House of Commons
Defence Committee


Sixth Special Report of Session 2012–13

Ordered by the House of Commons
to be printed 19 March 2013
The Defence Committee

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

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

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

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

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

Committee staff
The current staff of the Committee are Alda Barry (Clerk), Dougie Wands (Second Clerk), Karen Jackson (Audit Adviser), Ian Thomson (Inquiry Manager), Christine Randall (Senior Committee Assistant), Carolyn Bowes and Rowena Macdonald (Committee Assistants), and Sumati Sowamber (Committee Support Assistant).

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

The Defence Committee published its Sixth Report of Session 2012–13 on *Defence and Cyber-Security* on 9 January 2013 as HC 106. The Government’s response to this Report was received on 7 March 2013. This is appended.
Government Response

The Government welcomes the report of the House of Commons Defence Committee (HCDC) into the emerging threat of Cyber and the findings set out in the report of 9 January 2013.

The Government recognises the detailed work the Committee has put into formulating the report, especially in a technically complex and emerging area such as Cyber, and were grateful for the opportunity to brief the Committee in April and May. Our formal response to its conclusions and recommendations is set out below, and seeks to acknowledge or address each point in turn. For ease of reference, the Committee’s findings are highlighted in bold, with the paragraph reference given at the end, while the Government’s response is given in plain text.

The Inquiry was the second of the Committee’s “developing threats” series and focused on the nature and extent of the threat Cyber posed to the Ministry of Defence’s, and by extension the Armed Force’s, systems and operational capabilities. The Inquiry also looked at how the MoD was adapting to the emerging field of Cyber and how it was managing and planning to overcome the threats emanating from it.

The Government fully recognises the importance of Cyber to the UK, and as such is addressing the threats and opportunities on a pan-Government scale. The UK Cyber Security Strategy published in November 2011 provides the overarching framework. Underpinning this is the National Cyber Security Programme which puts in place £650 million of funding over four years to transform the UK’s cyber security capability of which the MoD’s Defence Cyber Security Programme is part. Cyber cannot be dealt with by one department or agency alone as each has its specific responsibilities and expertise. When discussing the threat from Cyber, the current role of the MoD is to protect its own systems and networks to ensure that our forces can continue to carry out their roles both at home and deployed. The protection of Critical National Infrastructure and provision of advice to the public and private corporations is a matter for Other Government Departments (OGDs) and Agencies.

During the preparation of this response, an error was spotted in the record of our evidence to the Committee on 16 May 2012. Having reviewed our briefing materials, video of the evidence session, and our own written records, it has become clear to us that an error has been made in the record of the evidence of the former Minister for the Armed Forces, Sir Nick Harvey MP. He said that the figure for funding of the DSTL Cyber and Influence Centre is £18M a year but this was incorrectly recorded as £80M.

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

Nick Harvey: The MoD works with others to promote and stimulate science and research and development. We are currently providing £80 million a year for research in the related areas of cyber and influence. For Defence, that is done through the Cyber and Influence Science and Technology Centre, which is part of the Porton Down Defence Science and Technology Laboratory.
The centre team up here work, as you have heard, with other Departments. We work with research councils to ensure that there is a co-ordinated programme of research here, and we invest, as John has told you, in pan-Government work. We are part and parcel of programmes that have placed work out in a number of universities. There is a lot of activity co-ordinated with other Departments—with the Cabinet Office and GCHQ—developing cyber-centres of excellence. Is there enough? Well, I don’t know. Is there ever enough? There is certainly a lot going on.

It is regrettable that this error has only come to light now, and not earlier, and we hope that this does not alter any of the Committees findings.

**Conclusions and Recommendations found in the Report**

1. There is a consensus that cyberspace is a complex and rapidly changing environment. (Paragraph 23)

The Government wholly agrees with this position, Cyberspace is a continually evolving environment and to defend against threats emanating from it we must keep pace with that change. We are determined that our cyber security posture will respond to these changing threats. Much progress has been made since the Committee took evidence.

**MoD Networks, Assets and Capabilities**

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

Our Armed Forces use some of the most sophisticated equipment in the world, designed and delivered to operate in the harshest conditions that our Service Personnel find themselves in. We therefore take the protection of our vital information systems extremely seriously, and in doing so plan for a wide range of attack scenarios and work closely with our partners to counter any threat to our military operations. It is true that Cyber is a fast paced, continually evolving environment, but we are aware of this and therefore understand that we must stay ahead.

The Department plans for and exercises a number of business continuity and contingency plans to ensure that we are able to continue to fulfil our role, should any number or combination of events occur. Certain areas within Defence, as with any other organisation, have been prioritised in case of an emergency. Given the all pervasive nature of Cyber, it is being integrated fully into our contingency operation planning process, as it is vital that any action we take is now Cyber aware, and that we now plan for any action taken by our adversaries in Cyberspace against us.
It would not be prudent to set out the specific details here of our planning or procedures in the event of a compromise or denial of these systems as they may assist hostile groups or states in their attack planning.

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

The Global Operations and Security Control Centre (GOSCC) is a key part of the mission to operate and defend, protecting our networks to ensure that the MoD and Armed Forces can continue to do its business securely. We welcome the Committee’s recognition and praise for the work of the GOSCC.

As the procurement process changes within the Defence Equipment and Support (DE&S) organisation, steps are being taken to ensure that Cyber issues are not forgotten and are part of the procurement steps put in place. The new Defence Material Strategy is currently being formulated and will set out clearly the future changes to the procurement process. The Department will keep Parliament informed in due course as the Strategy develops.

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

We are pleased that the Committee recognises the excellent work done by the GOSCC. It is rightly the centre of excellence within the MoD for the defence of our networks and securing our systems. The GOSCC has also done valuable work in giving briefing and visits to a range of OGD’s and Agencies as part of the wider Government effort, as well as briefings to Allies as part of our international engagement programme. The GOSCC has also been able to provide opportunities for UK media to visit their facility as part of media reporting on Cyber security.

For clarification, the GOSCC is one of the components of the Defence Cyber Operations Group (DCOG), a federation of Cyber entities across the Department pulling together to mainstream Cyber within Defence.

We have identified that good Cyber hygiene is a core part of defending our networks, with the potential that a large volume of the threat posed from Cyber can be eliminated by good practice. Within the Defence Cyber Security Programme, a skills and training team has been established to look at how best to educate our personnel at all levels in
this good Cyber Hygiene, and we have already instituted a mandatory Cyber awareness course for all staff.

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

We are not complacent on this issue and we are fully committed to improving cyber security within our supply chain. We have been reviewing our approach to the defence industrial base, with particular regard to information sharing, information assurance and incident reporting. This work has been done in consultation with the Cabinet Office, BIS and OGDs to ensure a consistent and coherent approach.

In particular, we have been working with our defence industrial base and we have already gained strong support from many of our key suppliers to develop jointly a measurement and assessment framework for cyber standards and a compliance mechanism by which it will be embedded across the supply chain. We will be working with industry to ensure that those involved in this procurement chain, both inside MoD and industry have the right skills and training to tackle this threat. The desired outcome is to reduce the risk posed to Defence and to have an effective model to protect critical defence information by helping industry to protect themselves. This will also have the added benefit of demonstrating that the UK defence sector is the exemplar on cyber security.

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

The Government fully supports this conclusion of the Committee, and welcomes their support in our endeavours. The MoD currently has a tri-lateral Memorandum Of Understanding in place with both the USA and Australia to work collaboratively on Cyber, drawing from each others specific experiences and allowing each nation to draw on best practices. This is vital to develop now so that Cyber can become part of the mainstream of future allied operations.

7. Good cyber-security practice needs to permeate the whole of the MoD and the Armed Forces. It would be a cause for concern if different units were to compete for particular roles and resources, if lines of accountability were to be unclear, if they were to operate in silos that would obstruct the best use of skills across the organisation, or if policy were to become fragmented. (Paragraph 56)
The Government recognises the concerns of the Committee, and wishes to reassure that Cyber is a joint field issue across the entirety of Defence.

Commander Joint Forces Command has been appointed the Defence Authority for Cyber. In practice this means that a clear line of accountability has been put in place for Cyber at a senior level to prevent Cyber being organised as a specialist silo, or separate entity and instead to ensure that Cyber is recognised as a whole of Defence issue that must be integrated within all areas of planning, preparation and budgeting. At the core of this is a new direction from the Chief of Defence Staff on Cyber which pulls together all the operational command of Cyber units under Joint Forces Command to ensure a consistent and holistic approach to Cyber in operations and Defence business. This includes a number of DCSP projects looking to ensure that we can grow and recruit the right skills, as well as offer the right incentives to retain them.

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

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

The Government recognises that at the time of giving evidence, the normal clear lines of command and control may not have been as clear as with other well established units within Defence.

The MoD has appointed Commander JFC the Defence Authority for Cyber, recognising that Cyber is by its very nature a joint endeavour and requires senior responsibility and accountability to be put in place. This will soon be supported by a Chief of the Defence Staff Directive on Cyber. This directive empowers Commander JFC to develop and maintain the department’s Cyber capability, as well as plan and prepare for all Cyber operations. On a day to day basis this authority is delegated to Chief of Defence Intelligence (CDI).

CDI has appointed Air Vice Marshal Rigby, who gave evidence to this Inquiry, as the Senior Responsible Owner (SRO) of the Defence Cyber Security Programme (DCSP). As SRO, AVM Rigby is responsible for ensuring the success of the programme in its stated aims and objectives. One of the initial aims of the DCSP was the formation of a Defence Cyber Operations Group (DCOG) a federation of cyber units across defence – working closely together to deliver a defence capability. The GOSCC (while being under
the command of ISS) is a member component of the Defence Cyber Operations Group (DCOG).

It is the intent of Commander JFC to set up a Joint Forces Cyber Group (JFCyG) to oversee operation Cyber functions of the Joint Cyber Units, Joint Information Assurance Units and the Cyber Reserve. It is our belief that this line of Command and Control gives us the necessary chain of command, while retaining the flexibility and agility required to deal with the threats and opportunities emanating from Cyber.

For clarity, Cyber Policy is currently accountable to Director General Security Policy, via Assistant Chief of the Defence Staff for Military Operations and Strategy.

The recent agreement of the Defence Board to establish a 3* Defence Chief Information Officer (CIO) will strengthen and centralise the Department’s leadership and accountability for information systems in both the military and business environments.

The Information Operating Model (IOM), which remains on track to be implemented in April, will facilitate progress in the management and delivery of ICT. It will provide a strengthened alliance between a significantly more empowered 2* Chief Information Officer (CIO), the creation of a new 1* Chief Technology Officer (CTO) and the Joint Force Command (JFC) in the role as Defence Authority for C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance) and Cyber.

Military Activity in Cyberspace—Conceptual Framework

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

The Government agree that there needs to be clear doctrinal and policy support for Cyber, but is far from complacent on this issue.

The MoD has drawn up doctrine on Cyber, but this is sensitive information and for reasons of national security will not be expanded on further here.

What actions require, or might require, a military response is not in strict terms set out as any response will be based on the context of the action and may require information about attribution or actions taken by others. This approach allows the UK Government to retain a flexibility of approach and not lead the UK into a fatalistic set of actions should certain events arise, and instead retain the ability to use whatever means, be they diplomatic or military, thought best for the situation. Cyber actions are unlikely to
happen in isolation, something we are keenly aware of and are factoring into our contingency planning requirements.

Any military response is governed by the Law of Armed Conflict (LOAC). If the UK is responding to an imminent or actual cyber attack the response is governed by the legal principles of necessity, proportionality and imminence where anticipatory self-defence is concerned. The test, including the evidential base of what would be considered an imminent attack, is high. The cyber implication of the law of self-defence turns on three practical issues: firstly, attribution; secondly, the speed with which an attack can be conducted, which greatly reduces the ability to respond to an imminent attack; thirdly, the difficulty of determining intent, even if actions are provable and actors identifiable.

11. We recommend that the Government ensure that civil contingency plans identify the military resources that could be drawn upon in the event of a large-scale cyber attack, such as additional staff, planning resources or technical expertise. In its response to this report the Government should set out what work it is doing to identify the reliance of the Armed Forces on the integrity and resilience of the Critical National Infrastructure, the steps it has taken to ensure that the CNI will remain sufficiently robust to meet the needs of the Armed Forces and its contingency plans for the event that any relevant part of the CNI should fail. (Paragraph 69)

As with other UK incidents involving the Critical National Infrastructure, the MoD is not currently the lead department. However the MoD will, when requested, supply resources under the mechanism of Military Support to the Civil Powers. We work closely across Government, via the National Security Council to identify threats to National Security and work to mitigate and prepare for them as required.

The MoD has robust plans in place to deal with our dependencies on the Critical National Infrastructure, including business continuity and emergency plans.

Relationships with Allies

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

The Government thanks the Committee for its recognition of the UK’s planned participation in the NATO Co-Operative Cyber Defence Centre of Excellence (CCD COE), and thanks them for their understanding that policy regarding our position was in development at the time of the Inquiry.

The MoD is now in the right position to provide a national representative at the Centre, starting in 2013, for an initial two year commitment. The liability for a Civilian post has been identified from within the existing DCSP programme, which will also fund the annual €20k subscription. Long term, MoD will have to make a decision on the ongoing funding of the post as the DCSP ends.
Resources and Skills Supporting Military Activity in Cyberspace

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

The 2011 UK Cyber Security Strategy highlighted that the Government is working to improve the resilience of its own critical data and ensure that its systems are secure, in particular the standard of Cyber security we expect in defence, and hence for suppliers of sensitive defence equipment.

Specifically, the MoD is working with OGDs to raise awareness of the threats from Cyber to help companies protect Government information, maintaining national security as well as protecting their own intellectual property, and to develop standards and guidance that can be readily used and understood. Defence companies are participating in the Cyber Information Sharing Partnership that the Government has established to share information on threats and pool situational awareness.

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

The Government recognises the great challenge that it faces recruiting and retaining skilled staff when competing with private industry and this is nothing new to the public sector. A great deal of work is ongoing within the MoD directed towards Cyber training and development. The new Cyber Skills Strategy for the MoD sets the vision and strategic policy for generating and sustaining Cyber skills. We have designed a new MoD Cyber competence framework, which is aligned with both the GCHQ competence framework and with civilian industry frameworks. Detailed training needs analyses have been produced for both wider Defence and for the Cyber specialist community.

To ensure that we have the right people and skills to undertake this work, we will grow a cadre of dedicated Cyber experts to support our own and allied Cyber operations and secure our vital networks. This will be done by bringing together existing expertise from across Defence, including the Armed Forces (both regular and reserves), and our Cyber and Influence Science & Technology Centre (our focus for Research & Development on Cyber matters).

15. MoD thinking about how reservists will help to deliver cyber-security is evolving, with many issues to be resolved. Although we welcome the initial steps taken by the MoD to develop the Joint Cyber Reserve it is regrettable that information about its establishment was not shared with us during our evidence taking. As a consequence, we were unable to explore with Ministers the details of this important development. (Paragraph 93)
16. We recommend that the MoD should build on existing strengths in the ways reservists contribute to cyber-defence and operations, and to retain the particular reserve-led command structures that facilitate those contributions. If any new reserve structure is to succeed, it is important that reservists who work in the civilian world should play a part in its design. The close relationships that have been established with contractors at the GOSCC could provide an avenue for recruiting more reservists from those companies, and we recommend that the MoD prioritise, as part of Future Reserves 2020, a strategy for recruiting personnel with specialist skills from the private sector. (Paragraph 94)

The Government acknowledges the Committee’s concerns that they were not able to cross-examine Ministers. However, as we explained at the time of the Inquiry, work on the Joint Cyber Reserve was developing in parallel and the final structure was not clear. We will of course keep Parliament informed of progress in this key area.

In the MoD have been developing the formation of a number of reserve elements to assist with our Cyber mission, by building upon the success of the current single Service and Joint Forces capabilities. The Cyber Reserve will provide support to the Joint Cyber Unit (Corsham) (JCU(Cor)), the Joint Cyber Unit (Cheltenham) (JCU(CH)) and tri-service Regular Information Assurance units.

It would be premature to announce criteria for selection or recruitment into the Joint Cyber Reserves at this time, but we will keep Parliament, and the public informed.

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

The protection of MoD’s key networks and systems remains a departmental commitment, with the funding for this allocated from the Defence budget. At present, a number of options are under consideration within the Annual Budgeting Cycle for further investment in Cyber defence. The resources allocated from the NCSP continue to be used by the Defence Cyber Security Programme (DCSP) to fund a broad transformation programme aimed at changing how the MoD approaches Cyber operations. On current plans this will end in 2015, and at that time the Defence budget will have to examine its priorities.

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

We welcome the Committee’s acknowledgment of the difficulty of this task, and can reassure the Committee that work is ongoing in this regard. However, there are no agreed or internationally recognised acceptable performance thresholds for measuring Cyber defence activity. It is reasonable to articulate incidents which have occurred and detail adversary activities mitigated at the gateways into our networks. However this will not present the picture that the Committee were hoping to see. Work on this area will continue and we will keep Parliament informed.

**Cyber-Security across Government**

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

The Government strongly agrees that cyber security is vital and urgent, which was why cyber was rated a Tier 1 threat to the UK’s security in the 2010 National Security Strategy. The National Security Council discusses cyber security as required and takes advice and evidence from many sources as expected. All relevant Ministers are in attendance as necessary.

In addition to these NSC meetings, the Foreign Secretary chairs a dedicated Ministerial group on cyber issues.

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

The Government agrees that the NCSP requires robust governance, and the Minister for the Cabinet Office plays an important role. The National Cyber Security Strategy provides the overarching strategic framework for all government activity on Cyber security. The Government is confident it has the authoritative leadership in place to drive delivery. Francis Maude has oversight of the Cyber programme with Chloe Smith to support him. Working to this clear overall plan, a number of Ministers are fully engaged on Cyber security in their policy areas to achieve maximum awareness and reach to a wide range of sectors.

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

The Government takes the need to be ready and prepared to respond to a cyber incident extremely seriously. The Government already has a clear set of National Incident Management procedures which have been drawn up with stakeholders and which are regularly exercised, including with Ministerial participation. Building on lessons learned and processes developed for, and tested at, the Olympics we have updated this policy, part of which will include the establishment of a UK National CERT (Computer Emergency Response Team). This will strengthen and protect the UK from cyber attack, improving our ability to respond to cyber attacks on both public- and privately-owned critical national infrastructure.

Conclusion

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

The Government notes this recommendation. The National Security Council and Defence Board keep Cyber security under review, including the potential role of the military in our national Cyber strategy. At present the MoD does not have a Cyber role in the protection of Critical National Infrastructure or civil society with regard to Cyber; those tasks are taken on by Other Government Departments and Agencies.

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

The Government’s 2010 National Security Strategy identified Cyber attacks on the UK as a “Tier 1” threat—one of our highest priorities for action.

Within the Ministry of Defence (MoD) there are technical, organisational, procedural and physical measures in place to protect against and mitigate the impact of Cyber attacks. We have refrained from public comment on the specific detail of cyber security incidents or threat assessments as this information could be useful to potential adversaries.
At a national level, the National Cyber Security Strategy sets out key objectives to meet the concerns of the Committee, with work being undertaken by a number of Other Government Departments, and co-ordinated by the Office of Cyber Security and Information Assurance within the Cabinet Office to ensure a truly joint approach and that the emerging threats identified can be met. On current plans, the programme runs until March 2015.