House of Commons

Defence Committee

Developing Threats: Electro–Magnetic Pulses (EMP): Government Response to the Committee's Tenth Report of Session 2010–12

Twelfth Special Report of Session 2010–12

Ordered by the House of Commons
to be printed 25 April 2012

HC 1925
Published on 30 April 2012
by authority of the House of Commons
London: The Stationery Office Limited
£0.00

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*)
John Glen MP *(Conservative, Salisbury)*
Mr Dai Havard MP *(Labour, Merthyr Tydfil and Rhymney)*
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)*

The following were also Members of the Committee during the Parliament:
Mr David Hamilton MP *(Labour, Midlothian)*
Mr Mike Hancock MP *(Liberal Democrat, Portsmouth South)*
Mr Adam Holloway MP *(Conservative, Gravesham)*
Alison Seabeck MP *(Labour, Moor View)*
John Woodcock MP *(Lab/Co-op, Barrow and Furness)*

Powers

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

Publications

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

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

Committee staff

The current staff of the Committee are Alda Barry (Clerk), Judith Boyce (Second Clerk), Karen Jackson (Audit Adviser), Ian Thomson (Inquiry Manager), Christine Randall (Senior Committee Assistant), Miguel Boo Fraga (Committee Assistant), Sumati Sowamber (Committee Support Assistant) and Frances Haycock (Sandwich Student).

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.

Twelfth Special Report

The Defence Committee published its Tenth Report of Session 2010–12 on *Developing Threats: Electro–Magnetic Pulses (EMP)* on 22 February 2012, as House of Commons Paper HC 1552. The Government's response to this Report was received on 25 April 2012. This is appended.

Government response

The Government's formal response to the HCDC's recommendations and conclusions are set out below, and has been prepared by the MoD in consultation with the Cabinet Office, DECC, and the Government Office for Science. Where appropriate, related recommendations have been grouped together and we have responded with a single narrative. The HCDC's findings are highlighted in bold, with the Government response in plain text. For ease of reference, paragraph numbering follows that in the "Conclusions and Recommendations" section of the HCDC's report.

The Government welcomes the HCDC's work in this area, and has considered its conclusions and recommendations carefully. We would like to emphasise that we take these threats seriously, and are already addressing them appropriately and proportionately across Government departments. We would also draw the Committee's attention to the National Space Security Policy being developed by the Cabinet Office, which will coherently address all aspects of the UK's space security interests and will be published later this year.

Nature of the threat

1. The risks posed by space weather are known and significant, though there is argument about the likely extent of their impact: a severe event could potentially have serious impacts upon UK infrastructure and society more widely. It is essential that this hazard is sufficiently recognised and addressed by the Government and relevant civil bodies. (Paragraph 28)

2. We recommend that work proceed as a matter of urgency to identify how seriously a future Carrington event would affect the UK infrastructure. It is clear that more modelling is required to establish the likely effect of a major space weather event on the National Grid. This should be independently validated and compared with the results of observations of Grid behaviour during space weather events. (Paragraph 29)

The risk of severe space weather is fully recognised by the Government. It has published its initial assessment of the likelihood and likely impact of a Carrington-magnitude event in the National Risk Register of civil emergencies.[1] Government departments have worked extensively with space weather scientists and engineers, industry, private sector asset owners and regulators to gain the best available quantitative assessment of the risk to UK infrastructure.

Depending on the magnitude of the event, the current assessment is that severe space weather would be expected to have moderate to significant effects upon a range of technologies and infrastructure, including communications systems, electronic circuits and power grids. In some sectors the extent and nature of the impacts are not yet clear,

1 www.cabinetoffice.gov.uk/resource-library/national-risk-register

but further analysis is in hand to enable infrastructure owners and operators to plan their response to future events and capability improvements.

In the energy sector, the Government is working closely with industry through the Energy Emergencies Executive Committee (E3C) to clarify the potential impacts of severe space weather on electricity assets and networks and this will inform contingency planning and mitigation that is appropriate and proportionate. The E3C has representation from industry, trade associations, Ofgem, the Health and Safety Executive (HSE), consumer groups and government. The Government believes that the effects of severe space weather events are more fully understood by extending and continuously improving on models developed through this forum.

3. On the basis of the evidence received, it seems likely that at present only those states with a known nuclear capability would be able to utilise a High Altitude Electromagnetic Pulse (HEMP) weapon. However, certain states such as Iran could potentially pose a realistic threat in the future, even if it does not currently do so, if nuclear non-proliferation efforts are not successful. Non-state actors could also pose a threat. While the risk may at present be low, the potential impact of such a weapon could be devastating and long-lasting for UK infrastructure. The Government cannot therefore be complacent about this threat and must keep its assessment of the risk under review. It is therefore vitally important that the work of hardening UK infrastructure is begun now and carried out as a matter of urgency. (Paragraph 42)

The Government keeps this risk under constant review. In the 2010 National Security Strategy, the risk of an attack on the UK or its Overseas Territories by another state or proxy using nuclear weapons was judged to be a second tier priority risk to national security. This reflects an assessment that this risk, though entailing very serious consequences if it were to materialise, has a low likelihood of being realised in the 5 to 20 year timeframe. The National Security Risk Assessment, which assesses these and other risks in support of the National Security Strategy, will be the means of providing strategic notice about future threats, enabling mitigation responses and capabilities to be planned in advance. The NSRA will be updated every two years and the next update, due during the course of this year, will update the assessment of the risk of nuclear attack on the UK.

Action to prevent hostile threats, such as high altitude nuclear explosions and use of non-nuclear Electronic Magnetic Pulses (EMP) devices, is implemented through a number of coordinated activities principally aimed at preventing the causes of EMP, and not EMP itself. These include cross-Government work on Counter Proliferation, which is led by the Foreign Secretary, and the nuclear deterrent, which is led by the Defence Secretary. The last National Security Risk Assessment suggested that the combination of likelihood and impact of the risks specific to EMP did not justify separate, duplicative governance mechanisms. Instead, the range of threats of which EMP is either a by-product or the principal element are managed coherently by the National Security Council, chaired by the Prime Minister.

The Government already takes significant action to prevent a state nuclear attack, including the maintenance of the nuclear deterrent and actions with international partners to control the spread of advanced technology and the development of nuclear weapons. The Government's approach to mitigating these, and other priority risks to national security, was set out in the National Security Strategy and the Strategic Defence and Security Review. Reinforcing the security and resilience of the national infrastructure most critical to keeping the country running forms part of this strategy; the Government is acting to enhance cooperation between public sector bodies and private sector providers of national infrastructure to improve their resilience to a wide range of hazards and threats. The Government is sharing its assessments of the risks of disruption to infrastructure operations arising from space weather effects, in order to inform priorities for investment in resilience to these and other threats and hazards.

As regards the risks posed by EMP and space weather effects on the energy infrastructure sector, priority is being given to work on space weather impacts and mitigations on electricity networks. National Grid and DECC are building on the work of the Space Environment Impacts Evaluation Group and E3C to analyse the range of impacts of extreme space weather events, with the Carrington Event being adopted as the reasonable worst case. These scientific assessments have enabled National Grid to change the design requirements for its Supergrid transformers, and to increase its reserve holding of transformers. National Grid is currently developing improved monitoring tools with the British Geological Survey (BGS) and installing or reinstalling Geomagnetically Induced Currents (GIC) monitoring devices into its Strategic Asset Management program. The next steps will be for National Grid, in association with BGS and working with E3C, to develop more detailed modelling of severe space weather events including impacts on generator transformers. This will extend and strengthen its analysis on the electricity transmission system completed so far.

As stated previously in the Government's evidence, Defence standards direct that military equipment must have an appropriate hardening against nuclear weapon effects, including EMP. This hardening provides a level of protection against space weather effects. Critical military infrastructure is designed to operate independently of nationally-provided utilities, with many facilities having back-up power generators and bulk fuel reserves.

All beyond-line-of-sight communications for the MoD are provided through a Private Finance Initiative (PFI) with Paradigm Secure Communications Ltd. Under the terms of the PFI, the military is afforded access to assured and protected communications; these are derived principally from the Skynet 5 satellite constellation (and its ground infrastructure), which is hardened to withstand a reasonable worst case space weather event and a high altitude electromagnetic pulse from a nuclear weapon. The PFI also accounts for the provision of commercial SATCOM for military purposes. While commercial satellites are designed to withstand routine space weather effects, they would be more susceptible to severe space weather than their military-grade equivalents,

and their ground stations would be less resilient to artificially-generated EMP effects and GIC caused by space weather.

4. While existing non-nuclear EMP devices may be crude and limited, the fact that viable devices could be produced by non-state actors is a cause for concern. Even localised damage could have the potential to disrupt activity, especially if combined with other forms of attack. (Paragraph 47)

The Government is keeping the risk of acquisition or use of non-nuclear EMP by State or non-state actors under review in the National Risk Assessment. As stated previously in our evidence, state development of non-nuclear EMP devices tends to require advanced engineering, although cruder devices with limited ranges of effects could be acquired or produced by non-state actors and maybe combined with other technologies. Indeed, there is evidence of the proliferation of the technology, which may have already led to its acquisition by countries and/or non-state actors of concern to the UK; for example, some open source information is available on the internet. While the Government monitors and assesses whether this open source information could be used to create a viable non-nuclear EMP device, this assessment is not disclosed in order to limit the opportunity for proliferation of this technology.

Resilience

5. We are pleased to note the recent intensification of efforts to forecast space weather. Its effects will not respect national boundaries, and it is important that the UK continues to contribute effectively to international efforts to improve forecasting. (Paragraph 55)

6. The Government must ensure that sufficient funding and resources are available and that the UK has sufficient access to up-to-date monitoring information. Monitoring space weather is a vital tool, both in terms of providing warning periods for potentially large space weather events, and in terms of understanding the risks more fully. (Paragraph 56)

The Government welcomes the Committee's acknowledgement of the progress being made in space weather forecasting. A new European Union project to forecast space weather began in 2011 and will run until 2014. Led by researchers at British Antarctic Survey (BAS), the €2.54m SPACECAST project will provide web-based forecasts so that satellite operators can take action to protect their satellites from space radiation damage. The UK is currently also involved in the European Risks from GIC (EURISGIC) Project (through the British Geological Survey) on the threat posed by magnetic storms to power distribution networks in Europe.

The signing of a Memorandum of Understanding between the Met Office and National Oceanic and Atmospheric Administration (NOAA) in February 2011 has paved the way for enhanced co-operation and collaboration between a range of UK and US agencies and organisations in the delivery of Space Weather alerts—which is now a tried and

tested system. The two governments have announced that they will create a combined space weather model capable of forecasting terrestrial weather and also indicating where, when, and for how long space weather effects will persist. As a result the UK is well-placed to take a significant step in accelerating the pace of advances in space weather forecasting ability.

The Met Office involvement in this work offers a means to exploit its 24/7 operational expertise to channel the UK expertise into forecast services. It also provides a route through to the efforts being made by the World Meteorological Organisation in space weather.

We agree that it is important that the UK has sufficient access to up-to-date monitoring information, both to inform any response to a significant space weather event, and to support routine business continuity. We are currently exploring funding streams and models by which any operational capability would work.

In general, space weather data is shared internationally on an academic free exchange basis, so access to up-to-the-minute monitoring information is good. This extends from space based observations made by, for example, the ACE spacecraft to data from the ground magnetic observatories participating in the INTERMAGNET programme.

7. It is clear from the evidence we received that there are both risks and benefits associated with hardening equipment. Nor is the cost clear. We recommend that the Government and National Grid work together to assess the cost and effectiveness of available technologies and if necessary coordinate further research into this area to establish whether retrospective hardening of equipment is appropriate, given the assessed level of risk to infrastructure from space weather and EMP disturbance. We would expect any such retrospective hardening to be carried out during routine maintenance of equipment in order to minimise the cost. (Paragraph 64)

As the Committee rightly states, there are both risks and benefits associated with hardening equipment. The costs are unpredictable but would be considerable; hardening is only one of many mitigations available when planning for the variety of circumstances we must address. It would not be cost-effective to harden civilian infrastructure unnecessarily. In some larger and diffuse structures, hardening one part of a system may simply transfer the vulnerability to another area. The effects of space weather, HEMP, and non-nuclear EMP can vary widely, as the differing causes produce different results. Hardening should be undertaken in a way that is cost-effective and appropriate to both the infrastructure and the risk in question.

The risks and benefits associated with hardening equipment are taken fully into account in the work DECC is carrying out with National Grid, and others in the energy sector, to clarify the potential impacts of severe space weather on electricity assets and networks. As a matter of course, this work already embraces the need to consider mitigation measures from both an operational procedure perspective and from an asset hardening

perspective. Work is currently underway to develop a detailed analysis of a severe space weather event to include generator transformers as well as transmission assets. The findings of this work will help to determine the need for installing and/or retrofitting asset hardening technologies, and the extent of further research in this regard, given the interconnectedness of the electricity networks and the many configurations they are able to offer.

8. The potential effects of a Carrington size space weather event or a high-altitude nuclear EMP weapon would have specific and potentially devastating impacts upon the electrical grid and other aspects of electronic infrastructure, which play an absolutely critical role in UK society. It is therefore vital that the UK electrical grid is as resilient as possible to potential threats such as these. The various Government departments involved must work with National Grid to ensure that its backup procedures and equipment are sufficient to meet the reasonable worst-case scenario for a severe space weather event. Consideration should further be given to the practicability and cost of establishing resilience against the event of a wide-spread loss of transformers, such as could be created by a HEMP weapon. This might be also an area in which other relevant Committees of this House might like to look at in greater detail in the course of their work. (Paragraph 65)

Given our assessment of the respective risks of HEMP and extreme space weather, we have chosen to prioritise planning and capabilities to mitigate the effects of extreme space weather, while focussing EMP protection on our critical military and national strategic command structures.

Resilience to the effects of extreme space weather is being improved in the energy sector through the work DECC is carrying out with National Grid and others. If, despite this, there were to be a major electricity supply emergency, both industry and government would have significant roles to play. So the E3C, which brings together network operators and public sector bodies, reviews and takes action to improve emergency preparedness and response across the electricity and gas sectors. E3C maintains and updates contingency plans for managing energy emergencies including the Downstream Gas and Electricity National Emergency Plan, Electricity Supply Emergency Code and the Fuel Security Code. These describe the steps industry and government might take to deal with an electricity supply emergency, and the emergency powers afforded to the Secretary of State under the Electricity Act 1989; these include implementing rota disconnections and prioritising supplies to essential users such as hospitals and transport infrastructure.

Defence may contribute appropriate military aid to the civil authorities under the Civil Contingencies Act 2004 (CCA) in order to augment the civil response in the event of a large-scale incident. An EMP event might constitute such an incident. General duties support by the military to the emergency services to help deal with the knock-on effects of an EMP event can be requested by any government department.

9. Although our Report concentrates on the military aspects of these threats, we hope that the evidence we have taken will also inform and influence discussions between governments and throughout industry. Such discussions are needed urgently, to consider the development of agreed standards for protection and resilience across all infrastructure and supply industries, and to explore the possible need for legislation to ensure that these standards are adopted. (Paragraph 66)

The Government agrees with the Committee on the ongoing need to co-operate between governments and throughout industry, and welcomes the body of evidence produced by this Inquiry. The Government is strengthening bilateral cooperation with the United States on approaches to the most serious resilience risks, including through shared assessments and, where appropriate, joint programmes. Similarly, the Government will work to ensure that European Union civil protection arrangements focus on shared risk assessment and prevention, and mutual awareness of critical infrastructure dependencies. The Government holds regular discussions with allies to consider security, protection and resilience issues.

The Government will work with owners and operators of national infrastructure, mainly in the private sector, to improve the security and resilience of infrastructure that is most critical to the running of the country to a full range of risks and hazards. The most effective approach to improving resilience of national infrastructure and supply systems is to share assessments of the risks rather than to impose new standards. Recent work undertaken by the Cabinet Office to develop a cross-government policy on infrastructure resilience concluded that the setting of standards across the national infrastructure to specific risks was disproportionate, given the diverse nature and varied importance of individual assets. Instead, the policy encourages industry and regulators to use the risk information provided by government to build resilience on an 'all risks' basis, using a combination of both 'hard' protection and emergency preparedness. Nonetheless, the policy recognises that where a particular industry faces a significant specific risk, site assessments of the most critical elements of the national infrastructure are required, and this is where government can usefully provide advice on appropriate standards of resilience.

For the energy sector, DECC continues to work closely with industry and other government departments. DECC is committed to continuously improving our understanding of the impact of these threats and to ensure any measures taken are proportionate to the risk and have a clear and well justified need case. The findings of the ongoing work with E3C will help to inform future developments in this regard.

The MoD and EMP

10. We note the MoD's assurance that the Nuclear Firing Chain is designed and maintained to assure the UK's ability [for] deterrent and retaliatory action should the UK be subject to a nuclear attack. (Paragraph 76)

The Government welcomes the Committee's acknowledgment of the high degree of protection of the Nuclear Firing Chain.

11. EMP disturbances pose a serious risk, not only to civil infrastructure, but to military systems and ultimately national security. There must be a clear line of responsibility within the MoD; an appearance is given that the MoD is unwilling to take these threats seriously. The Government must make clear in its response to this Report exactly where lead responsibility in relation to EMP disturbances lies within the MoD. (Paragraph 78)

EMP is a cross-cutting issue which must be addressed in the MoD's policy, intelligence, acquisition and scientific support structures. As such, EMP issues are addressed by:

- Policy: The Director General Security Policy leads on space security, nuclear and EMP policy matters.
- The Operations Directorate is responsible for co-ordinating any military aid to the civil authorities under the Civil Contingencies Act 2004.
- Intelligence: Defence Intelligence is responsible for the all-source assessment of the nuclear EMP threat to the UK and the required capabilities (nuclear warhead and ballistic missile technologies) of any states or non-state actors that might have the intention to threaten the UK with a nuclear EMP attack. Defence Intelligence is also responsible for the all-source assessment of the threat capability of non-nuclear EMP devices.
- Acquisition: Defence Equipment and Support is responsible for the standards for protecting military equipment against the effects of EMP, and for ensuring that when there is a requirement for military equipment to meet these standards this is met during the procurement process. There are a range of standards that are shared with industry and applied as part of the procurement process.
- Scientific support: The MoD's Chief Scientific Adviser (CSA) provides all relevant scientific advice to Ministers and other Senior Officials. The CSA provides the UK technical lead in support of the 1958 Mutual Defence Agreement with the United States on nuclear matters and has a key personal role in the development of the UK's nuclear programme. The CSA leads and funds a Science and Technology (S&T) Programme that works closely with industry, academia and our international partners across the full range of S&T to provide technical advice, including on EMP. As part of this, Defence Science and Technology Laboratory (Dstl) provides technical advice on EMP to the MoD, for example, Dstl sit on and co-chair JOWOG 36 which is a UK-US working group established under the 1958 Mutual Defence Agreement with its focus

being the exchange of information on the nuclear hardening and survivability of military systems (excluding nuclear payloads/warheads) and civil information systems and infrastructure to meet it overall goal: to better the UK and US ability to assess nuclear weapon affects.

12. The MoD has access to a great deal of scientific information regarding nuclear and non-nuclear EMP devices. While there is an understandable sensitivity to such information, the MoD must make sure that where security considerations permit, relevant information is shared with civil infrastructure providers that may be at risk. (Paragraph 80)

The MoD will share relevant information with civilian infrastructure providers that may be at risk from EMP, where security considerations permit this. Military standards have been developed to inform decisions on appropriate levels of protection, and these will be available to cleared civilian infrastructure providers. The MoD's primary focus remains on the protection of military equipment, although MoD works closely with the Centre for the Protection of National Infrastructure to support the broader resilience of UK infrastructure.

13. The reactive posture described by the MoD appears somewhat complacent. Prior wargaming and planning is required to assess the likely involvement of MoD resources in dealing with the consequences of EMP events. (Paragraph 82)

As previously stated in the written evidence, Defence as a national asset may be called upon to provide assistance to the civil authorities in the event of a large scale civil emergency or crisis; an EMP event might constitute such an event. Under the provisions of Military Aid to the Civil Communities, the MoD provides some specialist, niche capabilities to the civil authorities but it does not generally fill capability gaps that are more appropriately met through the civil authorities' and industry's own business continuity planning. Defence may, however, provide additional capacity in the case of unpredicted failures in the civil response, if the scale of the emergency overwhelms civil capabilities, or to provide access to specialist Defence assets. The provision of general duties military support to help deal with the knock-on effects of an EMP event could be requested by any government department. This would be facilitated through a standing nationwide network of Joint Regional Liaison Officers who work routinely with local resilience fora and others to enable access to military assistance.

The MoD engages routinely with the Cabinet Office and other Government departments across a range of resilience preparedness issues and takes part in the national exercise programme to exercise the cross-Government response to a range of emergencies.

Satellite security

14. Security of satellites is a matter of growing concern as our reliance upon such systems and the sheer number of satellites in orbit increase. The Government must consider the long-term security of satellite technology and ensure that national interests are protected where we rely on other nations for data, such as GPS. In the event of very severe space weather, even hardened satellite technology might be at risk of degradation. The MoD cannot therefore rule out the loss or degradation of satellite based-communications systems, and must plan for this eventuality. (Paragraph 86)

The National Security Strategy assessed the risk of severe disruption to information received, transmitted or collected by satellites as a Tier 2 risk—i.e. one in the second order of priority taking into account both probability and impact. This assessment took into consideration both severe space weather hazards and the possibility of deliberate damage to satellite systems. The Government accordingly decided, in the Strategic Defence and Security Review, to establish a National Space Security Policy (NSSP) to coherently address all aspects of space security. This will be concluded later this year, and will consider space risks (including from space weather) and dependencies, and further steps which might be needed to improve resilience. The NSSP will also cover our national space security capability requirements, and how international partnerships underpin many of these.

The MoD has not ruled out the possibility of the loss or degradation of satellites whilst in orbit, and the associated loss or degradation of SATCOM. All space infrastructure is at some risk from space weather and debris. Military space systems (including GPS) have significant hardening against space environment effects. It is probable that GPS satellites would survive an extreme event such as the Carrington event of 1859. Complete loss of GPS during space weather events would be short-lived (tens of minutes), although it may be degraded over periods of hours during extreme events. Furthermore, Defence standards direct that military equipment must have appropriate hardening against nuclear weapon effects, including EMP. This hardening provides a level of protection against space weather effects.

Defence has assured and protected communications under the terms of a Private Finance Initiative (PFI) with Paradigm Secure Communications Ltd. These are derived principally from the Skynet 5 satellite constellation (and its ground infrastructure), which is hardened to withstand a reasonable worst case space weather event and HEMP. As far as our next generation capability is concerned, the Beyond Line Of Sight (BLOS) programme, of which SATCOM forms a part from 2022, is in Concept Phase: all hardening and resilience adheres to current requirements. The PFI also accounts for the provision of commercial SATCOM for military purposes. While commercial satellites are designed to withstand routine space weather effects, they would be more susceptible to severe space weather than their military-grade equivalents, and their ground stations would be less resilient to artificially-generated EMP effects and Geomagnetically Induced Currents caused by space weather. The MoD's Skynet communications services are also available to other Government Organisations and Departments, and future

requirements across Government Departments are currently being discussed with a view to developing successor services for all potential Government users.

To prepare for situations where satellites are unavailable, the military practice reversion techniques as a matter of routine. The Armed Forces train to operate in degraded conditions, and traditional methods such as navigation with maps and compass are taught at basic training and maintained throughout service by all service personnel. The Royal Navy exercises in the use of fallback High Frequency communications and in reversionary navigation methods as mitigation against hostile or natural interference. The RAF trains frontline aircrew (from all three services) to operate under significant Electronic Warfare conditions; this includes training in live GPS and communications jamming, and denial of space-dependent mission systems. Dstl operate annual GPS jamming trials for Defence Equipment and Support (DE&S), where the effects of GPS jamming on any equipment can be tested.

Responsibility in Government

15. We are very concerned that there appears to be no one Government Department identified to take immediate lead responsibility should there be a severe space weather event. It is not good enough to say that that will depend on where the greatest impact fell. We support and reiterate the recommendation of the House of Commons Science and Technology Committee that the Government must urgently identify the Lead Government Department for space weather events as a matter of priority. We expect the National Security Council to play a major role in this. (Paragraph 92)

The Government has well practised central response arrangements that are able to respond quickly to events. This has been frequently demonstrated, including to a number of events where there is no predefined lead such as severe winter weather. Non-preventable, naturally occurring electromagnetic effects caused by extreme space weather events are among a number of hazards that can affect national infrastructure assets in the energy and telecommunications sectors, among others. The Ministerial lead for the security and resilience of the national infrastructure sectors lies with the departments with responsibility for oversight of the sectors themselves. This means that, in the event of a space weather event that engages the Government and has very widespread effects, there is likely to be a number of Ministers with lead responsibilities for infrastructure involved in the response. In those circumstances, and in accordance with the Government response mechanism to emergencies set out in the Central Government Concept of Operations,[2] the Prime Minister may choose to assign overall lead responsibility either to a Minister whose infrastructure sector responsibilities are most heavily engaged, or to a Minister appointed on a personal basis to ensure an effective cross-sector approach to the emergency. The Government believes that these arrangements, which are well tested and ensure the fullest possible engagement of cross-Government resilience interests as well as clear leadership in a crisis, are likely to be more effective than nomination in advance of a lead Minister for severe space weather,

2 www.cabinetoffice.gov.uk/sites/default/files/resources/conops-2010.pdf

whose appointment would be likely to result in a loss of clarity of responsibility for the key infrastructure sectors.

Plans to consider sector resilience to space weather from relevant Government departments are in place, co-ordinated by the Cabinet Office. These plans aim to set out the Government's understanding of the resilience of infrastructure to natural hazards, and a public summary was published in spring 2011.[3]

Conclusion

16. The consequences of EMP events must be addressed specifically: generic civil contingency plans which address blackouts and temporary loss of electronic infrastructure caused by a range of events are not sufficient. Space weather is a global threat and may affect many regions and countries simultaneously. This means that there is scope for mutual assistance, but also that there is no safe place from which it can be assumed that help will come. It is time that the Government began to approach this matter with the seriousness it deserves. (Paragraph 97)

The threat from a range of EMP events is already acknowledged by Government; the threat is also a developing one and is monitored as such. Given that the nature of these threats affects many areas of Government, it is appropriate that responsibility is distributed across Government, and within departments, to the appropriate areas of expertise.

The Government agrees that a generic approach to mitigating the impacts of natural events such as severe space weather has value, but is not sufficient. That is why Government departments, under Cabinet Office lead, have been consulting extensively with space weather scientists and engineers, industry, private sector asset owners and regulators, to assess the specific consequences of a severe space weather event. A National Space Security Policy (NSSP) team has also been established under the SDSR commitment to coherently address all aspects of UK space security. An NSSP document is due to be published through the NSC later this year and will look at these risks in a much wider context, including the governance and resourcing of any new cross-Government space security structures.

The Government agrees that space weather events are global phenomena, and has sought to learn the lessons of major events that have affected a number of countries in recent years. Planning for a space weather event that affects the UK will not assume the availability of assistance from neighbouring countries, but will involve consultation with other countries, in particular in the EU and US, with similar interests in resilience to such an event. In these ways, the Government will continue to give the risks arising from severe space weather the attention that they merit, and to monitor and re-assess both the likelihood of a recurrence of a severe space weather event on the scale of the Carrington event and how such an event might affect modern infrastructure networks that are essential to the running of the country.

3 www.cabinetoffice.gov.uk/infrastructure-resilience