could be misused to achieve an end. For example, databases could be manipulated to commit a fraud.

13 Secondary risks from impact on other technology systems, eg bringing down a telecoms network, or a utility company's control systems. Stuxnet is probably the interesting case study here, where it is claimed that

the Stuxnet worm succeeded in infecting control computers in an Iranian nuclear enrichment plant, resulting in several months of delay to their programme.

Disruption of use of Resources by Intended Users

14 DDOS—Distributed Denial of Service. This complicated term is simply co-ordinating lots of computers to make requests, typically of a web-site to the extent that the infra-structure can no longer cope and the website is effectively "down" to normal users. This has been a favoured tactic of activists, and has been likened to a modern-day form of political protest. The coordination of computers can be achieved either via a Botnet, or simply by organizing enough people to do it manually by either conventional or modern means. In a pre-Internet era (and still possible today), this has parallels with a letter-writing campaign—which can flood a post room to the extent that genuine post may be lost, or an orchestrated telephone campaign, which could easily flood a switchboard. During the Kosovo conflict, pro-Serbian hackers instituted a DDOS attack on NATO's servers. More recently, numerous sites in Georgia were overcome by DDOS attack before and during the time that Russia was physically attacking.

15 Various other exploits have been used to effectively shutdown part or all of a set of computer systems, or mislead users into receiving incorrect responses to their queries.

Methods

16 Compromising passwords. There are many ways of doing this, but some typical ones are:

- Social engineering—getting people to tell you passwords voluntarily, typically by lying to them. "Hi, I'm calling from your bank. Before I go into details, I need to ask you some security questions."
- Phishing—tricking people into entering their real passwords into a fake system. People are often led to the fake system by an e-mail purporting to be from a trusted organisation. "We have noticed some unusual activity on your account. Please log in here to verify your recent transactions."
- Brute force—trying passwords repeatedly, with the help of dictionaries until you find one that works
- Keyloggers—devices either physically attached to a computer, or software installed on your computer without your knowledge. These keep track of every key you press.

Systems are generally more secure when they are either critical systems or systems which if compromised could be expensive (eg banks requiring some sort of key-fob token, some providers of expensive data require fingerprint scanners, etc.).

17 Hacking—probably the best-known of the cyber-security issues, and so the one on which I will comment least. A hacker will attempt to compromise a system, typically taking advantage of some sort of bug that enables the security to be bypassed. Probably the most important thing to understand is that no connected system should be considered secure against this sort of attack from a determined and well-resourced attacker. There is a continual arms race to improve security and defeat it. This is not helped by the fact that systems are rarely constant with both software and hardware being retired regularly, and each change bringing with it the potential for a new set of security problems.

18 Man-in-the-middle attacks—this is where an attacker stands in the middle of the flow of data, observing, and potentially changing data as it goes past. There are numerous well-documented cases of this form of attack, including ones where it is claimed they were carried out by state-sponsored actors.

19 There are many more esoteric methods some of these are well documented, but it would be prudent to assume that there are other methods not generally known.

Miscellaneous Issues

20 Cloud computing—data and computer processing, both for individuals and for organizations is moving from home computers to "the cloud", where it is outside of your physical control. This trend is fuelled by the explosion of devices, and the desire to share data between them for convenience, and for reasons of economy: it is much cheaper to rent computers at a dedicated data-centre than to run them yourself. As cloud computing is typically accessed over the public internet, it becomes more susceptible to most types of cyber-attack. As a proof-of-concept, cloud computing has also been used to break cryptography.

21 BYOD—Bring Your Own Device. As people get more attached to their personal devices (smartphones, tablets, etc.), with their familiarity, ease-of-use, and integration into people's lives, people are opting to use them for their work. Recognizing this trend, IT managers are allowing (or being forced to allow) these devices to access what would previously have been a more secure network.

22 Impact of research—a breakthrough could be made that makes defeating most of our current-day encryption possible. This could happen through better algorithms for factoring prime numbers (key to most secure communications) or through developing scalable quantum computers, for example.

23 Lack of experience/interest from today's youth. Our computers are so sophisticated today, that users are not forced to interact with them in the same way as they were a generation ago. Put another way, IT and programming are no longer even closely related. Many claim that this will lead to a dearth of programming talent amongst the younger generation, leading, in the long term, to economic and security problems.

24 It is now possible to buy, for a few hundred pounds or less, personal reconnaissance drones—basically model aircraft with a camera attached. Some of these can be controlled in real-time from a smartphone. They have hit the media in several circumstances, at least one of them positive. See, for example, http://tinyurl.com/drone-image, where a member of the public in the US used one of these to expose alleged environmental abuses at a factory.

25 Cyber-security problems usually arise because of peoples' behaviour, not because of technological wizardry. Education in cyber-security (not just "how", but also "why"), and good management of people is important. If management structures value business effectiveness over security, and security is perceived as cumbersome or burdensome, it will be skipped or diluted.

26 Smartphones and tablets may become more of a cyber-security issue than computers. People rarely worry about security on their smartphones, beyond the physical security. Yet they contain vast amounts of highly personal data, and if compromised could be used for bugging, tracking, and many other nefarious purposes.

27 Anecdotally, travellers' smartphones, tablets and laptops have been confiscated or searched when in foreign countries. Depending on circumstances this could compromise the travellers in any number of ways.

Observations

28 Psychology and security. Most people don't care about security: they just want things that work. If things become too hard to use because of over-onerous security, people will go elsewhere or work around the security. Force users to change passwords too often, or to make them too complicated, and they will write them down. Ban them from using a website on a work computer, and they will turn to their smartphone or find a way around the technological ban. Education enables people to strike a balance between security and convenience.

29 Commercial reality and security. For many businesses, security probably should take second-place to reliability. If your website, or worse, your payment processing service is not working, you will lose customers. If you accidentally leak details of your customers to hackers, it may have a very limited impact on your bottom line. Provided you have "the little padlock-thingy", people will assume that security is good enough.

30 Despite the varied problems that breaches in cyber-security could cause for an individual institution, the cost and effort in fixing them has to be compared not only to the potential costs of leaving them, but also to the cost of and cures for "business as usual" operational issues: a faulty computer in the server room may cause just as many problems as a hacker.

31 Censorship and intervention. Looking at the riots of last year, when it was suggested that social media be "turned off", because it was letting people communicate freely brought forth comparisons with both the Arab Spring and censorship in more repressive regimes.

Relevance for National Security

32 Institutions will typically evaluate the potential impact of cyber-security issues as it affects them in isolation, they will not generally consider the impact of a systemic failure, or simultaneous failure of multiple institutions. A parallel could be drawn with the financial crisis.

33 Hostile actors, whether they be state-sponsored or otherwise have tried, and will continue to try to exploit flaws in Britain's cyber-security for their own ends. Espionage, and particularly industrial espionage, has been cited to be on the increase. This should be expected, as cyber-security approaches to industrial espionage are much simpler, cheaper, and safer than traditional methods.

34 Expertise in cyber-attacks, once built up, can be redirected at different targets swiftly. If you have the know-how to compromise a technology company today, you may choose to switch to a newspaper, a bank, or a government department tomorrow.

35 Against this backdrop, it seems fair to ask what the House of Commons Defence Committee might do to help government in tacking these problems.

20 February 2012

Written evidence from BAE Systems

Introduction

1. The Government's commitment in the National Cyber Security Strategy is a key element of the UK's response to cyber-attack on public and private sector organisations. The Ministry of Defence (MoD) has a critical role to play in delivering this strategy.

2. The National Cyber Security Strategy clearly articulates the role of the private sector in improving cyber security. The key to success will be ensuring that private companies see it as beneficial to their business to work in partnership with government, and for them to understand how, and in what way, they should engage with government most effectively.

3. BAE Systems welcomes the House of Commons Defence Select Committee's intention to conduct an inquiry into cyber security. BAE Systems Detica, part of BAE Systems, has over 30 years of experience working with government and is a leading provider of cyber security services and solutions in the UK. BAE Systems is pleased to be able to contribute to this inquiry and would be happy to discuss with the Committee any points raised in this submission.

The Cyber-Security Threat

4. In a knowledge based economy, every organisation relies on information assets and systems to operate and compete. A cyber-attack which compromised the confidentiality, integrity or availability of its information would damage performance and bring operational and reputational risk to the organisation. Generic and MoD specific examples are shown below.

Generic	*MoD Specific*
Leakage of confidential and personal emails	Publication of confidential email between senior staff during budget decisions
Compromise of real-time control systems for operational equipment	Loss of the command channel to operational remotely operated vehicles
Compromise of core planning and control processes to direct the overall operation of the organisation	Logistics information relating to deployed operations being visible to an adversary
Publication of Intellectual Property (IP) regarding the future products or services of the organisation, including an understanding of how they may themselves be compromised	Performance details of future weapons systems being visible to an adversary

5. A growing range of threat actors are mounting such attacks including:

- "hacktivists" intent on causing reputational damage;
- "insiders" as individuals or supported and motivated externally through advanced social engineering; and
- "corporate" and "state-sponsored" attacks determined to steal high value IP or to reduce the operational ability of the organisation.

6. The increasing use of COTS products and dependency on internet protocol (as opposed to proprietary) networks will have brought a wider range of vulnerabilities into MoD systems. Some of which will already be known to attackers.

MoD and the UK National Cyber Strategy

7. It is essential that the governance of cyber security across government clearly defines the roles and responsibilities of government departments and public bodies individually and in collaboration. Without this clarity:

- outcomes would be weaker given the limited resources available; and
- private sector companies would find it difficult to engage effectively with government, reducing their contribution and their benefit.

8. We believe MoD's role and responsibility will include internal activities and activities conducted collaboratively with other government departments and the private sector. Examples are as follows:

Internal Activities:

- ensure security of its own Department;
- assure security of its supply chains; and
- establish active defence and offensive capabilities.

Collaborative Activities:

- implement effective exchange of information on a trusted basis across government and the UK defence industrial base and, possibly, other industry verticals;

— contribute to the secure implementation of cross-government networks (eg the central Government "Public Services Network"); and

— support the security of Critical National Infrastructure (CNI).

9. Possible approaches to these collaborative areas range from sharing "best practice" to the provision of a shared network security service and support to CNI. (For example, is the MoD required to provide the cyber-security equivalent of "military aid to a civil power"?). MoD and others will need clarity regarding remit to ensure expectations are met.

10. MoD has well-established Information Assurance (IA) processes for reviewing cyber risk, and should continue to share knowledge and expertise with other government departments and private sector organisations. We suggest five areas of specific focus: defining the perimeter of the MoD; sharing threat intelligence; increasing the efficiency and effectiveness of IA processes; secure by design; and policy.

Defining the "perimeter" of MoD

10.1 The nature of cyber threat means the supply chain is also liable to attack and its vulnerability being, potentially, a "weak link" access to MoD systems. Risk mitigation actions might include sharing threat intelligence, providing "best practice" guidance and improving identity and access management. Government policy is to encourage the use of SMEs in the defence supply chain. These companies may require additional support to accelerate their cyber-security maturity.

Sharing threat intelligence

10.2 The trusted sharing of each organisation's operational experiences will improve the overall cyber security posture. Individual risk assessments will be informed by wider experience enabling them to deliver up to date and valuable conclusions and, hence, more timely mitigation. The UK Government's Cyber Security Operations Centre should be a key part of this exchange.

Increasing efficiency and effectiveness of IA processes

10.3 MoD can ensure that a "lean" IA approach, driven from a close understanding of business risk, is applied. This will be more effective in that it will ensure assets are appropriately protected rather than a broad brush approach which may over-protect some assets and under-protect others.

Secure by design

10.4 MoD could lead wider government in endorsing "secure by design". Through its understanding of the threat MoD could encourage its suppliers to adopt an affordable risk based approach to information security and, hence, reinforce that security is an essential, rather than excessive, differentiator.

Policy

10.5 MoD should explore the policy options for "rules" governing operations in cyber space and its increased freedom of action; the extent to which it can actively defend its assets and interests in near real-time without need to invest time seeking higher approvals. It would need to determine how to deliver these operations given limitations in critical skills.

11. MoD could also explore, within the context of the existing national crisis response, any requirement to refresh the command and control mechanisms to ensure they are "fit for purpose" in the cyber age.

12. The development of a business case for investment in cyber defence can be challenging due to the requirement to quantify the risk of cyber-attack through measures of vulnerability and threat. The private sector has the identical challenge. It follows there is an opportunity to share approaches. In addition to simply sharing "best practice" this has the potential benefit of common understanding of "return on investment" in cyber-security which would avoid the scenario where one party chooses to invest and one does not hence rendering the investment worthless.

Resource Availability and Management

13. Cyber expertise is scarce across the UK and the market is very competitive. In common with many organisations, MoD is likely to find it difficult to recruit and retain suitably qualified and security cleared staff.

14. The National Cyber Security Strategy sets out a range of initiatives to address this resource gap. It follows that MoD should encourage government to develop an action plan to implement these initiatives and to close the skills gap as a priority. In the US, for example, the public/private "US Cyber Challenge" has been established to find 10,000 new cyber security professionals.

15. In the short-term MoD may need to draw on resources from the private sector although this is likely to be a partial mitigation. For example, an active defence and offensive capability will be particularly difficult to establish as this capability is not normally required within the private sector.

16. It is possible, with new delivery models, that the private sector could not only be a source of skilled resources but deliver "surge capacity" through a "cyber reserve". In addition, the private sector can be a partner in addressing the national shortage of cyber skilled professionals. Here MoD, wider government, the private sector and academia could work together to identify core security skills and to encourage and provide education and accreditation of relevant professionals.

17. To inform the development of the appropriate skills base, the MoD must understand the scope and scale of resource required to counter the current threat, and then predict the change in cyber threat and forecast the impact on resource requirements.

18. The pace of change in cyber threats to information systems and platforms will require the MoD, working with its supply chain, to maintain a fast-moving, agile defence:

- the commercial contracting structures that the department employs with the supply chain should enable this to happen;
- the security requirements for new platforms must be considered from the outset as an integral part of the overall requirement definition; and
- the security requirements for many long term equipment and platform refresh programmes may have been baselined well before the understanding of cyber threat reached its current state of maturity, and may now need case-by-case review.

20 February 2012

Written evidence from EADS

Introduction

1. EADS welcomes this opportunity to respond to the Defence Select Committee's inquiry on cyber-security.

2. This response opens with an executive summary followed by background information on EADS' presence in the UK and the cyber capabilities of its Astrium and Cassidian units. It then addresses some of the specific issues raised by Committee.

3. Given the Committee's intention to return to the topic of cyber-security, we would welcome the opportunity to contribute to any further work investigating a broader range of issues beyond the scope of this present inquiry.

Executive Summary

4. The cyber-security threat is real, persistent, and continually evolving. It is targeted at both the public and private sector and knows no international boundaries.

5. The cyber-security threats that are visible represent only the "tip of the iceberg" and in reality a true understanding of the potential dangers is not yet known.

6. A simple "boundary defence" approach will not be sufficient. MoD must defend from within to truly mitigate the developing cyber threat.

7. Industrial partners have a great deal of experience helping public and private sector organisations in the UK and around the world deal with cyber-security threats.

8. In light of this, enhanced, two-way, communication and information sharing between the public and private sector, with government playing a strong coordinating role and providing greater clarity on the nature of the threats they face, would enable the latest international experiences to be used to the benefit of UK cyber defences.

9. Specifically, EADS recommends that industry sits on specially created Cyber Boards where information on the very latest cyber threats, risks and mitigation measures can be shared. Such an approach, as outlined in the government's Cyber Security Strategy, would help foster a true partnership between industry and government.

10. Another key requirement is bringing the activity to life, and executing the "doing" rather than the planning. Industry is experienced in "doing" cyber and is well positioned to form long lasting strategic partnerships that will offer greater resilience to the Government.

11. Industrial partners are investing a great deal to research and develop solutions to cyber-security threats and are well positioned to assist the government's decision making process and make up for any shortage of public funding.

12. EADS therefore recommends an approach that looks to improve how government and industry interact on three levels: Communications, Relationships and Resources. We believe that addressing these will ensure the UK has the most robust defence possible against the cyber-security threat we face.

About EADS

13. EADS is a global leader in aerospace, defence and related sectors. The EADS group of industries includes Airbus, the leading manufacturer of commercial aircraft, Eurocopter, the world's largest helicopter supplier, Astrium, the European leader in space programmes from Ariane to Galileo, and Cassidian, a leading provider of cryptography and other security solutions. EADS is the second largest aerospace and defence company in the world and a major partner in many of Europe's largest aerospace projects, including Eurofighter Typhoon. EADS has a major industrial presence in the UK. Over 18,000 high value-added, highly-skilled jobs are directly supported at EADS' 25 key UK sites, and a further 135,000 jobs are indirectly supported throughout the UK supply chain.

EADS in the UK's Cyber-Security Capabilities

14. EADS' UK businesses with a specific involvement in cyber-security include:

(a) **Astrium.** With bases in Stevenage, Portsmouth, Poynton and Surrey, Astrium is a world leader in military and civil satellite systems, Earth observation, science and navigation programmes. It is a $3 billion business, the No.1 space company in Britain and Europe, and No.3 worldwide, after Boeing and Lockheed Martin. Astrium is responsible for delivering secure satellite communications for MoD through the Skynet 5 programme.

(b) **Cassidian.** Based in South Wales, Cassidian provides lead systems integration, information assurance, cryptography, and other cyber services to support the Armed Forces, Government agencies and Emergency Services in their cyber defence strategies. Cassidian has consolidated its cyber security portfolio and competencies into a dedicated International Cyber Security Centre which shares the knowledge, intelligence and best practice gained from many years of experience in the cyber security domain with its global customers. Its cyber-security activities for the UK Government include computer network defence operations for MoD's Defence Information Infrastructure programme, provision of Cryptography solutions to many government agencies and Consulting Services to help government customers counter the cyber threat.

15. Cassidian and Astrium's specialist expertise in providing cyber protection and cyber incident response for defence and government customers around the world provide both companies with awareness of the latest cyber threats. EADS invests significantly in R&D and is actively developing cyber-defence capabilities across many technical domains from secure cryptography solutions to secure satellite communication capabilities. Innovation is key to the R&D development processes as EADS is constantly looking to reuse existing research from other sectors to bolster the company's knowledge. For example, EADS has expertise in software design methodologies and techniques used to assure safety critical software on commercial and military aircraft which is being further developed to identify security vulnerabilities in software designed for use on both aerospace and terrestrial platforms and systems. In addition, Cassidian is applying technologies developed to protect Critical National Infrastructure Industrial Control Systems to other domains and industries.

16. Security is embedded throughout EADS' culture and approach to business. Over 500 people in Cassidian and Astrium are actively involved in developing and designing cyber-defence capabilities.

17. Furthermore, as a global organisation EADS is able to apply the significant international resources, experience, skills, and knowledge of the latest cyber threats in a local context.

Detailed Response

Improving communications

18. The nature of the cyber-security threat is real, persistent, and continually evolving. It is targeted at both the public and private sector and knows no international boundaries. It would therefore be dangerous to view this threat as simply a UK issue, and try to deal with it unilaterally.

19. Although the cyber-security threat is recognised, it is not yet adequately defended or managed. In fact the cyber-security threats that are visible represent only the "tip of the iceberg", and a true understanding of the potential dangers is not yet known. Similarly, the impact of a cyber-attack could be much more severe than is currently generally understood.

20. There is therefore a requirement to assess the impact of an aggressive cyber-attack on power, water and food distribution, and how an adversary could exploit this.

21. Industrial partners have a great deal of experience helping public and private sector organisations in the UK and around the world deal with cyber-security threats.

22. In light of this, enhanced, two-way, communication and information sharing between the public and private sector, with government playing a strong coordinating role and providing greater clarity on the nature of the threats they face, would enable the latest international experiences to be used to the benefit of UK cyber defences. For example, the risk of attack could be reduced by enhancing the mitigation measures currently in place via anti-jamming or Advanced Persistent Threat (APT) monitoring.

23. Given the nature of the cyber-security threat, a more open and advisory approach would have many advantages, and is likely to result in the MoD and Armed Forces being offered a greater range of protective measures (we would draw a comparison to current publicity highlighting the threat of car crime which warns people not to leave their valuables in their car).

24. MoD's existing cyber capabilities are well positioned to contribute to, and support, the government's overall approach in this domain. However, command and control of non-MoD capabilities is not currently envisaged, or truly realised, by Government.

25. Astrium and Cassidian are, respectively, the sole partners for delivering MoD's secure satellite service provision and computer network defence operations for MoD's network through the Skynet 5 and Defence Information Infrastructure programmes.

26. With this in mind EADS believes the UK Government needs to recognise the power that can be created by defining a group of trusted "Cyber Savvy" industrial partners that both understand the threat and appropriate mitigation strategies and can help all relevant government departments tackle the threat in a coordinated manner.

27. A pre-requisite of such collaboration is giving industry and other specific organisations the freedom to share intelligence anonymously.

Industry's relationships with Government, MoD and the Armed Forces

28. EADS is supportive of full sharing and openness by industry of R&D and other critical technical developments, as well as the development of common standards, to permit the seamless integration of multivendor security products and services.

29. EADS would also actively encourage MoD and wider Government to enhance and improve its level of engagement with industry. While there is a good level of engagement at the technical and programme level, there is room for improvement in terms of utilising industry's expertise to inform the development of long term strategic and operational policy.

30. There is therefore a requirement for a central agency to draw together the UK's entire cyber defences, comprising MoD, other government departments, and Critical National Infrastructure providers in order to provide clarity on the most appropriate national reaction, response and governance to cyber-security issues. At present it is not clear who owns the coordinated response to a national cyber security incident. Greater information sharing and technical interoperability is key to enabling a truly cross governmental and coordinated approach to major cyber-attack.

31. Initiatives that improve awareness and share information must be applauded, but ultimately acting upon such information in a coordinated and structured way is essential. EADS' recommendation is to initiate a series of scenario-based cyber exercises, both simulated and real time, involving a multi-agency response, to test and improve these capabilities.

32. Government should nominate a department or agency to take the lead, including an advisory role, in these types of exercises to ensure their experience is shared across the key agencies.

33. EADS recommends the MoD's Global Operations & Security Centre (GOSSC) should act as the central hub for the UK's response to a cyber-attack, and further recommends it be re-named the Governmental Operations & Security Centre, with top level Governmental Command and Control teams working alongside MoD in this environment.

34. EADS also recommends the Cyber Emergency Response team is extended beyond MoD, the National Security Council, Cabinet Office and GCHQ to include industrial partners because the private sector often possesses expertise mitigating the latest threats.

Maximising the impact of available resources

35. Cyber-security is the fastest growing threat to the UK and there is now a requirement for greater investment by Government and MoD to address this. The UK can no longer afford to just paper over the cracks—more money needs to be allocated to solve the problem.

36. It has often been said that the price of security is constant vigilance. In our contemporary world that is only half the task. Today, that price must also include constant innovation; pro-active, strategically-guided, but free-thinking, innovation.

37. Today the MoD is primarily focused on the protection of fixed assets and the traditional battlefield via advanced network security. The more subtle threats like APT and social engineering techniques that are used to compromise system security are increasingly becoming more prolific. Traditional boundary defence will not work to detect and mitigate these threats, because vulnerabilities inside the boundary are not sufficiently managed.

38. National infrastructure owned by the private sector has the same responsibilities as those owned nationally and must stand up to the cyber threat. Addressing the cyber-security threat to the UK must bring

together the public and private sectors, as well as academia. Fundamentally, success will depend upon the development of skills and knowledge across all industries, government and academia.

39. The work done by UCL's Institute for Resilience Studies provides strong doctrine recommendations regarding the security of Critical National Infrastructure which EADS would like to bring to the Committee's attention.

http://www.ucl.ac.uk/isrs/publications/CyberDoctrine

40. In this document, the cyber environment is described as "clouds of fog and friction", at the centre of which is the citizen, dependent upon critical infrastructures and network services from public, private and voluntary sectors. Currently there appears to be a distinct lack of integration, and chain of command and actions seems to have moved to individual agencies.

41. Strong relationships have been developed via the launch of Office of Cyber Security & Information Assurance (OCSIA) which appears to be shaping the environment. However, the interface between OCSIA and industry has yet to emerge. Industry's focus must be on the provision of Cyber Consultancy to support the shaping of UK Cyber strategy and protection mechanisms.

42. The risk to critical national infrastructure is probably not a legislative issue as the adversaries launching cyber-attacks pay no heed to legislation. Where legislation is needed is to support the protection of Intellectual Property rights, since IP theft has been identified as the biggest cybercriminal impact on the UK economy. (Estimated by the Cabinet Office[10] to cost £9.2 billion per annum to the UK economy). Legislation needs to force organisations to declare the occurrence and impact when IP is stolen or lost. This is an important protection for shareholders.

43. Working from the old adage that attack is the best form of defence, it is clear that in developing our defensive capabilities we now have a much clearer understating of how potential aggressors may attack. We need to form a view on how our defensive capabilities could be turned to our advantage, to challenge those who mean harm to UK Defence and infrastructure. This proactive stance must involve using knowledge of attack vectors (gained by both government and industry) to bolster the UK's defensive capability.

44. The Government's ability to respond rapidly to cyber-attacks is a critical success factor. The Government's existing procurement processes can result in a bottleneck and hold up the roll out of dynamic cyber responses, so there is a requirement to accelerate the process as the threat to systems is exacerbated by delays in the procurement process.

45. In specialised areas we would recommend building on the successes of the Skynet programme, in which a PFI model is used to develop and manage the core infrastructure, thereby allowing industry to be more adaptable with flexible arrangements for procurement and MoD to benefit from a cost effective service delivery model which consumes only the services required at the time they are needed.

46. MoD and Government should adopt a service based approach to facilitate a rapid response to cyber-attacks. This approach would bring cost efficiencies, as less capital investment would be required by the customer. In addition to reducing the total cost of ownership to the MoD, a service based approach will increase flexibility and allow MoD to modify its requirements according to the changing cyber threat level and so adapt to peaks and troughs in demand.

47. There needs to be a clear recognition of Cyber as a profession, with continued development of skills throughout an individual's career, supported by exchanges between industry and government.

48. Increasingly industry is establishing advanced cyber training academies. Examples include the Cassidian Cyber Security Training Centre, which focuses on developing world leading cyber skills through intense practical training and development courses, or the Space School sponsored Astrium Security Academy which develops both security awareness and secure system design skills throughout the organisation.

49. Government should exploit industry's advanced skill set, which comes with significant international resource and knowledge, to support their cyber protection requirements.

16 February 2011

[10] *The cost of cyber crime;* Cabinet Office; February 2011; http://www.cabinetoffice.gov.uk/resource-library/cost-of-cyber-crime

Written evidence from Research Councils UK

BACKGROUND

1. Research Councils UK is a strategic partnership set up to champion research supported by the seven UK Research Councils. RCUK was established in 2002 to enable the Councils to work together more effectively to enhance the overall impact and effectiveness of their research, training and innovation activities, contributing to the delivery of the Government's objectives for science and innovation. Further details are available at www.rcuk.ac.uk.

2. This evidence is submitted by RCUK and represents its independent views. It does not include, or necessarily reflect the views of the Knowledge and Innovation Group in the Department for Business, Innovation and Skills (BIS). The submission is made on behalf of the following Councils:

- Arts and Humanities Research Council (AHRC).
- Biotechnology and Biological Sciences Research Council (BBSRC).
- Engineering and Physical Sciences Research Council (EPSRC).
- Economic and Social Research Council (ESRC).
- Medical Research Council (MRC).
- Natural Environment Research Council (NERC).
- Science and Technology Facilities Council (STFC).

3. The Engineering and Physical Sciences Research Council (EPSRC) invests in cyber security research and training through the Global Uncertainties programme of the research councils.

4. EPSRC is the main UK Government agency for funding research and training in engineering and the physical sciences, investing more than £850 million a year in a broad range of subjects, including in cyber security. EPSRC invests in internationally excellent UK science and engineering research in funding primarily in universities, and draws on independent advice to help inform research strategy and make investment decisions. EPSRC also supports the financing of postgraduate training to ensure the ongoing supply of skills for academia and business. BIS is the main supporting Department.

5. Improving the level of interactions between business and the research base in the UK universities is a priority for EPSRC. The EPSRC vision is for the UK to be as renowned for knowledge transfer and innovation as it is for research discovery. EPSRC is working with universities, businesses, charities, and government departments on joint initiatives and activities, to understand their needs and challenges and use this information to inform strategic priorities and investment plans. EPSRC funds a range of research projects that are relevant to the real world research needs of many organisations. To help ensure that the research EPSRC sponsors have impact beyond academia we strongly encourage collaborative working with users in both the public and private sectors. As a result about 40% of EPSRC's portfolio of research projects typically features user engagement of some kind. EPSRC has a strategic relationship with the Technology Strategy Board and supports a number of joint initiatives with that organisation.

6. The Aerospace, Defence and Marine sectors are a priority for EPSRC collaboration due to their R&D intensity and importance to the UK economy. The current EPSRC portfolio relevant to these sectors has a total value of around £300 million in 300 research projects. The majority of the defence related grants support projects focused in materials or electronics with a smaller number of computational projects. There are also a number of security related projects including research related to terrorism, cyber security, CBRN (Chemical, Biological, Radiological and Nuclear), crime and ideologies. There are around 300 collaborators involved in this portfolio.

7. EPSRC has entered into Strategic Partnerships with a number of organisations in the Aerospace, Defence and Marine sectors. Examples include:

- Airbus/EADS—focused on reducing in flight drag via the creation of an active aircraft system.
- BAE Systems—focused on autonomous and intelligent systems; design, manufacture and maintenance of Unmanned Aerial Vehicles (UAVs); systems engineering; modelling, design and the building of integrated decentralised data systems; and technological, operational and strategic issues for next-generation industrial service organisations.
- GE Aviation—focused on electrical power and actuation technology, smart composites and metallurgy to enable the delivery of future electronics systems to aircraft and also pave the way towards adaptive wing technologies through the use of new materials.
- MoD/Dstl—focused on data intensive systems; signal processing; enhancing the damage tolerance of materials; and the battery-free soldier.
- Rolls-Royce—focused on structural metallurgy.

8. EPSRC is actively engaging with the Aerospace Technology Strategy Group (ATSG) and the Aerospace and Defence Knowledge Transfer Network (KTN),and is developing a strategic relationship with AWE.

9. EPSRC has made cyber security a strategic research priority. It is supported as a core theme in the multidisciplinary Global Uncertainties programme supported by all the research councils.

Why is research into cyber security important?

10. Better cyber security research is a fundamental requirement for the effective and reliable information infrastructure on which the UK's future prosperity relies and for tackling future threats to our security. The dependence of societies on the internet and other network-based services is increasing, not only through personal and corporate use of these services but through the development of the internet of things which are a vital part of the "smart" society, and through energy efficiency developments, improved mobility, adaptability to changing circumstances and events and economic growth. Research and development in the security aspects of these services and associated technologies are vital for the quality and dependability of service from them. Research and training funded by EPSRC is an important underpinning component of better cyber security, and is helping to ensure a critically important UK capability in this area. Researchers funded by EPSRC are already contributing to better cyber security in the UK.

11. The work EPSRC support is carried out in UK universities. Much of the research activity is driven by the curiosity of academic researchers. EPSRC has been supporting research and skill development underpinning cyber security for many years. Much of this research has been carried out in collaboration between the research councils and in partnerships with key agencies including GCHQ, CPNI and Dstl. The UK has world-class research in cyber security, building on internationally renowned ICT and mathematical science capabilities in the universities. There is expertise in computing, mathematics and the sociological and psychological disciplines that shed light on governance issues and on human behaviour and enable the building of better, more resilient systems which are better designed and easier to use. Good cyber security requires long-term underpinning research and skill supply that can keep pace with a fast changing environment and with future horizons.

What cyber security research does EPSRC fund?

12. Research relevant to cyber security issues is funded primarily by the EPSRC's Information and Communication Technologies theme. The EPSRC investment folio tends to address issues that are technological. It includes everything from fundamental work on quantum computation, cryptology and quantum key distribution through to more human-centred, work which, for example, tries to understand the practice of software engineers or develop methods to detect deceptive behaviour online. There are no technological areas relevant to cyber security in which EPSRC does not fund research, though the level of support varies. EPSRC manages its investment in cyber security as a core priority in the Research Councils UK[11] Global Uncertainties[12] programme.

13. The Global Uncertainties programme brings together the activities of all seven UK Research Councils to examine the causes of insecurity and how security risks and threats best can be predicted, prevented and mitigated. The programme is managed by the Economic and Social Sciences Research Council on behalf of Research Councils UK (RCUK). Commencing in 2008, it will run until 2018. The total funding of research and related work accredited to the Programme amounts to more than £220 million. It aims to integrate current research investments as well as support new multi-disciplinary research in security. The six core areas are Cyber security**;** Ideologies and beliefs**;** Terrorism**;** Transnational organised crime**;** Threats to infrastructures**;** and CBRN.

14. The programme helps governments, businesses, societies and individuals to better predict, detect, prevent and mitigate threats to security. The programme enables more effective co-ordination across RCUK and other stakeholders to maximise the impact of the activities that are funded through:

- Facilitating and supporting high-quality, interdisciplinary research that is problem-based.
- Co-design, co-production and co-delivery of research and linking research base expertise with end users.
- Co-operation in future strategy development with users so that activities are aligned with shared goals.
- Shared horizon-scanning activities to identify and respond to emerging challenges and priorities.

15. Engaging with the public and other users to ensure research is addressing relevant questions and issues. The Programme receives external advice on its strategic priorities and direction from its Strategy Advisory Group which has representatives drawn from academia, government, business and the third sector and is chaired by Sir Richard Mottram, GCB, formerly Permanent secretary at the MoD.

16. A list of cyber security-relevant research and researchers funded by the seven Research Councils is maintained and monitored; in practice the vast majority of funding in the area comes from EPSRC.

[11] www.rcuk.ac.uk
[12] www.globaluncertainties.org.uk

How much cyber security research does EPSRC fund?

17. Despite some problems relating to the definition and scope of cyber security it is estimated that each year EPSRC spends about £15–20 million supporting the national capability in research and doctoral level training.

18. The estimate for the overall UK annual spend on academic cyber security research is around £40–45 million. About 100 PhD students are estimated to graduate each year, making a significant contribution to enhancing the UK's capability in better cyber security.

What is EPSRC doing to support the UK national cyber security effort?

19. EPSRC's funding is provided on the basis of the quality of the research proposed and its strategic need. EPSRC has published a discussion paper to raise the visibility of increasing research in cyber security,[13] a Cyber Security strategy[14] and a position pamphlet.[15] The position pamphlet is intended for a wide audience and contains some useful statistics and case studies drawn from examples of EPSRC investments in UK universities.

20. During the next 15 months, the EPSRC has plans to strengthen the university research community in cyber security, in terms of the links between researchers and suppliers/users, improving the networking between researchers, and investing in innovative new research. EPSRC has entered into a strategic relationship with GCHQ which is helping to focus activities and increase partnerships and coordination of research effort. GCHQ is wishing to engage much more with the science base than previously. This is part of a recent strategy to embrace open innovation. It wishes to create a number of strategic partnerships with universities in cyber security research, but recognises that such partnerships have to be selective to make it effective.

21. GCHQ and EPSRC are jointly pioneering an experiment to create Academic Centres of Research Excellence (ACE) in Cyber Security based on their current level of research activity and reputation. It is hoped that by recognising such centres of research excellence in cyber security the university science base will become less fragmented and collaborations with problem owners will increase. The intention is that the Centres will be widely recognised as having an international research reputation in cyber security and a critical mass of effort devoted to cyber security research. EPSRC and GQHQ wish to regard these Centres as being national centres of excellence in cyber security research in the hope that they will stimulate other organisations engaging with the science base in cyber security. GCHQ plans to put resources in place to establish a relationship with each centre and plans to promote the Centres among its supplier companies and others. This initiative is referred to in the 2011 National Cyber Security Strategy[16]. EPSRC intends to offer a small grant to each of the recognised ACEs to support their activities as a centre, and help them to engage with business and other users to share problems and expertise. The outcomes are expected to be made public in April 2012.

22. EPSRC also plans to create two Research Institutes in universities of about £3 million each jointly with GCHQ which will influence their scope based on future challenges in cyber security. The first will focus on the science of cyber security and a decision on its location is expected to be made in summer 2012. The content of the second is currently being determined. These are also referred to in the 2011 cyber security strategy.

23. EPSRC also has a strategic partnership with Dstl and it is planned to invest jointly about £2.5 million in 2012 into research in Data Intensive Systems.

24. EPSRC is continuing to facilitate engagement of academic researchers with businesses and other users to maximise the impact of their research through organising research showcases events at which the researchers whom EPSRC funds presents the outcomes of their research to those interested from industry, policy makers and others. The first showcase event was held in November 2011 and attended by over 100 people. Such opportunities to engage with those same businesses and users help to refine the EPSRC approach.

25. EPSRC is liaising with the Cabinet Office's Office of Cyber Security and Information Assurance (OSCIA), GCHQ, Dstl, the Home Office and BIS. The Chief Scientific Adviser (CSA) to the MoD is a member of the EPSRC Council and EPSRC has close relations with the previous and future CSA of BIS.

Where is cyber security research being carried out?

26. Cyber security research expertise is found, to varying degrees, in around 50 UK universities. Relatively few, however, have large programmes of effort specifically in cyber security. EPSRC invests in significant activity in about a dozen universities. A better picture of the landscape will emerge later in 2012 when the outcome of the initiative to identify academic centres of excellence is known.

[13] http://www.globaluncertainties.org.uk/Image/Cyber%20green%20paper_tcm11–15897.pdf#false
[14] http://www.epsrc.ac.uk/ourportfolio/themes/globaluncertainties/strategy/Pages/default.aspx
[15] http://www.epsrc.ac.uk/SiteCollectionDocuments/Publications/corporate/CyberSecurityHLP.pdf
[16] http://www.cabinetoffice.gov.uk/resource-library/cyber-security-strategy

What might EPSRC do next?

27. The relatively small amount of resource we have will be used to build on our current portfolio and address strategic gaps, in partnership with other Research Councils through the Global Uncertainties programme and with user stakeholders.

24 February 2012

Written evidence from McAfee

EXECUTIVE SUMMARY

— McAfee welcomes this opportunity to respond to the Defence Select Committee's inquiry into Defence and Cyber-security. As the world's largest dedicated security company, McAfee is at the forefront in combatting the cyber-threat for a range of stakeholders including governments, public and the private sector, and individuals.

— We welcomed the elevation of the cyber-crime threat to "Tier 1" status in the National Security Strategy (NSS) and the Strategic Defence and Security Review (SDSR). Protecting against cyber-attack requires action at many levels. Implementing technological solutions is vital but the skills, behaviour and attitudes of personnel are equally crucial.

— McAfee also welcomes other initiatives by the Government in raising awareness of or combatting the cyber-security threat, such as the London Conference on Cyberspace, the Cabinet Office Cyber Security Strategy (CSS) and the creation of the Defence Cyber Operations Group (DCOG).

— As a leading authority on cyber-security, McAfee believes that it is more important than ever before for the Ministry of Defence (MoD) and Government to undertake in-depth, regular reviews of the evolution of the cyber-threats the UK faces. The best-in-class tools we have developed and have at our disposal coupled to the unrivalled experience we have in this specialised area, we believe, can enable the Government to do this in the cyber-security space.

— By undertaking regular risk assessments of the cyber threat the Government can have a more adaptive strategy to prepare against the dangers of cyber-attack, malware and other threats. However, in what are difficult financial times it is important for the Government to work in tandem with the private sector, and draw on the wide range of technical expertise and experience that they have to offer. McAfee, for example, undertakes regular studies of the ever-changing cyber-threats, such as our recent Night Dragon, Shady RAT and Operation Aurora reports.

— This is a problem that can affect all parts of government, and so the response must be equally wide-reaching. Rather than simply continuing to use suppliers to fix and patch systems that fail or come under attack, a systems integrator for the whole of government could be adopted; the issue is just as important to the Department for Work and Pensions for example, as it is to the MoD. This would provide a more cost-effective solution that is proactive, rather than reactive to this ever growing threat.

Issue 1: *The nature and threat of the cyber-security threat to the Ministry of Defence and Armed Forces, operations and capabilities*

1.1 The cyber-threat is a complex one and one that is growing daily. As reported in our Threats Report for the Third Quarter of 2011, there were 70 million malware samples collected by McAfee and stored in our "malware zoo." As recently as October of last year, Foreign Secretary William Hague confirmed that on average British Government and industry computer systems face over 600 cyber-attacks every day.

1.2 Following the elevation of the cyber-threat to "Tier One" status in the NSS, cyber-security has suddenly become a far larger part of the nation's defence. McAfee welcomed the recognition of this through the commitment of additional resources and new organisations (eg DCOG) in this regard.

1.3 McAfee has frequently seen cyber techniques complement traditional methods of intelligence or espionage operations with many players accusing others, friends and foes alike. It is a very low-cost way of spying, always leaving room for plausible deniability, does not endanger human lives and at present is highly effective. What is yet to be seen on a larger scale is the use of cyber as part of the arsenal in an armed conflict. So far this has been witnessed only on a rather small scale with very limited sophistication of the attacks, for example, in the Georgia conflict.

1.4 However, the situation is now beginning to change. Many countries realise the crippling potential of cyber-attacks against critical infrastructure and how difficult it is to defend against them. Their potential opens up opportunities for attack by small countries or organizations, particularly if there are few targets to strike back against. The Stuxnet attack on Iran's nuclear facilities was a game-changing event in many aspects; one of them was to make it absolutely clear that the threat is real and what impact such attacks could have.

1.5 Given the nature of its business and responsibilities, the Ministry of Defence (MoD) is one of the most attractive and high-profile targets for cyber-attacks. These types of attack can range from the basic; such as fake anti-virus, spam emails and malicious websites, to the complex and highly dangerous; such as advanced

malware, remote access tools (RATs) and attacks on portable devices that handle sensitive material such as mobile phones and laptops.

1.6 There is also the increasing threat of cyber-espionage. While Government systems have been the traditional and obvious target for cyber-attacks, attention is now also focusing on the suppliers of the equipment our Armed Forces use. For example, it was recently reported that the Pentagon was assessing whether Chinese espionage (specifically Chinese hackers actually sitting in on what were supposed to have been secure, online program-progress conferences) was the reason behind the delays and cost increases of Lockheed Martin's F-35 Joint Strike Fighter programme.

1.7 If Britain's adversaries are gaining access to information on technology and equipment that is in service or intended to be procured for our Armed Forces, this could seriously compromise the capability and ultimately the safety. One way to insure against this type of threat is for Government to ensure that those companies who work with the Government on matters relating to the Armed Forces or national security comply with minimum security standards to protect sensitive data.

1.8 Operation Shady RAT was a recently completed investigation of targeted intrusions into more than 70 global companies, governments, and non-profit organizations during the last five years.[17] It showed an historically unprecedented transfer of wealth—closely guarded national secrets (including those from classified government networks), source code, bug databases, email archives, negotiation plans and exploration details for new oil and gas field auctions, document stores, legal contracts, supervisory control and data acquisition configurations, design schematics, and much more has "fallen off the truck" of numerous, mostly Western companies and disappeared in the ever-growing electronic archives of dogged adversaries.

1.9 Another aspect of the cyber-espionage threat to industry and Government is the level of awareness and knowledge of the threat by individual employees and civil servants. Malicious websites or programmes encrypted onto fake free or promotional USB devices or CDs that are then loaded onto computers by the user, threats to mobile devices or using work equipment to log onto unsecure networks away from the office can all present vulnerabilities that can be exploited by cyber-attackers. Given this danger, it is vital that individual employees, both in Government and industry, are alerted to the dangers that now face them.

1.10 In this regard, McAfee welcomed the MoD's "Think before you share" campaign, designed to encourage Service personnel and MoD civilians to carefully consider possible repercussions before posting information on social networking sites. Indeed it is similar to McAfee's partnership with Facebook to provide users with free advice and tools on how to protect against cyber-threats that they may encounter on the social networking site and elsewhere. Initiatives such as this are a step in the right direction, however, such campaigns could and should be promoted further across Government and industry.

Issue 2: *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

2.1 McAfee welcomed the publication of the UK Cyber Security Strategy as a method of setting out how the UK will support economic prosperity, protect national security and safeguard the public's way of life by building a more trusted and resilient digital environment.

2.2 The Strategy has major implications for the MoD because it is the most prominent Department in terms of both carrying out and defending from cyber-attacks. McAfee also welcomed government plans to share tactics and technology with businesses. Effective cooperation between Government and industry is a vital component of the Government's cyber-security plans in terms of enabling Government to draw on the extensive knowledge and experience within the private sector, while imparting its own requirements and issues to enable the private sector to better use its resources.

2.3 With regard to Critical National Infrastructure (CNI) protection, the MoD has an important role to play. Many of its functions are reliant on the continued functioning of CNI and so it is vital that they are adequately protected. An added dimension to this is that the majority of CNI is owned by the private sector, so it is equally important that those companies that own CNI assets are aware of and protecting against the cyber-threat.

2.4 Threats to CNI networks have recently garnered a lot of attention, and there is a very good reason for that; it is one of the few areas in which a cyber-threat has the potential to threaten real loss of property and life. A survey of global cyber experts in the Security & Defence Agenda's latest report; "*Cyber-security: The vexed question of global rules"* (which was sponsored by McAfee) showed that damage or disruption to CNI is seen as the greatest single threat posed by cyber-attacks.[18] 43% identified this as a national threat with wide economic consequences, while 45% view cyber-security *as* important as border security.

[17] *Revealed: Operation Shady Rat*, http://www.mcafee.com/us/resources/white-papers/wp-operation-shady-rat.pdf

[18] *Cyber-security: The vexed question of global rules*, http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf

2.5 Starting in November 2009, coordinated covert and targeted cyber-attacks have been conducted against a specific aspect of CNI—global oil, energy, and petrochemical companies. These attacks have involved social engineering, spear-phishing attacks, exploitation of Microsoft Windows operating systems vulnerabilities, Microsoft Active Directory compromises, and the use of RATs in targeting and harvesting sensitive competitive proprietary operations and project-financing information with regard to oil and gas field bids and operations. McAfee conducted a detailed study of the attacks on this particular sector, which we named "Night Dragon".[19]

2.6 Well-coordinated, targeted attacks such as Night Dragon, orchestrated by a growing group of malicious attackers committed to their targets, are rapidly on the rise. These targets have now moved beyond the defence industrial base, Government and military computers to include global corporate and commercial targets. While Night Dragon attacks focused specifically on the energy sector, the tools and techniques of this kind of attack can be highly successful when targeting any industry. Our experience has shown that many other industries are currently vulnerable and are under continuous and persistent cyber-espionage attacks of this type, particularly the defence industry. More and more, these attacks focus not on using and abusing machines within the organisations being compromised, but rather on the theft of specific data and intellectual property.

2.7 The relationship between the MoD, National Security Council, Cabinet Office and GCHQ is a complex one, but one that must be managed correctly and work effectively with regards to the continually evolving nature of the cyber threat. The MoD must coordinate its actions and planning with these and other Departments to ensure that there is a comprehensive cross-governmental approach, rather than numerous strategies from each body or department that could result in confusion, confliction and duplication which will in turn lead to rising costs.

2.8 A single, uniformed approach from Government in relation to cyber-security is the most desired outcome, and the outcome that will deliver value for money, comprehensive protection and provide clear guidance for industry and opportunities for cooperation and sharing of knowledge and expertise. Given that the Cabinet Office published the CSS, this could be the Department that is given overall ownership and leadership on such a uniformed approach to provide direction to the rest of Government.

2.9 The CSS is a welcome step in this direction and provides a uniform strategy for cyber-security. However, while it is an effective document in terms of identifying the needs and shortcomings of the Government, it needs to be accompanied by a more detailed implementation plan and set of measurable targets.

2.10 In addition and with regard to the above-made points on CNI, because much of the UK's CNI is owned and operated by the private sector but yet is vital to the operation of Government and every-day services, it is therefore important that there are minimum security standards imposed on those companies that own CNI assets. A minimum standards register could be compiled by the Government and either made a pre-condition to be met by a private sector company before a purchase of a CNI asset, or applied retrospectively. Government could also consult private sector technology security companies such as McAfee on the appropriate standards that should be met. The SDA report provides evidence for such a need. Of those surveyed for the report over two thirds (67%) saw the need for more government regulation in the private sector.

2.11 In order to build up trust in the private company-to-private company and private company-to-Government relationships, pilot programmes could be conducted as has taken place in other countries. For example, as a result of growing fraud the US financial services set up the Financial Services Information Sharing and Analysis Centre to share information on attack techniques and cyber-threats to the banking systems. On a smaller scale, the 238 member Belgian Financial Sector Federation does similar work using freelance experts.

2.12 Indeed, the SDA report shows a desire for such action. While the majority saw such exercises as important, only one fifth surveyed in the private sector had actually taken part in such an exercise.

Issue 3: *How the Ministry of Defence and the Armed Forces are managing and planning responses to threats in the cyber domain, including;*

Skills, capacity and expertise within the MoD and the Armed Forces, including in research and development;

How the MoD and National Cyber Security Programme resources are being used to address cyber-security.

3.1 The MoD and Armed Forces are taking active steps, both independently and in coordination with the rest of Government, to manage and plan for the cyber-threat. The £650 million in funding announced in the SDSR, formation of DCOG, the CSS, consideration of cyber issues in the recent White Paper and the appointment of a SRO in Government for the security industry are all part of a welcome response to this threat, providing both recognition of the challenges we face and the shortcomings in our capabilities that need to be addressed.

3.2 There is measurable and demonstrable evidence that this effort is achieving success. The SDA report, which featured a country-by-country stress test of resilience to cyber-attack, gave the UK a score of four out of a possible five. This places the UK level with countries including the US, Germany, France Spain and

[19] *Global Energy Cyberattacks: "Night Dragon",* http://www.mcafee.com/ca/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf

Denmark, and only just behind Israel, Sweden and Finland who scored 4.5 out of five. No country obtained five out of five.

3.3 However, as mentioned above there needs to be a clear plan of action as to how the aims and vulnerabilities identified in the various strategies and reports that Government has produced are to be addressed. This can be achieved by working in partnership with private sector security companies who can assist in identifying the best method to achieve the aims of Government policy.

3.4 Indeed, such efforts have already occurred, such as the Science & Technology Committee's seeking of a demonstration on cyber-crime from McAfee and Symantec. But this is only a small example of a Committee, which can only recommend not form Government policy, acting under its own initiative to further develop and expand its knowledge. Similar and indeed larger endeavours need to be undertaken by Government in order for it to benefit from the wealth of knowledge and experience that the private sector possesses.

3.5 The survey in the SDA report confirms this need. It found that in both the private and public sectors, 56% highlighted a coming skills shortage as a future concern. The MoD's recent White Paper: "*National Security Through Technology*" also highlighted the need for industry and Government to cooperate more closely and to find "new ways to work together, establishing agile partnerships that can meet the changing cyber challenge."

3.6 One example of an effective Government-private sector partnership in the cyber domain is McAfee's work with the US Department of Defense (DoD) on its Host-Based Security System (HBSS) programme. Through the HBSS programme, the DoD is deploying McAfee's Host Intrusion Prevention and ePolicy Orchestrator software packages to centrally manage the security of more than 5 million servers, desktops and laptops (hosts).

3.7 Such a situation does not entail a reliance on only one private sector supplier, however. McAfee worked in partnership with Northrup Grumman to install HBSS software on the US Air Force's Non-Classified Internet Protocol Router Network, with 500,000 hosts installed with the protection over a six month period. McAfee also has 75 third-party companies whose products can be managed through this platform. HBSS also provided the DoD with a siloed approach to cyber-security; while one company was responsible for the overall integration of the programme, individual needs were siloed and managed by different contractors, thereby avoiding reliance on a single contractor.

3.8 The HBSS system provides system administrators with a significant improvement in situational awareness, allowing them to better respond to cyber-attacks, and also enables the DoD's Defence Information Systems Agency to collect and correlate alarms as cyber-attacks occur.

3.9 McAfee's relationship with the DoD is leading to improvements in our commercial offerings. For example, the ePolicy Orchestrator now features a three-tiered architecture that was required by the military, enabling security policies to work from the top down, while situational awareness moves from bottom up. At the same time, work with established Government departments, in this case the DoD in the US, provides McAfee with an excellent reference for future work with potential private sector clients. (More information on HBSS can be found in Annex 1.)

3.10 Overall, McAfee feels that the MoD and wider Government have made great strides since the National Security Strategy in identifying the needs of the UK to respond to the cyber-threat and in providing strategies as to how this threat can be met. However, more needs to be done in terms of the implementation of these strategies, and in these difficult economic times the Government cannot afford not to cooperate with technology security companies such as McAfee and draw on their extensive experience and knowledge to meet the ever-evolving nature of the cyber-threat.

21 February 2012

Annex 1

MCAFEE PARTNERS WITH US DEPARTMENT OF DEFENSE TO DELIVER ON KEY IT SECURITY REQUIREMENTS

McAfee launched an open architecture technology programme, largely in response to the needs of one of its largest customers, the U.S. Department of Defense (DOD).

McAfee technology underlies the largest IT security deployment within the DOD, the Host Base Security System (HBSS), which provides multi-layered threat protection for between 5 to 7 million host platforms worldwide. HBSS was launched after the DOD decided that host computer defence was critical to the protection of the Global Information Grid, and the system is mandated for installation on all unclassified and classified systems in the department.

McAfee® Host Intrusion Prevention solutions are the underlying technology of HBSS, providing monitoring, detection, and counters to known cyber-threats to the DOD's enterprise architecture and delivering integrated security capabilities such as anti-virus, anti-spyware, whitelisting, host intrusion prevention, remediation, and security policy auditing.

Recently, McAfee partnered with Northrop Grumman to deploy HBSS for the Secret Internet Protocol Router Network (SIPRNet) within the US Air Force. SIPRNet is the communications backbone of the DOD that facilitates the exchange of classified tactical and operational information at the secret classification level for both the Air Force and other branches of the US Armed Services. McAfee has also partnered with Northrop Grumman in the UK to deliver the company's cyber-test range, which was opened by Defence Minister Gerald Howarth in October 2010.

In deploying HBSS, the DOD wanted an open framework that would enable the department to plug in any number of solutions from different vendors. Largely in response to this need, McAfee initiated a technology partnering programme called the McAfee Security Innovation Alliance. The purpose of the McAfee Security Innovation Alliance programme is to accelerate the development of interoperable security products and simplify the integration of those products within complex customer environments.

McAfee security risk management solutions are at the heart of the McAfee Security Innovation Alliance programme, allowing organisations of all sizes to benefit from the most innovative security technologies. They now can simply snap into the McAfee management platform, McAfee ePolicy Orchestrator® (McAfee ePO™) software. Today, more than 100 technology partners across Europe, North America, the Middle East, and Australia have joined the alliance.

We believe that the McAfee Security Innovation Alliance programme provides an important value proposition for government and commercial customers who do not want to be locked into a single vendor.

Written evidence from Raytheon UK

Introduction

Raytheon UK would like to highlight the following areas for the Defence Select Committee inquiry into Cyber Security as it relates to the Ministry of Defence (MoD) and the Armed Forces.

Education

Skills and Cyber Subject Matter Experts

1. Raytheon UK would like to highlight the importance of education and information assurance awareness for cyber security. At every level the cyber threat can be mitigated by general awareness and safety conduct guides for IT users. Such awareness may not have been traditionally studied as part of the national curriculum. Where appropriate the inclusion of specialised cyber security modules within the traditional military educational establishments could support individuals interested in this field to nurture and expand their skills, particularly those tasked with computer network defence; attack and exploitation; and information assurance. Raytheon UK would highly recommend that this is done in partnership with industry and academia to ensure these modules can be adapted in a very fluid cyber threat environment.

Cyber awareness within the MoD

2. All employees should have a general awareness of how to protect and deal with a cyber threat and this training should be mandatory. Training solutions should be considered at all levels from the executive through to the practitioner level and rolled out within the MoD. Individuals and organisations need to be prepared with the knowledge and confidence to excel at computer network defence; attack and exploitation; and information assurance. By using virtual classrooms, Computer Based Training (CBT) and traditional classroom based activities, MoD personnel can be kept informed of how to detect, identify and respond to the many types of cyber threats as quickly as possible whatever location they may preside at. This must be a key cog in the MoD's Cyber Incident Response strategy.

Sensitivity of Information & Sharing

Cross sector collaboration with MoD

3. The role of the MoD in cyber security policy and implementation needs further clarification. We welcome the emphasis that the Defence White Paper has given to cyber security and the creation of the Defence Cyber Operations Group (DCOG) launched in April 2012, but industry needs further details on who will lead cyber security within the MoD and how cyber measures will be implemented through the newly formed strands and how the MoD will interact with other government departments such as OCSIA and GCHQ. Cyber security is one area that requires cross government and cross sectoral interaction to make the best use of resources and investment.

4. Raytheon UK are already collaborating with industry through the Intellect and ADS Virtual Task Force on Information Sharing. We would like to see how the MoD intends to ensure sensitive information is shared with industry to ensure it's supply chain is secured.

Research & Development

5. In order to help industry to develop the right solutions Raytheon UK would welcome a roadmap of cyber requirement and intended investments to be made by DSTL and MoD over the next 5 years. This can only be done in collaboration with industry and academia. R&D needs to be maximised with as many stakeholders as possible, to ensure security is in the design of systems going forward and cyber attacks are an acknowledged "almost expected" risk.

Future Collaborations

6. UN, NATO and the EU, through the European Organisation of Security, are looking at setting standards on cyber security and ways in which a country will deal with an attack. The UK needs to be clear on how it is co-operating with these institutions and how it intends to flow down the decisions to industry in a timely manner, again securing its supply chain.

7. Promoting greater levels of international cooperation and shared understanding on cyber crime needs to continue on the international platform. The Foreign and Commonwealth Office led conference on Cyberspace in 2011 should see involvement from the Ministry of Defence also. An understanding on how the new EU Directive on information systems and the implications of security provisions from the EU Data Protection Directive will impact suppliers and their system designs should be considered as early on as possible.

27 February 2012

Written evidence from Symantec

EXECUTIVE SUMMARY

- Cyber security is no longer just about antivirus and firewalls. The UK Cyber Security Strategy's acknowledgement of cyber security as a tier one level threat is an indication that the potential impact of cyber related attacks on the national security and defence capability of the UK are recognised.
- Discussions on acceptable norms of behaviour in cyberspace and development of specialised cyber defence units show how this topic has been elevated in the international arena.
- Given the issues raised by the Committee for discussion it is important to recognise that there is a difference between cyber security and cyber defence.
- It is important to understand the changing nature of the current online threat environment, to have the right information at the right time to identify and address key cyber threats and the importance of a multi-layered defence.
- Cyber attacks directed against government and critical infrastructures are seen as either targeted/tailored (incidents such as Hydraq and Stuxnet) or massive such as denial of service attacks (as seen in Estonia).
- A major security incident that can affect the strategic assets of a country, whether accidental or due to malicious outsiders or insiders, could impact that country's ability to command and coordinate its military forces.
- The more integrated and information–centric the infrastructures of the armed forces or a particular branch, the more the information security threats need to be taken into account.
- Effective information and communication technologies can be a key force-multiplier in a combat situation. Therefore the security and control of information and communication technologies becomes a critical component of any national security strategy.
- However, it is not enough to consider what the threat is from just the perspective of the military networks and systems, it is important also to understand the potential risks and vulnerabilities that can affect systems that are critical in supporting the armed forces.
- Increased technological sophistication of a country's armed forces has numerous advantages but may also create a new type of information security challenge that is not yet fully understood, studied or realised.
- The UK Cyber Security Strategy provides a considered response to the continuously evolving threat of cyber attacks and lays the foundations for required action to reinforce the defensive borders around our connected experiences.
- The MoD's role outlined in the strategy and the importance placed on the need to explore ways to strengthen engagement with industry partners is seen as appropriate and relevant.
- Coordination and partnership between public and private sector on cyber related issues is key to addressing cyber security challenges we face.
- Given the stealth and asymmetric nature of cyber attacks one of the biggest challenges to be faced is determining the moment a cyber security incident becomes "military" in nature.
- A discussion about a proportionate response to an incident also needs to try to determine what constitutes an "act of aggression". Distinguishing between "acts of aggression" and acts of espionage or cybercrime is particularly complex as malware will combine capabilities that can be used for multiple purposes.

— "He who defends everything defends nothing". Systems will be attacked and inevitably penetrated. It is extremely important that there is some kind of hierarchy of priorities and understanding of the interdependencies so as to be able to focus defensive resources on what needs to be defended the most.

— Cyber security threats are a global problem. Development of initiatives that can enable the sharing of technical expertise and guidance on addressing cyber security related incidents could strengthen or enhance national and international cooperation and colloboration.

— Further joint activities bringing the MoD closer to the technology community could help to identify specific technical requirements, enable industry to demonstrate existing technological capabilities and increase understanding of research developments in this cutting edge and highly technical area.

— Issues that may warrant further consideration by this Committee include the importance of recognising threats can be both external and internal, the threat is primarily asymmetric and the opportunity to address these challenges offered by new business models such as virtualisation and cloud computing.

Introduction

1. The recent publication of the UK Cyber Security Strategy and the acknowledgement by the UK government of cyber security as a Tier one level threat are indications that it is now an issue being taken extremely seriously due to the recognised potential impact of cyber related attacks on the national security and defence capability of the UK. The discussions around acceptable norms of behaviour in cyberspace and the development of specialised cyberdefence units in some countries indicate how the topic of cyber security has been elevated in the international arena. This is driven by a belief that networks and the internet have become another "dimension" of the battlefield like ground, sea, air and space. It is also driven by the increased reliance of our societies and critical infrastructure on computers and the internet. In addition there is an increased realisation that cyber-attacks, as a means to achieve an objective, have numerous advantages such as their asymmetric nature and the deniability that comes with them.

2. A key issue that Symantec believes warrants clarification upfront in this submission is the difference between cyber security and cyber defence. Often, in the media and in different discussions, the terms cyber security and cyber defence are used interchangeably. Other terms such as cyber war, cyber terrorism and cyber espionage are also often undefined or used in different contexts. It is important, for the purposes of this discussion, to distinguish the difference between these terms.

3. Cyber security is the activity of protecting one's information systems (networks, computers, databases, data centres, etc) with the appropriate procedural and technological security measures. In that sense the notion of cyber security is generic and encompasses all protection activities. However, cyber defence seems to be a much more specialised activity linked to particular themes and organisations. The distinguishing factors in what should make security different from defence in the networked, cyber, environment should be the nature of the threat, the assets that need to be protected and the protection mechanisms applied.

4. The UK is not alone in recognising the threat from the cyber or networked environment that we face today. NATO, in its next generation defence policy, described a number of threats that require consideration by strategists and policy makers. Proliferation of Weapons of Mass Destruction (WMD), terrorism, climatic change and cyber-threats are some of the areas of focus for NATO.

5. Cyber security has been a discussion topic for several years, attracting attention from policy makers, industry and the media. Historically this attention was fuelled by concerns of a major malware outbreak that could take over IT systems across the planet in a few minutes, causing substantial damage and disruption. Code Red, Nimda, Sasser and Slammer are a few examples of the threats that highlighted how a widespread infection could travel around the world, sometimes in a matter of less than thirty minutes.

6. But times now have changed. While there are now rarely the major malware outbreaks of the type we saw at the beginning of this century, with the notable exceptions like the Downandup/Conficker malware, what is seen now is a rise in targeted attacks, including incidents such as Hydraq and Stuxnet. The Stuxnet attack is a good example of how malware is being used as part of targeted cyber attacks on critical systems and networks. This is a significant step on from the traditional forms of cyber crime, such as fraud or extortion. What makes Stuxnet special compared to other threats is the malware's additional ability to steal information and also to cause physical harm by sabotaging the functionality of industrial facilities.

7. Just as the online threat environment continues to evolve, investment in cyber security seems to be increasing, as seen in the UK's £650 million investment, and so does the focus of policy makers and government officials. In fact, more and more government departments are attempting to procure information technologies and to adopt a posture that links cyber security with national security.

8. The decisive driver for this link is two-prone. First, it is based on the realisation that information and communication technologies are a key component of the national critical infrastructure. As a result, a major cyber security incident could cause significant disruption to the national critical infrastructure and affect the strategic assets of a country thus threaten national security. This type of activity such as a denial of service attack can be devastating in a time of national crisis.

9. Second, this link is based on the principle that effective information and communication technologies are a key force-multiplier in any combat situation. In warfare, the ability to project force depends on the effective communication and coordination of those in the field. The objective is to project maximum power with the minimum possible force in the shortest possible time. This requirement has existed from the beginning of time but it is the technology that alters the means. In short information is power. Confidentiality, integrity and availability of communicating information are key operational requirements. If one looks at history, effective communication has often played decisive role in combat effectiveness and survival of units. Similarly, insecure information and communication technology can have devastating effects on its user and partners connected to them.

10. Consequently, security and control of information and communication technologies becomes a critical component of any national security strategy. A major security incident can affect the strategic assets of a country, whether this is accidental or due to malicious outsiders or insiders. Such an incident can affect that country's ability to command and coordinate its military forces, or could result in it providing vital intelligence to the adversary about its capabilities, intentions and actions of friendly forces. Such a security incident would grant the adversary a decisive advantage over its opponent.

11. The following comments aim to provide input on the specific questions raised by the Committee

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

12. For the last seven years, Symantec has produced its *Internet Security Threat Report,* which provides an overview and analysis of worldwide internet threat activity and a review of known vulnerabilities and trends in areas such as phishing, botnets and spam. The report is based on the most comprehensive source of internet threat data which is gathered from Symantec's Global Intelligence Network. This network is based on 240,000 sensors in over 200 countries that monitor attack activities through the deployment of Symantec's products and services which actively protect businesses and consumers online. Information on the key finding of the latest *Internet Security Threat Report,*[20] published in April 2010 can be found at the end of this submission.

13. The nature and the extent of the cyber-security threat to the defence sector is dependant to the use of information and communication technologies by a modern army and may vary considerably depending on the characteristics of each branch of service. The more integrated and information-centric the infrastructure of the armed forces or of a particular branch, the more the information security threat needs to be taken into account. In addition, in order to get a complete understanding of the risk, it is not enough to consider what the threat is from just the perspective of the military networks and systems that can be affected by a cyber-attack. It is also important to try to understand the potential risks and vulnerabilities that can affect systems that are critical in supporting the armed forces in carrying out their mission or hold vital intelligence about the objectives of that mission.

14. It is difficult to fully predict the different threat scenarios in the current interconnected and interdependent environment, especially if one adds the critical infrastructure elements. A lot depends on the objectives of the adversary, its own operational planning and escalation path, as well as the tools and mechanisms at its disposal. Such tools could include the ability to "access" the target to insert the attacking code either remotely or through human intelligence. 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. These examples are non-exclusive and do not necessarily suggest that there is a vulnerability in any of these areas for the UK armed forces, but rather how a determined adversary could try to use the technological sophistication of a country's armed forces to attack it in different ways.

15. 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. Historically the security threat has been linked with the confidentiality, integrity and availability of communications and the use of electronic counter measures against devices and sensors that any armed force (even less technologically advanced) needs to have in the operations theatre.

16. In the area of the use of robotic devices, there are obvious information security challenges linked to the security of communications and the functionality of sensors. However, there is also the additional challenge of maintaining effective control of the robotic device, which—if compromised—could fail in its mission or even be used against its owner. This is even more the case because the technology used in military and other critical infrastructure systems relies, to a degree, on technological components that are commonly used in civilian technologies and applications, including off-the-shelf software. This is very cost effective but opens up the military infrastructures to some of the same vulnerabilities and attack techniques as the civilian space. A

[20] Symantec Internet Security Threat Report April 2011 http://www.symantec.com/threatreport/

number of incidents have recently been reported in the press, where there has been discussion of cases of cyber-attacks against UAVs and their supporting infrastructure.

17. An important aspect of today's online threat landscape observed by Symantec is the elevated value of information as a target for attack. Attacks on information are more difficult to detect and can be used to generate revenue for those stealing the information, or may enable them to gain a valuable political, economical, technological or military advantage. Given the focus on information-driven attacks it is important that all organisations are aware of where their critical information assets reside and have in place information management policies and procedures to ensure information is protected appropriately based on an assessment of the level of risk.

18. Attacks directed against government and critical infrastructures have fallen usually within two different categories. They are either targeted/tailored or massive. They aim either to collect confidential information or to attack and disable the infrastructure, rendering it unusable and inaccessible to its users.

19. Massive attacks usually take the form of denial of service attacks against the infrastructure. Denial of service attacks are easily discovered because their effects can be observed. They result in computers and networks not working because their processing capacity is exhausted by fake requests.

20. Usually these attacks use remotely controlled compromised computers. These are often used without the knowledge of the computer owner, who has been consumed into a bot network. These "botnets" are created by infecting computers belonging to both individuals and organisations with malicious code that remotely controls them and directs them to issue communication requests to the target that has been selected by those operating the botnet. In addition botnets are available "for hire" around the Internet, making attribution of the attack even more problematic, while providing "firepower" for hire to launch it.

21. Probably the most well-known case of large-scale denial of service attack against a country was the case of Estonia, where large-scale denial of service attacks took place that lasted for several weeks, and which used numerous botnets, significantly impacting the government and the critical information infrastructure.

22. The scenario of cyber-attacks preceding military operations as a first strike does not look very remote. The adversary may want to make use of an advantage gained in cyberspace to collect intelligence and disable infrastructure before or during a physical attack. In this way, the adversary achieves the desired effect of incapacitating enemy communications as well as the ability to deliver public messages and propaganda in an effort to "win hearts and minds". At the same time the adversary limits the amount of targets it needs to focus military efforts and the exposure of its armed forces to the defensive efforts of its opponent. It can also force the adversary to consume precious resources in bringing its communications back online. The denial of service attacks during the 2008 war in Georgia are a good example of how the ability to broadcast the Georgian side of the story was significantly restricted by a number of distributed denial of service attacks on the already limited Georgian infrastructure.

23. The execution of a targeted attack is done in a stealthy manner. The attacker aims to infiltrate the defences of the victim without detection, and then to collect information as well as elevate their privileges in the network to allow the attacker to move laterally through the network and establish a foothold, making it all the more difficult to remove if discovered. The purpose of a targeted attack can be either the collection of sensitive information or the alternation, suppression or destruction of sensitive information, or even that of the infrastructure on which the information resides. It could even go one step further and combine all these operational objectives. Depending upon the specific characteristics of the malware used, the term "advanced persistent threat" (or APT) is often used to describe some of these very advanced, highly stealthy and very difficult to remove types of malware.

24. The value of collecting intelligence about sensitive financial, technological, political or military information cannot be underestimated. A well-deployed attack can yield information that compromises communications and encryption ciphers. It can also give a clear insight on the motivation, plans, strengths and weaknesses of the victim. If, for example, the malware used has the ability to sabotage physical infrastructure (similar to Stuxnet) it can be used to inflict physical damage on an infrastructure that is supporting the military effort. In that case, the cyber-attack is used to project power and to demoralise the opponent if or when it becomes aware that critical systems are compromised. In addition in a crisis situation it calls into question the ability of a party that is successfully compromised to escalate the crisis to a next level: if there is no degree of certainty that the underlying infrastructure is able to support the effort, confidence is lost.

25. In 2010 Symantec also observed a number of key attack trends which included a rise in targeted attacks with incidents such as Hydraq and Stuxnet. The Stuxnet attack is a key example of how malware is being used to conduct traditional cyber crime, such as fraud or extortion, as well as to launch targeted cyber attacks on critical systems and networks such as, in the case of Stuxnet, those used by the energy sector.

26. The Stuxnet[21] attack targeted energy companies and represented an example of a malware threat that can be designed to gain access to and reprogramme industrial control systems. Stuxnet was able to steal confidential Supervisory Control and Data Acquisition (SCADA) design and usage documents for industrial systems such as those used by the energy sector. The way the attack was carried out indicates that the people

[21] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_stuxnet_dossier.pdf

needed to develop and execute such an attack were not amateurs. The use of zero-day vulnerabilities, root kits, stolen digital certificates, and in-depth knowledge of SCADA software are all high-quality attack assets and this usage points to an estimated group of up to ten people being involved in developing this specific, targeted and technically sophisticated cyber attack. In the past, this type of cyber attack focusing on such a critical national infrastructure was seen by many as theoretically a possibility, however it is fair to say that most would have dismissed such an attack as simply a movie-plot scenario. The Stuxnet incident has shown that such targeted, organised threats do exist where external actors, perhaps motivated by organised crime, terrorism or even hostile nations, are designing, developing and deploying malware in an attempt to gain control of industrial processes and then place that control in the wrong hands. The utilisation of Stuxnet as an attack tool has given food for thought to policy makers, not only because of the resources and skills needed to mount such an attack but also because it constitutes a decisive shift in the thinking and practical use of cyber techniques, beyond the collection of intelligence and information, into actually conducting sabotage.

27. In October 2011 a targeted threat was discovered that shared a great deal of the code in common with Stuxnet malware. The Duqu[22] threat was essentially a precursor to a future Stuxnet-like attack. Based on Symantec's analysis Duqu's purpose was to gather intelligence data and assets from entities, such as industrial control system manufacturers, which suggests that information was being sought to conduct a future attack against another third party such as a provider of a critical national infrastructure.

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.

28. Symantec welcomed publication of the UK's Cyber Security Strategy in November 2011 and the UK Government's considered response to the continuously evolving threat of cyber attacks. The strategy document lays the foundations for cyber security to remain a key public policy issue for the UK government and for required action to reinforce the defensive borders around our connected experiences.

29. In particular Symantec welcomed the strategy's acknowledgement of the scale of the problem facing the UK and the need for a National Cyber Security Programme that can coordinate existing and new activities across different government departments. The role given to the Ministry of Defence (MoD) in coordinating and integrating the civilian and military aspects of the capabilities involved in protecting national UK interests in cyberspace is seen as appropriate and relevant.

30. The allocation of the highest amount of the overall National Cyber Security Programme budget behind the Single Intelligence Account, to the MoD for mainstreaming cyber in defence, is a welcomed acknowledgment of the important role the MoD has to play in coordinating and bringing together cyber security focused activities across the armed forces. The acknowledgement in the strategy that this budget will be used to consider the need for investment in the network and equipment, to provide the UK's armed forces with the capabilities to address cyber threats as and when necessary, is also welcomed. Given the coordination role given to the MoD by the strategy, the establishment of the Joint Forces Command and the Defence Cyber Operations Groups are seen as key vehicles for ensuring the increased development, integration and harmonisation of the UK's defence cyber capabilities. The importance placed on the need to explore ways for the Ministry of Defence to strengthen engagement with industry partners is particularly welcomed as it ensures the emphasis placed on the important role of public-private partnership in addressing the cyber security challenges facing the UK is also recognised and acknowledged by the defence sector.

31. Coordination between the public and private sector on cyber related issues needs to occur at many different levels of the UK internet community, depending on the sector involved, the specific type of threat or the level of seriousness of the threat or risk. For example, internet service providers, security providers, law enforcement, security services and national critical infrastructure protection authorities may be the first port of call and clearly have a role to play in dealing with an incident. At the same time Symantec recognises that military organisations, such as the MoD, and NATO, will also become increasingly active in this area from the national security and national defence standpoint. This move is recognition of the fact that as soon as the threat becomes military in nature, there is a role for military involvement and appropriate response. However, industry will continue to play an important role in working alongside the defence sector, given that it is estimated that industry owns around 90% of the critical national infrastructure, and also taking into account the real time information, awareness and intelligence industry retains in relation to the current online threat environment.

32. Having the right information at the right time is, of course, key in identifying and addressing cyber threats. Symantec believes that information sharing is a fundamental component of a modern cyber security strategy and that the development of trusted information sharing networks and systems is a key element in the development of successful public and private cooperation. This is why the importance placed on the role of public-private partnership in addressing cyber security issues is so important and must continue to be a long term overarching public policy objective through the work of the National Cyber Security Programme and beyond to future strategies and initiatives in this area.

[22] http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/w32_duqu_the_precursor_to_the_next_stuxnet.pdf

33. The focus in the strategy document on the need for the MoD and GCHQ to work closely together in light of the responsibilities of these organisations is understandable given their remits and is seen as appropriate. Given the way in which the National Cyber Security Programme of work is outlined, engagement and coordination of actions between the MoD, National Security Council, Cabinet Office and GCHQ is necessary to achieve the overall objectives of the strategy. Symantec sees the Cabinet Office's Office of Cyber Security as playing a key coordinating role across all government activities in this area and already works well with key partners, such as the MoD and GCHQ, on aspects related to more operational responses needed to address cyber related issues.

34. In terms of determining a policy for the role of the MoD and the armed forces, there are a number of significant challenges that planners and policy makers would need to address. The development of doctrines, rules of engagement and the overall policy of how a military organisation needs to plan and act to handle cyber-attacks against its own infrastructure, as well as the nation, can be a daunting task. One of the biggest challenges in a crisis scenario, given the stealthy and asymmetric nature of cyber-attacks, would be to determine the moment a security incident becomes "military" in nature and justifies the involvement of the MoD.

35. 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?

36. 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?

37. 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?

38. 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.

39. 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.

40. Equally, in a discussion about proportionate response to an incident, one would need to try to determine what constitutes an "act of aggression" that would justify military action and what would be a proportionate military action against that aggression versus, for example, acts of espionage or acts of cybercrime that in themselves do not justify in international law the use of armed force.

41. Distinguishing between "acts of aggression" and espionage online is particularly difficult and complex because, as explained previously, very often the use of the malware as attack tools will combine capabilities that can be used for multiple purposes. In addition, even if it is possible to determine the motives of the attacker, the attribution of the attack to a particular country, with any degree of certainty, is a significant challenge. The decision to attribute a certain attack is a highly politicised decision that is dependent on the quality of intelligence that can be made available during the time the decision needs to be taken. An additional difficulty could also be linking attacking individuals to the particular government that called for the attack. Obviously the attacker will take steps to cover its tracks. Even in a case of attacks against a backdrop of mounting political tensions between two countries, one cannot exclude the possibility that the attack is mounted by a third country for its own purposes.

42. In a scenario of political tensions, the use of cyber as an escalation tool is another interesting aspect of the debate. What kind of cyber-attack indicates an intention to escalate? Are the cyber attacks happening because the adversary is trying to collect as much intelligence as possible or is it a definitive escalation indication? Is the use of cyber an indication that the other side is preparing for a kinetic conflict and cyber, in this case, serves as a preparatory step? If convinced that the other side will follow the escalation path leading eventually to conflict, should cyber be used as a first strike?

43. It is not surprising that the discussion of proportionate response and ultimately deterrence is riddled with similar challenges. What constitutes proportionate response to a cyber-attack that is primarily intelligence driven? Is it happening in the context of mounting tensions or while relations are good? Would a cyber-sabotage incident have a catastrophic impact significant enough to justify a kinetic counter-attack? Similarly how can you effectively deter when many countries will chose not to publicly disclose their capabilities?

44. It is evident that there are no easy answers to any of these questions and that these are points that strategy planners and policy makers will be struggling with for a while as technology develops. Some of the answers will be provided by the development of doctrine and capabilities and of technology. In other cases the answers will be given by the practical implementation of those doctrines into the field and the lessons learned in practice.

How the Ministry of Defence and the Armed Forces are managing and planning responses to threats in the cyber domain; including:
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.

45. From the perspective of the computer security industry, Symantec is supportive of the various activities and initiatives already in place and underway by the MoD and Armed Forces in these areas. For example the UK participation in cyber security related exercises, such as Cyber Storm with the US, are welcomed and supported by Symantec and should continue going forward so that the UK not only plays a leading role in international efforts in this arena, but also has the opportunity to plan and test its skills in dealing with cyber incidents.

46. Another example of activities in which Symantec has been involved are the UK part of the Coalition Warrior Interoperability Demonstration (CWID) in 2007 and 2008. This was one of the world's largest demonstrations of new military technology, and included cyber related capabilities.

47. While the UK must address its national response and management of cyber security incidents, it must not be forgotten that cyber threats are a global problem. It is also important to consider greater or strengthened international co-operation and collaboration between countries in planning for and managing cyber incidents that may impact more than one country. This planning should involve not only the action needed before an incident occurs but also the cooperation and collaboration that may be needed during and after a cyber incident. It is therefore suggested that the development of initiatives that can enable the sharing of technical expertise and guidance on how to address cyber security related incidents could be a way to strengthen or enhance national and international cooperation. The establishment of NATO Cooperative Cyber Defense Centre of Excellence in Tallinn, Estonia is an example of a project that has developed to foster greater understanding and sharing of expertise on how to plan for and react to cyber related incidents. Although cooperation at a European or international level is important, this should not be a substitute for countries taking a national approach appropriate to their level of maturity, identified risk and therefore specific requirements.

48. Moreover, it is suggested that the UK MoD could work closer with industry in order to identify promising security technologies and research that could be used in the military domain. The MoD could identify areas of research in cyber technologies that could receive national funding from UK R&D efforts. These technologies could then be piloted and evaluated by the MoD in its efforts to develop new and additional capabilities. In addition the MoD might consider joint activities with industry that could help to identify specific technical requirements and enable industry to demonstrate existing technological capabilities and solutions that could address those technical needs.

49. Such actions would bring the MoD closer to the technological community and would allow it to get a better understanding of the research developments in this cutting edge and highly technical area. It would also allow for better development of tools to meet the specific needs of the MoD, ultimately creating a virtuous economic circle of linking research and technological development with actual operational needs.

Issues That Merit Further Discussion/Consideration

50. When discussing cyber security and cyber defence and the current threat environment, one needs to bear in mind some of the following key factors, which may warrant further consideration by this Committee.

The threat is obviously external

51. While this may be the case, it should also be remembered that the threat is also very much internal. The internal aspects could include well-intended insiders, who did not mean to cause harm and could simply have lost information, as well as malicious insiders who deliberately attempted to steal information or disable the infrastructure. Any information security strategy needs to be able to monitor against both internal and external threats. This is the case for any organisation, but even more the case for the MoD, which should assume that it is the target of both technical and human intelligence efforts.

The threat is primarily asymmetric

52. This means that very significant damage can be done to valuable information or infrastructure despite considerable security investments. This could be the result of the use of means and methods that are disproportionately less resource-intensive in comparison to those used by the defendant. This very asymmetric nature of the threat can potentially lead into some very challenging threat scenarios in the future, especially when operations in a battlefield are becoming more and more unmanned. These types of technologies are easily and readily purchased, they can be procured not only by heavily funded organisations but also by groups or individuals with malicious intentions or who want to make names for themselves. At this stage cyber attacks aim to steal confidential information or disable a system by disrupting it or making it unavailable In the future it is not inconceivable that we will see attempts to take over a system and to use it against its owners.

The world we live in is increasingly interconnected

53. Information and communication technologies impact every facet of our daily life. In fact, the malfunction of those technologies could have unexpected consequences for systems that we consider safe or that we reserve exclusively for usage for our own defence. There have been reported cases of weapon systems, such as fighter planes and warships, being impacted by cyber attacks (which at the time were not targeted). We therefore need to be mindful that such technology has the potential to be used also for real military operational implementation. Given the interconnected nature of the world today, a morale element also plays a part in military operations and at times of national crisis. The enemy certainly has the ability to attack tactical communications, but there is another avenue that they can take as well. Critical infrastructure networks could also be vulnerable to these types of attacks. This premise leads back to the perception of power projection, showing the enemy that their own strategic assets are at risk, anywhere, anytime, affecting their lifeline without even a gunshot being fired. In many ways the ancient saying of Sun Tzu that "the great general wins battles without having to fight" comes closer to being true.

Need to look ahead

54. When discussing protection from any kind of threats, especially technological ones, it is necessary to bear in mind that the world is changing and so is technology. The strive for security is very much a moving target. The discussion about cyber defence and critical infrastructure is addressing some aspects of the current threat landscape but technological paradigms, as well as threats, evolve together. Virtualisation and cloud computing promise the next wave of technological evolution in the way we manage desktops as well as data centres. It is yet unclear how the business model of cloud computing will evolve or what the consequences of wide-spread deployment "to the cloud" will be. There are a number of ideas about the creation of multiple clouds, some dedicated to particular entities such as the government. Existing technological solutions suggest that the ability to detect targeted attacks, such as for phishing or malware, would be a lot more effective in the cloud than on the desktop level.

55. Delivering security over the cloud offers increased effectiveness because it is possible to identify more easily attacks and suspicious behaviour when data from multiple sources is aggregated together. It also has significant scaling advantages, as large cloud providers can invest in sophisticated monitoring and dedicated security personnel that are shared across a customer base where any single customer may not be able justify the cost. The same argument can also apply to making it easier for a cloud provider to invest in multiple data centres and connectivity to provide a level of redundancy. Finally, if an issue is detected in a cloud environment that affects one single customer, this issue can be fixed once and the protection is shared across the entire customer base. If a new threat against a single customer is identified, the protection put in place to mitigate against that threat is shared across all customers, so that they are protected even if they are not (yet) exposed to the new threat. In addition the existence of a cloud layer provides for an additional layer of defence and therefore increases the strategic depth of the defender and the layers of security that the attacker needs to successfully penetrate in order to have an impact.

27 February 2012

The Year in Numbers

Some of the more noteworthy statistics that represent the security landscape in 2010

286M+

Threats

Polymorphism and new delivery mechanisms such as Web-attack toolkits continued to drive up the number of malware variants in common circulation. In 2010, Symantec encountered more than 286 million unique variants of malware.

93%

Increase in Web Attacks

A growing proliferation of Web-attack toolkits drove a 93% increase in the volume of Web-based attacks in 2010 over the volume observed in 2009. Shortened URLs appear to be playing a role here too. During a three-month observation period in 2010, 65% of the malicious URLs observed on social networks were shortened URLs.

260,000

Identities Exposed per Breach

This was the average number of identities exposed in each of the data breaches caused by hacking throughout the year.

42%

More Mobile Vulnerabilities

In a sign that the mobile space is starting to garner more attention from both security researchers and cybercriminals, there was a sharp rise in the number of reported new mobile operating system vulnerabilities—up to 163 from 115 in 2009.

6,253

New Vulnerabilities

Symantec recorded more vulnerabilities in 2010 than in any previous year since starting this report. Furthermore, the new vendors affected by a vulnerability rose to 1,914, a 161% increase over the prior year.

14

New Zero-Day Vulnerabilities

The 14 zero-day vulnerabilities in 2010 were found in widely used applications such as Internet Explorer, Adobe Reader, and Adobe Flash Player. Industrial Control System software was also exploited. In a sign of its sophistication, Stuxnet alone used four different zero-days.

74%

Pharmaceutical Spam

Approximately three-quarters of all spam in 2010 was related to pharmaceutical products—a great deal of which was related to "Canadian Pharmacy" websites and related brands.

1M+

Bots

Rustock, the largest botnet observed in 2010, had well over 1 million bots under its control. Grum and Cutwail followed, each with many hundreds of thousands of bots.

$15

per 10,000 Bots

Symantec observed an underground economy advertisement in 2010 promoting 10,000 bots for $15. Bots are typically used for spam or rogueware campaigns, but are increasingly also used for Distributed Denial of Service

$0.07 to $100

per Credit Card

This was the range of prices seen advertised in the underground economy for each "stolen" credit card number, and, as in the real economy, bulk buying usually gets the buyer a significant discount.

Written evidence from the Institute for Security & Resilience Studies, UCL

This submission comes in two parts. The first addresses the current inquiry's three questions. The second takes up the invitation to flag issues for subsequent consideration by the Committee.

Key points offered in part one of the submission include:

- Threat analysis is a necessary but insufficient approach to assessing the risks and uncertainties of cyberspace for MoD and the Armed Forces or any other body.
- Following the 2011 UK Cyber Security Strategy there is work to be done to bring coherence to practical cyber-security arrangements across government (eg clarity about Lead Government Department responsibilities in a variety of cyber circumstances), which development of doctrine could deliver.
- The UK's Cyber Security Challenge makes clear that we have skills gaps and are failing to fill these through formal secondary or tertiary education. Rather than treating symptoms—however profitable—it is vital that continuous learning is enabled through R&D on broad and deep fronts to shape rather than just react to the evolving environment. Although MoD is among the very few bodies to have addressed such a challenge before, it is not clear they can take a similar lead in cyberspace.

Part two, goes onto flag the following four items for further consideration:

- The Net Assessment of Resilience and Irresilience to supplement threat analysis.
- The Capacity for Innovation as the decisive measure of cyber-resilience.
- The Organisational Fitness of Capabilities has to be grounded in learning competencies.
- Twining empiricism with entrepreneurship defines the leadership ethos fit for cyberspace.

ISRS will be happy to support the work of the Committee as best it can in the exploring issues, considerations and factors raised by part one and/or two of our submission.

1 Introduction

1.1 The Institute for Security & Resilience Studies (ISRS) at UCL offers innovative approaches to the challenges of security and resilience in our world of networks. We do this by bringing together the public, private and third sectors to seek out ways to catalyse innovation. For us, Resilience to Crises (R2C) combines two vital words into a powerful concept fit for our times. It is a concept born of pioneering cyberspace research for the defence community during the 1990s.

1.2 Use of the word resilience is evolving. It has moved beyond its classical origins and narrow engineering definition in terms of bounce back to the status quo ante. Our use of the word resilience and its inverse—*irresilience*—are grounded in scientific advances in the mathematics of networks and from across the life sciences. We define *resilience* as *the enduring power of a body or bodies for transformation, renewal and recovery through the flux of interactions and flow of events.* Resilience is the power to bounce forward and thrive, not an idealistic notion of bouncing back to a status quo ante overtaken by events.

1.3 We also adhere to the dictionary definition of crises as *decisive moments and turning points for better or worse*. This again affirms key advances in the mathematics of information and decision taking over the last century. R2C offers a concept that enables decision-takers at all levels to contend with the risks and uncertainties of dynamic networks. Doing so does not just raise awareness of dangers; it also offers options for coherent decisive actions, which produces rather than just protects value because it focuses on the continuous learning of fitness. In sum, resilience is synonymous with healthy competitiveness.

1.4 Our response to the Defence Committee's inquiry into cyber-security will come in two parts: the first will contribute to the committee's short initial enquiry; and, the second will flag issues for further consideration by the Committee in due course. Both parts offer responses based on three parameters of our current research programme:

- In general, we are examining how the prospects for cyber-resilience are affected by the depth and breadth of the Capacity for Innovation spurred by competition.
- In particular, we are concerned with organisation of evolving capabilities in competitive environments, in which the combination or recombination of capabilities using diversity and selection defines immediate and enduring fitness.
- In practice, we are emphasising the need for Competent Authorities that inspire trust because they embody an ethos that twins empiricism and entrepreneurship.

1.5 Leadership without enhanced empiricist and entrepreneurial characteristics will be found wanting in cyberspace. Such deficiencies are an issue for all big incumbent organisations whether in the public, private or third sectors.

2. Committee's Current Inquiry

2.1 The current inquiry poses three good questions, which will flout full and complete answers. Indeed, the pretence of definitive answers would suggest odds are being stacked for errors to ensue. The three questions are taken to ask for evidence on:

(a) The nature, character and extent of the threat posed to the systems of the Ministry of Defence (MoD) and the Armed Forces in terms of operations and capabilities.

(b) The implications of the UK's 2011 Cyber Security Strategy for MoD and the Armed Forces, in terms of policy, practice (including National Infrastructure Protection (CNIP)) and the relationship of MoD's actions and planning to other governmental bodies.

(c) How the MoD's cyber capacity building is planned and managed in terms of skills, expertise, research and development (R&D), again mindful of the interface with the National Cyber Security Programme (NCSP) run through Cabinet Office.

2.2 This submission will offer the imperfect views of ISRS on these questions, more in terms of the factors that need careful consideration than as definitive answers. Whilst it is important to distinguish what is peculiar to defence where possible, cyberspace tends to erode neat categories. Arbitrary constraints on the scope of the questions will be no more helpful.

Threat

2.3 The character and nature of the threat is the first question asked in orthodox security analysis. Such orthodoxy has been questioned for decades, particularly during the Cold War. The collection and collation of threat data is necessary but inadequate to the risk assessments needed to support decision-takers promoting fitness for any competitive environment. Cyberspace just makes that reality obvious. Although the first manufactured environment, cyberspace is transnational and permeates all other environments (maritime, land, air and space). It makes the dynamics of evolutionary forces impossible to ignore; ideal assumptions—such as perpetual status quo—do not endure. However, fixation on cacophony of tactical threats will draw the unwary into attrition and sap their resilience.

2.4 Detecting, profiling and patching software has become big business. The close battle of dealing with malicious code is reaching staggering proportions. Nonetheless, the streams of evolving threats cyberspace spawns are far from confined to malicious software. Mobile devices will soon attract the attention popular "fat client" computer networks have for over a decade. Smart metering based on mobile technology will create another link between Computer Information Systems (CIS) and Industrial Control Systems (ICS). "Thin client" devices dependent upon the Cloud are unlikely to design out the vulnerabilities that attract malicious code but will push most of the current limited capacity for computer forensics into obsolescence. Chasing these myriad threats with retrospective profiles may only increase a system or decision-taker's susceptibility to deception.

2.5 Beyond the close battle with malicious code and the protection of existing channels, comes the deeper and wider issue of content. It poses a challenge in at least two major guises:

— First, mindful of Clausewitz, the overriding friction in war is politics through which content can promote or subvert morale as the power of social software perhaps evidences in the Arab Spring.

— Second, content includes the intellectual capital that fuels innovation and shapes our futures; indeed, it is the capacity for innovation that is decisive in winning wars and peace.

2.6 MoD systems cannot be isolated from evolving global and local networks. These are increasingly woven together and populated by agents that never rest. Together they create the dynamics of the cyber environment. Here, the characteristics of the threat cannot be limited to consideration of electronic attack and the use of malicious code whether or not war is declared. Inasmuch as the intent component of a threat may remain an unfathomable mystery rather than an undisclosed secret, the absence of intent can still leave great hazards fermenting. If assumptions about intent are mishandled, the challenges for decision-takers only multiply—whether agents of a sovereign state or not.

2.7 Threat is an inadequate approach to the risk and uncertainty that saturates cyberspace. Confronting this reality can make the challenges ahead seem intractable. Yet it is realising the limits of a threat based approach that enables the assessment of risks and uncertainty to become pragmatic. Such pragmatism can be better informed by Net Assessment as is outlined in the second part of the submission "signposting further issues".

Coherence

2.8 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.

2.9 During the conference the answer for the UK was unclear. Subsequently it was said to be the Minister for the Cabinet Office—Frances 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 (LGD). For example, unless the Prime Minister is to be available for every cyber incident:

- It is difficult to believe that cyber crises abroad would not make the Foreign and Commonwealth Office (FCO) the LGD and put the Foreign Secretary in the chair; or
- Crises at home—whether security or crime related—would not make Home Office the LGD and put the Home Secretary in the chair; or
- Cyber crises in the financial sector would not make Her Majesty's Treasury (HMT) the obvious LGD and put the Chancellor in the chair.

2.10 As with any crises doubt about the competency to lead is a recipe for disaster, particularly in the golden minutes and hours at the onset of crises. The transnational nature of cyberspace is likely to place any cyber crises at the centre of UK Government in the first instance, even more so if events are to be construed as "armed attack". However, as Libya seemed to demonstrate, it is less how MoD works with the National Security Council (NSC) and more how the NSC works with legacy national crisis management arrangements through COBR that might benefit from clarification, particularly with regard to the LGD doctrine. Fast onset crises make getting the drills right important but slow onset crises can also deliver shock and surprise.

2.11 For example, the compromise of intellectual capital can do economic and strategic damage of unexpected proportions that stuns or lulls authorities into inaction akin to those in response to "white collar crime". Is the Business Innovation and Skills (BIS) department the LGD for cyber incidents involving content? The LGD question could create unnecessary duplication of capabilities among Government departments. In wealthier times CNIP could spur such expenditure and have it reach into local government too. This would not mean that private firms would match such capabilities as befits their CNI ownership. Amidst the tussles for lead roles and to avoid costly commitments many wrinkles remain to be smoothed out by clear doctrine in the wake of the 2011 Cyber Security Strategy.

Capacity building

2.12 Historically, MoD and the Armed Forces have provided resilience to what might be thought the moral hazard of Other Government Departments (OGDs). From Foot and Mouth Disease, to Fire Fighters Disputes and even the London Olympics, MoD has provided critical reinforcements. Whilst this has often been about reserves of disciplined labour with enormous stamina, there have also often been vital skills needed, in particular higher levels of tactical and operational command and control. It is not obvious how such capacity will be built for cyberspace. This is not an issue confined to MoD.

2.13 The UK's Cyber Security Challenge has produced an alarming pattern of evidence to suggest that the skills and expertise for cyber resilience and security are not being produced through formal secondary or tertiary education. Amateurs—ie those with a love of the challenges cyberspace throws up—emerge from self-education. Likewise, the bulk of R&D outside of particular areas of government tends to either address security as an afterthought or cherry picks what can be readily commoditised for profit. Over the last decade or so, policy decisions to rely increasingly on Commercial-Off-The-Shelf (COTS), deskilled software engineering and light-touch de facto standards have sown problems of growing consequence. For some, this recipe has produced profitable business streams. It has also led to recruitment and retention problems for core government business.

2.14 Merely treating symptoms rather than the causes of skills gaps and expertise deficits will compound problems. Building capacity has to embody processes of continuous learning, particularly if fitness for the dynamics of cyberspace is to endure. This makes R&D on broad and deep fronts imperative. MoD and the Armed Forces are among the few bodies in Government that have ever attained the kind of depth and breadth of learning necessary for such environments. Uniformed and MoD civil servants alike have continued to deliver similar services in hostile environments on scales seldom rivalled.

2.15 Nevertheless, it is not clear that MoD or the Armed Forces are in a position to reproduce such capacity for cyberspace, even if they have to become a major contributor. This is not necessarily a budgetary issue even in straightened times. It is more to do with the ethos that would need to be created, making a far greater virtue of empiricism and entrepreneurship than any large incumbent organisation has hitherto shown itself inclined. That ethos could not be exclusive to the defence sector but would have to be shared in by a diversity of public, private and third sector bodies. The National Cyber Security Programme in combination with MoD programmes (new and longstanding) will doubtless offer some steps forward but it is not clear that our fitness for cyberspace is yet adequate.

2. Signposting Further Issues

2.16 Four issues are flagged below that may be relevant to the Committee's subsequent deliberations.

The Net Assessment of Resilience and Irresilience

2.17 Resilience and irresilience have specific mathematical meaning in networks. In the financial sector these are now termed "superspreader" hubs. These do not just sow catastrophic collapse; they can also catalyse the

uptake of healthy transformation. The former is characteristic of irresilience; the latter is characteristic of resilience to crises. Both move beyond ideal assumptions about risk to harnessing the reality of uncertainty in evolving systems for better and worse.

2.18 The development of a Net Assessment for resilience and irresilience is more comprehensive, robust and realistic than over-reliance on error or deception prone threat analysis. It has a pedigree that stretches back to the Strategic Bombing Survey of WW II looking for industrial webs and bottlenecks and the "Breakdown" studies at the dawn of the Cold War but also harnesses the insights of the most advanced mathematics and modelling today. Development of such capabilities will enable defence and security to avoid wasting money and focus on how to add value by continuously learn fitness in cyberspace.

Capacity for innovation

2.19 Our work on cyberspace has concluded that the capacity for innovation is the decisive measure of fitness for the challenges ahead. Whilst Lord Dannatt (a former Chief of the General Staff) was right to celebrate the ingenuity of "transformation in contact", cyberspace will require transformation in far greater depth and breadth. We will be happy to detail how deep and broad transformation can be made tractable and rewarding.

Organisational fitness of capabilities

2.20 The term "equipment capabilities" may have done considerable disservice to the development of capabilities. We have reviewed leading academics in the field of capabilities and synthesised a fresh definition of capabilities and meta-capabilities:

— Capabilities are evolving ecologies of competencies and technology.

2.21 This definition underscores that returns on investments and productivity gains only come when innovation brings users and developers together with an equal concern for competencies and technology rather than just integrating the technology. Moreover, albeit training is important, the rapidity of change means that competencies are ultimately more about continuous learning, in particular drawing research beyond invention into innovation.

2.22 This approach enables greater agility in combining and recombining capabilities fit for diverse circumstances and opens up more feasible innovation pathways. These are all attributes that are vital to cyberspace, where disruptive innovation is every day.

Leadership: An ethos befitting competent authorities

2.23 Cyberspace demands a distinctive characteristic of leadership too often squeezed out of big organisations—entrepreneurship. Indeed, we go further and suggest that to continuously learn fitness for cyberspace empiricism and entrepreneurship have to be twined. This is how concurrent research, education and innovation deliver the competitive advantages fitness for cyberspace demands. Confidence in the competence of authorities that cannot deliver such outcomes will suffer sooner than incumbents too often imagine.

2.24 Finally, it is important to recall few people other than the armed forces are capable of operating in hostile environments for protracted periods enduring high degrees of uncertainty. Moreover, the ethical use of force is something with which they have grim experience. Cyberspace may involve indirect forces where that ethical knowledge is more not less pertinent than non-combatant colleagues may care to realise.

5. Conclusion

5.1 ISRS will be happy to support the work of the Committee as best it can in exploring the issues, considerations and factors raised by part one and/or two of our submission.

20 February 2012

Printed in the United Kingdom by The Stationery Office Limited
01/2013 023461 19585