



House of Commons
Defence Committee

Developing Threats: Electro-Magnetic Pulses (EMP)

Tenth Report of Session 2010–12

*Report, together with formal minutes, oral and
written evidence*

*Ordered by the House of Commons
to be printed 8 February 2012*

HC 1552
Published on 22 February 2012
by authority of the House of Commons
London: The Stationery Office Limited
£14.50

Defence Committee

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

Current membership

Rt Hon James Arbuthnot MP (*Conservative, North East Hampshire*) (Chair)
Mr Julian Brazier MP (*Conservative, Canterbury*)
Thomas Docherty MP (*Labour, Dunfermline and West Fife*)
Rt Hon Jeffrey M. Donaldson MP (*Democratic Unionist, Lagan Valley*)
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 Seabek 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. A list of Reports of the Committee in the present Parliament is at the back of this volume.

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 Clayton McCleskey (Intern).

Contacts

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

Contents

Report	<i>Page</i>
Conclusions and recommendations	3
1 Introduction	7
The threat	7
How likely?	7
The inquiry	8
2 Nature of the threat	10
Space weather	10
The probability	11
Potential impact on electronic infrastructure	11
High Altitude Nuclear EMP Weapons (HEMP)	13
The EMP components	14
Practical experience	15
Potential impact on electronic infrastructure	15
Risk?	15
Non-Nuclear EMP	18
3 Resilience	20
Forecasting space weather	20
Protecting civil infrastructure	22
Strengthening the systems	23
Telecommunications	25
Advice to the public	25
4 The MoD and EMP	27
MoD resilience to EMP events	27
Responsibility in the MoD	28
MoD role in responding to an emergency	29
5 Satellite security	30
6 Responsibility in Government	32
7 Conclusion	35
Formal Minutes	36
Witnesses	37
List of written evidence	37
List of Reports from the Committee during the current Parliament	38

Conclusions and recommendations

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)
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 an 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)
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)

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)
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)

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)
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 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 deterrent and retaliatory action should the UK be subject to a nuclear attack. (Paragraph 76)
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)
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)
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)

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)

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)

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)

1 Introduction

The threat

1. Today's society places an ever-growing reliance on technology. Modern infrastructures such as power, telecommunications and water systems, businesses, industries and services are now interdependent to a very significant degree, and disruption can therefore spread very quickly as the effects cascade through connected systems. A failure of the national grid for example, would inevitably have repercussions for a wide range of businesses and services, from energy supplies, water processing, traffic control and logistical systems and even parts of the finance sector. Similarly a growing reliance is placed on satellite-based technology such as GPS (global positioning system); for instance the operation of financial markets relies on accurate timing supplied by GPS. The UK military are greatly reliant on a range of electronic communications and navigation systems.

2. Such technologies are known to be vulnerable to the effects of space weather and other electromagnetic activity, such as that which would result from the detonation of a nuclear weapon at high altitude. The potential threat of EMP (Electro-Magnetic Pulse) used as a weapon against the UK also poses a significant risk to UK National Security. Understanding the extent of these risks and the need to mitigate them is therefore at least partly within the remit of the MoD.

3. For 50 years, governments concentrated on the threat of deliberate attack, and electromagnetic pulse was regarded as a problem to be addressed by the military. It was only in 2008 that space weather was accepted as a threat of which civil authorities should also take account.

How likely?

4. The National Security Strategy (NSS) published in October 2010 itemised several tiers of "priority risks" which had been identified by the National Security Risk Assessment. The highest, Tier 1, risks included "a major accident or national hazard which requires a national response". Space weather is referred to as part of this identification:

We also monitor new and emerging risks, such as the potential impact of severe space weather on our infrastructure. Given the range of hazards and accidents that can cause large-scale disruption and the very severe impacts of the worst of these, this risk grouping is judged to be one of the highest priority risk areas. Our approach is to plan for the consequences of potential civil emergencies no matter what the cause.¹

5. Written evidence from the Government suggests that a severe space weather event, with resulting damage, may occur in the next few years:

The impact of EMP events caused by nuclear devices would be very severe but the likelihood is currently considered to be low. Non-nuclear EMP devices exist and the

1 Cabinet Office, *National Risk Register of Civil Emergencies*, 2010 Edition, para 3.44

risks are being kept under review but are not currently considered to be sufficient to warrant recognition as a national security risk. Severe space weather, which might cause geomagnetic storms impacting the Earth's magnetosphere, has been the subject of extensive research over the past year. The likelihood of a severe space weather event is assessed to be moderate to high over the next five years, with the potential to cause damage to electrically conducting systems such as power grids, pipelines and signalling circuits.²

6. The most recent published version of the National Risk Register (2010) contains no explicit reference to space weather or EMP events and the only reference made to electricity outages assumes that there is no actual system damage.³ However, space weather is currently under assessment by the Government for the National Risk Assessment and Risk Register 2011.

7. While there are a number of similarities between the effects of severe space weather and deliberate EMP attack —not least in that neither is likely to respect national boundaries— they merit separate treatment both by the Government and in this Report.

The inquiry

8. On 13 September 2011, the Committee announced an inquiry with the following terms of reference:

- The extent of any threat posed to UK electronic infrastructure by EMP events caused by space weather events, nuclear weapons detonated at high altitude or other EMP weapons;
- The likelihood that a viable EMP weapon can or will be used by either state or non-state actors;
- The extent to which space weather is forecast and the effectiveness of early warning systems that may be in place;
- The potential impact of such events for both civilian and military infrastructure;
- Ways of mitigating electromagnetic pulse events, either targeted or naturally occurring;
- The resources available in respect of research and development in this field;
- Contingencies in place to react to a large-scale loss of UK electronic infrastructure, and the role of the military in such an event;
- The broader security of UK electronic and space infrastructure, particularly satellites and satellite navigation systems and the risk posed by space debris.

2 Ev 20

3 Cabinet Office, *National Risk Register of Civil Emergencies*, 2010 Edition

9. This inquiry is intended to be the first of a series into emerging threats. We acknowledge that we may, as our first contribution to the debate, have raised more questions than can, at this stage, be answered.

10. The Committee invited the submission of written evidence by 14 October 2011. We received evidence from HM Government, the Electronic Infrastructure Security Council (EISC), the US Federal Energy Regulatory Commission (FERC), the Chair of the Commission to Assess the Threat to the United States from Electro-Magnetic Pulse Attack (the EMP Commission), the Office of Electric Reliability, the International Electrotechnical Committee, Peter Taylor of Ethos Consultancy, the Royal College of Physicians, the National Grid and Research Councils UK. We held one oral evidence session, hearing evidence from Professor Richard Horne of the British Antarctic Survey, Dr David Kerridge of the British Geological Survey, Avi Schnurr, Chairman and Chief Executive of EISC, Chris Train of the National Grid, Nick Harvey MP, Minister of State for the Armed Forces, Charles Hendry MP, Minister of State, Department of Energy and Climate Change, Sir John Beddington, Chief Scientific Adviser to HM Government, David Ferbrache, head of Cyber, Ministry of Defence and John Tesh, Deputy Director, Civil Contingencies Secretariat, Cabinet Office. We are grateful to all who assisted us, and particularly to Michael Hapgood and Philip Sturley, our Specialist Advisers⁴ and to our staff.

11. It is noteworthy, and indicative of the complexity of the subject, that the Government evidence was provided by the MoD in consultation with officials from other Government Departments and the National Security Council.

12. We note that the Science and Technology Committee, in its Report on Scientific Advice to Government, has commented on the implications for the UK of severe space weather events. Our own Report, to some extent, builds on theirs, and we are grateful to them.⁵

4 For the interests of the advisers, see Minutes of the Defence Committee, 13 July 2010, and 13 September 2011.

5 Science and Technology Committee, Third Report of Session 2010–11, *Scientific Advice and Evidence in Emergencies*, HC 498, para 18

2 Nature of the threat

Space weather

13. “Space weather” is a naturally occurring phenomenon that can impact upon the Earth’s environment in ways that are detrimental to key technologies in operation in space, the atmosphere and the surface of the Earth. “Space weather” generally refers particularly to changes in the space environment near Earth, caused by varying conditions in the sun’s atmosphere. Solar activity adheres roughly to an eleven year cycle, with solar activity increasing during a “solar maximum”, making space weather events more likely. The next solar maximum is predicted to occur in 2013. However, space weather events do not necessarily obey this cycle; the Carrington event of 1859 (see below) occurred in the middle of a cycle. Space weather events are an everyday occurrence. Indeed, the well-known phenomenon of the aurora borealis, or “Northern Lights”, is an effect of charged particles originating from the sun colliding with the Earth’s atmosphere.

14. The following table summarises some of the different types of space weather and their potential impacts.

Table 1: Categories of Space Weather

Space Weather	Cause	Potential impact
Coronal Mass Ejections (CMEs)	Plasma ejected violently from the outer atmosphere of the sun	Fluctuations in the Earth’s magnetic field (geomagnetic storms), driving additional current into power grids, disrupting satellites, GPS (global positioning system) and radars
Solar Energetic Particle (SEP) events	High energy particles expelled from sun during solar events like CMEs	Damage to electronics, computer chips and power systems in spacecraft [and aircraft] (possibly at ground level too), raised ground radiation levels
Solar radio bursts	Intense bursts of radio noise produced by solar events like CMEs	Interference with low power wireless radio technologies such as mobile phones, wireless internet and GPS receivers
Solar flares	Outburst of radiation and energetic particles	Modest effects on Earth

Data Source: Science and Technology Committee, Scientific Advice and Evidence in Emergencies, para 18

15. The largest ever recorded space weather event occurred in September 1859. It is known as the Carrington Event after Richard Carrington, the British astronomer who observed a solar flare so strong that it could be seen with the naked eye. The huge coronal mass ejection (CME) that followed induced enormous electric currents that surged through telegraph systems, causing shocks to telegraph operators and setting fire to papers.⁶ Operators were able to disconnect their batteries and continue to send messages using only this induced current. The impact was so wide-ranging that auroras, normally limited to polar regions, were observed as far South as Hawaii and the Caribbean.⁷

⁶ “A Super Solar Flare”, *NASA Science News*, 6 May 2008, science.nasa.gov/science-news/science-at-nasa

⁷ *Severe Space Weather Events – Understanding Societal and Economic Impacts*

16. The Carrington event is thought to have been up to ten times larger (depending on what effect is being measured) than anything seen in the past 50 years.⁸ There have been less significant, but still destructive, events in the more recent past. In March 1989 a large CME caused the Canadian province of Quebec's power grid to collapse within 90 seconds, after stabilising equipment failed to cope with the effects of the geomagnetic storm. Around six million people were subsequently without power for nine hours. The same storm caused a transformer to fail in New Jersey and various other effects across the North American grid. It is also thought to have been the cause of damage to two transformers in the UK. The adverse effects of extreme space weather on modern technology are therefore well documented.

17. Resilience to space weather events is routinely built into some components of infrastructure, such as satellites, which are frequently exposed to its effects. However, events vary in intensity, and the potential impact of a severe event could be devastating.

18. Space weather events have the potential adversely to affect human health in some cases. Exposure to even very high levels of electromagnetic activity is not thought to have any direct ill-effects on humans or any other living organisms. However, there could be potential implications for patients with implantable cardiac devices, as highlighted to the Committee by the Royal College of Physicians.⁹ Solar energetic particle events may lead to increased exposure to radiation for workers such as pilots and flight attendants on long-haul flights.

The probability

19. The Government told us that the likelihood of a severe space weather event (not necessarily, of course, a Carrington-magnitude event) over the next five years was assessed as being moderate to high, with the potential to cause damage to electrically conducting systems such as power grids, pipelines and signalling circuits.¹⁰

Potential impact on electronic infrastructure

20. The maximum possible severity of a space weather event is, of course, impossible to estimate, but witnesses use the Carrington event as a reasonable worst case possibility.¹¹ Since 1859 the reliance of the world on electrical power has increased enormously. As a result, as the Met Office put it, "the potential effects of space weather are growing rapidly in proportion to our dependence on technology".¹² The impact of an event on the scale of the Carrington Event occurring today would be huge; the US National Research Council estimated the wider societal and economic costs of a severe geomagnetic storm occurring today to be around \$1–2 trillion.¹³

8 Ev 22

9 Ev 46

10 Ev 30

11 Q 17

12 Ev 50

13 *Severe Space Weather Events – Understanding Societal and Economic Impacts*, p 4

21. The cause of the damage would be geomagnetically induced currents (GICs). These are electric currents driven by electric fields that are induced in the surface layers of the Earth crust by rapid changes in the geomagnetic field (such as those occurring during magnetic storms). These currents are most evident in long metal structures, such as power grids, pipelines and railway circuits, with earth connections to the surface layers, so that currents can flow between the Earth and these structures. Research Councils UK highlighted in particular the risk of GICs causing damage to electrical grid transformers:

GICs pose a threat to electricity distribution grids extending over long distances which can cause blackouts and damage. Permanent damage to transformers caused by GIC is a major concern. Transformers are costly, not available as “off-the-shelf” items, and replacing one is a major exercise. The consequences of a prolonged loss of electrical power are potentially catastrophic as the infrastructures and services that modern developed societies rely on are entirely dependent on electricity. Examples include heating, lighting, refrigeration, communications, pumping of fuel, water and sewage.¹⁴

22. The US National Academy of Sciences has estimated that if a magnetic storm that occurred in May 1921 was repeated today then 130 million people in the US would lose their electricity and more than 350 transformers would be at risk of permanent damage.¹⁵ Avi Schnurr, Chair of the EIS Council added that the Federal Energy Regulatory Commission (FERC) had estimated that the duration of the impact would be five to 10 years.¹⁶ He thought it would be fair to say that the conclusions about the UK would not be better.

23. While experience of, and forecasts about the likely impact of, severe space weather on the USA, are relevant, it cannot automatically be assumed that the effect of the UK would be the same. FERC wrote “while the threats posed by EMP and the vulnerabilities of electrical infrastructure to EMP are not unique to the US, differences between the US and UK power grids should be considered when reviewing the applicability of these responses to the UK”.¹⁷ Chris Train of National Grid thought that the consequences in the UK would be less because the UK infrastructure was differently formulated:

We have been working along with our partners—the BGS and Manchester University and others—looking at what the potential impacts would be here in the UK.

Because of the meshed infrastructure here in the UK, we believe that the impact would not be as great here. The effort that we have been putting in has been around operation mitigations following a coronal mass ejection to understand how we might manage the system to minimise the impact of the potential in such an event. But I do not think that it would have the same catastrophic cascading effect that would

14 Ev 25–26

15 *Severe Space Weather Events – Understanding Societal and Economic Impacts*, p 3

16 Q 3

17 Ev 48

happen in the United States because of the different nature of the configuration and development of the networks.¹⁸

24. In response to Chris Train, Avi Schnurr made clear that he thought that the National Grid assessment was, for a variety of reasons, too optimistic.¹⁹ Both witnesses did, however, agree that there was more work to be done on the modelling.²⁰

25. National Grid, while noting that contingency plans were in place to react to damage, admitted that in the event of an extremely severe storm, long-term blackouts could be a possibility:

If all transformers at a node are damaged then, depending on the location of the node within the network, this could result in a local area being disconnected until replacement transformers could be installed. Replacing a transformer can take two or more months depending on the availability and location of spares. In this extreme event scenario National Grid estimates that the probability there would be a disconnection event is 62% for England and Wales and 91% for GB as a whole.²¹

26. If, as might be expected, several countries were affected simultaneously and needed new transformers, this would, presumably, affect the availability of spares and hence extend the delay in restoring power supplies.

27. As noted by several commentators, including Research Councils UK, modern developments in technology have actually led to greater vulnerability to the effects of space weather, as microchips become smaller and more advanced. This is a particular hazard for satellites which are exposed to the greatest effects of space weather.

28. 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.

29. 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.

High Altitude Nuclear EMP Weapons (HEMP)

30. Space weather events have always been with us, though their likely effects have become more significant as technology advances. A newer threat, though one which has been the subject, until recently, of more research, is the possibility of deliberate attack, perhaps with

18 Q 4

19 Ev 41

20 Q 5

21 Ev 26

little or no warning. A single nuclear weapon detonated between 25–500 miles above the Earth could create an electromagnetic pulse (EMP) – i.e. a high density electrical field--with the potential to cause severe damage to technology over a wide geographical area, the area depending on the height of the detonation.

31. The effect of such a high-altitude nuclear EMP (HEMP) burst would not be identical to those of severe space weather because it would create a series of electromagnetic “waveforms” that each has a slightly different effect on Earth. The overall effect, however, would be similar in nature to the effects of naturally occurring space weather, but faster and more intense, which makes HEMP potentially highly destructive.

The EMP components

- “E1” or “Fast” component occurs within a few billionths of a second of detonation. It produces a very brief but intense electromagnetic field that can induce very high voltages in electrical conductors. Unlike naturally occurring geomagnetic storms, which pose the greatest risk to long electrical conductors like power line transformers, this effect has the power to disrupt or damage micro-electronic systems, electronics-based control systems, sensors, communication systems, protective systems, computers and similar devices. Damage and disruption could occur almost simultaneously over a very large area.²²
- “E2” covers roughly the same geographic area as the first component and is similar to lightning in its effect, though far more geographically widespread and somewhat lower in amplitude. In itself this component would not be an issue for critical infrastructure systems since they have existing protective measures for defence against lightning strikes. The most significant risk derives from the fact that this component follows a small fraction of a second after the first (E1) component, which may have already impaired or destroyed protective and control features. The energy associated with the second component therefore may be allowed to pass into and damage systems.
- “E3”, or “slow” component is a slower-rising, longer-duration pulse that creates disruptive currents in long electricity transmission lines, similar in effect to that of a severe geomagnetic storm.

32. The sequence of E1, E2, and E3 components of EMP is important because each can cause damage which can allow subsequent components to cause greater damage than they might independently. The combined effect of a nuclear EMP is therefore very difficult to mitigate,²³ and witnesses agreed that such an event would be “a different kettle of fish” from a Carrington-sized event, and a “truly catastrophic event”.²⁴

22 *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1: Executive Report, 2004, p 5*

23 *Ibid.*, pp 5–7

24 Q 90

Practical experience

33. In July 1962, the United States conducted an experiment with the detonation of a 1.4 megaton nuclear weapon (Starfish Prime) 250 miles above the Pacific Ocean, around 900 miles from Hawaii. The effect of this explosion was the generation of an electromagnetic pulse that was far larger than expected. The EMP caused damage to electrical equipment in Hawaii, knocking out streetlights, setting off fire alarms and damaging telephone equipment. There were also visible auroras in the sky following the detonation. In 1962, the Soviet Union also performed a series of three high-altitude nuclear tests in space over Kazakhstan. The weapons used were smaller than that of the US's Starfish Prime test, but the EMP effects were reportedly more significant, as the detonations occurred over a populated area. While there is little information available about these tests at least in the public domain, what there is suggests that there was significant damage to telephone wires and power cables.

Potential impact on electronic infrastructure

34. An EMP Commission was established in the United States in 2001 to look expressly at the potential impact of a high altitude EMP attack on key US infrastructure. It published a preliminary report in 2004 which established the nature of the threat being faced, followed by a final report in 2008 which went into much greater detail as to the potential impact on critical national infrastructures and recommended courses of action to address the threat. Its overall conclusions were that US society is vulnerable to an EMP attack, the consequences of which might be long-term, widespread and catastrophic, and because of the interdependency of the systems which are likely to be affected, the current recovery plans may be of little value.²⁵

35. National Grid's written evidence reiterated the concerns of the EMP Commission:

The effect of E1 and E3 pulses from HEMP would be considerably more extreme [than space weather events]. For these effects we have no practical experience to fall back on, although the Commission to Assess the Threat to the United States from EMP Attack did conduct a number of experiments on E1 and its effect on SCADA. They concluded that "Large-Scale load losses in excess of 10% are likely at EMP threat levels" and that "widespread collapse of the electrical power system [...] is virtually inevitable."²⁶

Risk?

36. While the probability of a HEMP attack is judged by the Government to be low, it is accepted that its impact would be high, and in view of this the Government includes it in the second tier of priorities for UK national security.

37. The Government does not differentiate in its risk assessment between HEMP and other elements of a nuclear attack:

25 *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, Volume 1*, preface vi–vii

26 Ev 27

The National Security Strategy and National Security Risk Assessment assessed the risk from a nuclear attack and thus HEMP, as part of the risk of an attack on the UK by another state or proxy using CBRN (chemical, biological, radiological and nuclear) weapons. This risk was judged to be low likelihood but in view of the impact, to be considered in the second tier of priorities for UK National Security.²⁷

It views the threat as potential rather than actual.

Currently no state has both the *intent* to threaten our vital interests and the *capability* to do so with nuclear weapons. MOD's view is that over the next decade, existing space launch vehicle technology could theoretically be adapted by states to deliver a nuclear device; however, the MOD does not currently see the UK or Western Europe as a target for such an EMP attack. MOD does not believe that any non-state actors can currently produce improvised nuclear devices and none are likely to be able to make a sufficiently robust warhead for missile delivery in the foreseeable future.

And

To generate more widespread damage from EMP, a nuclear warhead would have to be detonated at high altitude to generate the EMP from the interaction between the radiation from the weapon and the outer layers of the atmosphere. This could only be achieved by launching a device by missile to an altitude of several tens of kilometres. A limited number of States possess this capability.²⁸

38. The US EMP Commission found that some “rogue states”, including Iran and North Korea, are aware of the potential of such an attack. Iran, in particular, is reported to have been conducting what appear to be missile tests to simulate a nuclear EMP strike.²⁹ According to US Senate testimony, an Iranian military journal publicly discussed using EMP against the West:³⁰

Once you confuse the enemy communication network [...] you will, in effect, disrupt all the affairs of that country. If the world's industrial countries fail to devise effective ways to defend themselves against dangerous electronic assaults then they will disintegrate within a few years.³¹

39. We asked Avi Schnurr if Iran had the capability to launch a weapon to an altitude of several tens of kilometres. He replied that there was a serious risk that rogue states and nations, some of which already possessed the launch capacity, would acquire the necessary weapons:

There are only two things that stand right now between us—by “us” I mean the United Kingdom, the United States and other allies—and having this level of catastrophe. One is that although they have the ships and the missiles, terrorists

27 Ev 52

28 *Ibid.*

29 “*Global Single Point Failure: The EMP threat*”, the EMP Awareness Coordination Taskforce (EMPACT), 2009

30 Statement from Dr. Peter Vincent Pry, EMP Commission Staff, before the United States Senate Subcommittee on Terrorism, Technology and Homeland Security, March 8, 2005: *Foreign Views of Electromagnetic Pulse (EMP) Attack*

31 “*Electronics to determine the fate of future wars*,” Nashriyeh-e Siasi Nezami, December 1998-January 1999

groups and rogue nations do not today, necessarily, have access to nuclear weapons. That is a very thin boundary, because, for example, North Korea has nuclear weapons. Could North Korea sell its nuclear weapons? Could there be destabilisation in a state that has nuclear weapons? I could name a few. Those are things that could happen in the future. The other thin boundary is will. We are dependent on keeping any warhead of any size out of the hands of transnational terrorists or rogue nations and on their good will if they acquire them.³²

40. We asked the Ministry of Defence if Iran could launch a missile from a ship. Following a rather confusing exchange,³³ we asked for written clarification. They explained:

A number of elements are required to enable a state or non-state actor to successfully launch a nuclear EMP attack:

A **delivery system** capable of adequate range and altitude, with the capacity to carry a significant payload. A ballistic missile is, therefore, the most likely delivery system and, given the weight of a HEMP device, it must be capable of carrying a payload significantly heavier than a high explosive warhead.

A **nuclear device** is also required to deliver a HEMP. Successful uranium enrichment and sophisticated weapons engineering are required to manufacture a viable nuclear device. To be delivered at high altitude to generate a HEMP, the nuclear device must also be ruggedised sufficiently to withstand: the harsh conditions of launch; the high velocity journey through the atmosphere and into space; and, perhaps, depending on where on the flight path the nuclear device is detonated, a period of re-entry.

As well as manufacturing a robust nuclear device, it must then be successfully **integrated** into the ballistic missile to create a weapon system.

The development of all these elements is technically very challenging and expensive, with progress likely to be made in small incremental steps over a period of many years, and we judge this to be within the grasp of only a limited number of state actors.³⁴

41. Consistent with its view of the threat of an HEMP attack as potential rather than actual, the policy of the Government is to try to ensure that no attack occurs. David Ferbrache said:

We are very much focused on trying to ensure that that event does not occur in the first place, which is all about counter-proliferation action to prevent the acquisition of nuclear weapons or ballistic missile capabilities. Deterrent capability is one of the areas that we make absolutely certain is protected against EMP, in terms of our ability then to retaliate against such an aggressive act.³⁵

32 Q 29

33 Q 41

34 Ev 51–52

35 Q 90

42. 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 an 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.

Non-Nuclear EMP

43. It is also possible to build non-nuclear devices which can disrupt electronic systems, though so far only over a limited area. The Chair of the US EMP Commission wrote:

Non-nuclear EMP weapons, like radiofrequency weapons, can damage and destroy electronics locally. Such weapons have short ranges, kilometers for some military systems to meters for devices improvised by terrorists or criminals. Industrial EMP simulators, intended to test commercial systems for hardness against interference from stray electronic and radio emissions, are on the open market and can be purchased by anyone. At least one such EMP simulator is designed to look like a suitcase, can be operated by an individual, and is powerful enough to damage or destroy the electronic controls that regulate the operation of transformers and other components of the power grid. Armed with such a device, and with some knowledge about the electric grid, a terrorist or lunatic could blackout a city.³⁶

44. Avi Schnurr said:

The biggest issue with non-nuclear EMP weapons is that the complexity and threshold required to produce them is minimal, to say the most. At the summit meeting in Washington DC, for example, there were two Assistant Secretaries of Defence, a Deputy Under-Secretary and the Pentagon's chief lawyer, all of whom expressed grave concerns over this risk—the non-nuclear EMP risk in particular, but the risk of EMP in general. The non-nuclear EMP risk is much shorter-range. However, that range, which could be 100 metres, a fraction of a kilometre or a kilometre—under certain circumstances, which I could discuss separately, it could be multiple kilometres—includes the risk of having a field strength that would be even greater, although limited in extent, than a nuclear EMP [...]. We had a speaker at that summit who described, to the extent he was allowed to describe it, a device that he built from hardware he acquired from retail stores in the United States, which he had built into a van.³⁷

45. A number of nations are thought to be undertaking research into the development of non-nuclear EMP attack weapons, but the Government does not currently regard them as a serious risk.³⁸ Nick Harvey said “it is certainly considered a potential threat. It is not

36 Ev 54

37 Q 33

38 Ev 20

considered a particularly likely one, certainly in the foreseeable future; but we keep that constantly under review. It is a material risk that we need to consider, but we do not think there is any imminent likelihood or threat from it”.³⁹

46. While in the UK material relating to non-nuclear EMP is highly classified, other nations, particularly in the EU, are apparently much more open about devices in existence and in development. We asked the MoD why the UK kept information about non-nuclear EMP under a higher security classification than did other countries, and whether this affected its ability to share best practice with allies. The response was:

We collaborate with our allies on non-nuclear EMP effects, including research and development into countermeasures, through the NATO research and technology organisation which has a working group looking at those issues—so that is quite a close linkage.

In terms of classification, there is quite a bit of material on the internet. We routinely monitor that and assess it. Some of the devices are potentially viable; some are not. Most of them are rather short-range; for instance, with modified microwave sources, you are talking about ranges in the category of hundreds of metres. We keep an eye on those threats. Is it classified? There are some classified areas. We do not want to share our view on what viable devices might be at the high end of non-nuclear EMP, so we protect that very sensitive area, because we do not wish to see further proliferation of those competent devices. That is the classification reason.⁴⁰

47. 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.

39 Q 72

40 Q 111

3 Resilience

48. The Government's approach to mitigating the effect of an EMP attack and the EMP-like effects of space weather is three-pronged:

Prior warning is given, either through forecasting or the collection of intelligence, enabling appropriate action to take place, for example switching off vulnerable satellite systems;

Infrastructure is hardened where appropriate, this is especially critical with military infrastructure;

We prepare for these events although the Government's approach to civil resilience management is to plan for the consequences of potential civil emergencies no matter what the cause. Contingencies are in place to react to large scale loss of electronic infrastructure with the restoration of the National Grid being a priority.⁴¹

49. The key to successful mitigation of EMP events, whether natural or made-made, is successful forecasting both of the likelihood of such events and of their probable effects. The Government explained that "The UK has significant research resource available. The civil sector focuses on the effects of space weather whereas the military sector covers both space weather and its possible EMP effects".⁴²

Forecasting space weather

50. Given that space weather cannot be prevented, efforts are being made to improve forecasting in order that pre-emptive action may be taken. As Research Councils UK told us "Warning and prediction of space weather events is one of the most important ways of mitigating effects. Essential systems can then be put into safe mode, but this may not always ensure survival".⁴³

51. Space weather forecasting is in its infancy. Research Councils UK told us that "the UK has a long and successful heritage in relevant solar observations [...]. However, forecasting space weather is very difficult and it is still at an early stage often considered comparable to weather forecasting in the 1960s".⁴⁴ National Grid told us that CMEs can take 18 hours to three days to reach Earth. Forecasting models are used to decide on their trajectory and timing. NASA issue forecasts of arrival time giving a six hour window. However, these forecasts are frequently inaccurate, with the arrival time being many hours early or over a day late.⁴⁵ Nonetheless, witnesses told us of encouraging progress in the last few years, at least in terms of awareness.⁴⁶ We received evidence of a number of organisations active in

41 Ev 20

42 Ev 1

43 Ev 31

44 Ev 29

45 Ev 26

46 Ev 21 and 32

the field of space weather and of their co-operation. Dr Kerridge of the British Geological Survey said:

There has been a great acceleration over the past year in the way we have addressed this problem. The event about a year ago, which Mr Schnurr led, led a few of us to sit down and say, “How can we better organise ourselves to address this problem?” As a result of that, in October 2010 we began something that we have termed the Space Environment Impacts Expert Group. At the same time, there had been developing through the Met Office, the Ordnance Survey and the Environment Agency a Natural Hazards Partnership. Those two things have developed quite quickly to look particularly at space weather and other hazards. Each of those has the support of the Civil Contingencies Secretariat in the Cabinet Office. So the latest development is to advise on the national risk assessment for the space weather and other hazards and to provide advice to the Government Office for Science.⁴⁷

52. Sir John Beddington, Chief Scientific Adviser, told us of another initiative:

I might add that there is a rather awkward acronym SEIEG, which stands for the Space Environment Impacts Expert Group, led by Rutherford Appleton Laboratory, with the British Geological Survey, British Antarctic Survey, QinetiQ, SolarMetrics and the Met Office as members. That group is working closely within the Cabinet Office’s orbit. In my role as Chief Scientific Adviser, I have met the group and provided a critical-friend challenge to some of these things. It is fair to say that there is a fair bit of work in progress.⁴⁸

53. Significant in this context is the joint announcement by President Obama and the Prime Minister following the presidential visit. Professor Kerridge said:

Following President Obama’s visit, there was a joint statement from the Prime Minister and the President⁴⁹ indicating that we were going to enhance the collaboration on space weather in all aspects: monitoring, prediction, assessment of mitigating measures and so on. That is active at present. In particular, one of the things that has been taken forward is an agreement between the Met Office and NOAA, the National Oceanic and Atmospheric Administration, to co-operate on providing 24/7 cover for prediction and warning of space events. That is active. The aim is to enhance that; that is very much the view of the Prime Minister and the President that it should be done. That is active engagement, primarily at official level at the moment, but also for our organisations.⁵⁰

54. There have been two Infrastructure Security Summits, the first in Westminster in September 2010 and the second with wider participation from industry (as well as by the Chair of this Committee) in Washington in April 2011. Both led to further research work by industry providers on the likely effect of severe space weather. The next one is due to be

47 Q 19

48 Q 79

49 “Prime Minister and President Obama strengthen collaboration”, www.number10.gov.uk/news, 25 May 2011

50 Q 79

held in the UK in the spring of 2012. All such evidence of international co-operation is encouraging in view of the transnational nature of the space weather threat.

55. 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.

56. 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.

Protecting civil infrastructure

57. The management of disruption to electricity or telecommunications in the event of severe space weather is for the suppliers themselves, with some Government assistance. As the Government evidence said:

Successful management of a major electricity supply emergency requires effective communication and cooperation between industry and government. The wider consequences of an incident could be mitigated by the choices that industry is able to make, and some of the practical aspects of managing an incident could be assisted by the activities of government. *The National Emergency Plan for Downstream Gas and Electricity* (NEP-DG&E) sets out a framework for industry and government to work together to manage a major supply emergency.⁵¹

58. Charles Hendry told us that a letter had been sent by National Grid and the Department of Energy and Climate Change in October 2011 to all energy providers seeking industry support further to develop collective understanding of the impact of a severe space weather event on the GB electricity system. He explained:

The purpose of the letter that one of our directors in the Department wrote to the energy companies and others at the beginning of October—it was a joint letter with National Grid—was to increase greatly their active engagement in this work, to make sure they understand the urgency we attach to it and to say that we need their active engagement in ensuring that the strategy being prepared for early next year reflects their needs.⁵²

We congratulate DECC and the National Grid on this initiative to involve the energy companies.

59. Chris Train of National Grid explained how mitigating measures could be taken:

In terms of naturally occurring space weather, we have a set of operational mitigations in place, which start with the better forecasting of space weather and

51 Ev 24

52 Q 94

increased understanding about the likelihood and any timing of impacts. We have a number of operational measures that we can put in place, such as de-loading vulnerable transformers, spreading generation around the network and manning particular sites.⁵³

Should a storm exceed National Grid's worst planned-for scenario, however:

In conjunction with Government, National Grid would consider a controlled shut-down of the network. National Grid has a well developed Black Start Policy: Training exercises are regularly held on Black Start, and generating units are at all times scheduled for Black Start capability.⁵⁴

60. The Grid has also recently increased the number of spare transformers it holds.⁵⁵ Even so, National Grid estimated that in the case of an event of the size of a Carrington-sized event there was a 91% chance that an area of the United Kingdom would be without power for two months or more while a damaged transformer was restored or replaced.⁵⁶

61. The protective measures described apply to space weather events. National Grid said:

Research to investigate options to harden the UK system, rather than relying on operational procedures as is appropriate for solar events, would be needed to mitigate this threat. But given the size of the undertaking, and the subsequent cost of procurement and installation, this is beyond the resources of any one commercial organization, or group of organizations, and would need to be pursued at national level.⁵⁷

Strengthening the systems

62. Current planning is based to a large extent on pre-emptive action, such as shutting down equipment as a precaution, and on restoring service after damage has, despite these precautions, been done, though new systems are being built to a higher standard. National Grid described the development of technologies whereby new equipment can be made more resilient to space weather events. Charles Hendry, Minister of State, Department of Energy and Climate Change, for instance told us that "since 1999, all the transformers purchased by the National Grid have been ones that can stand the high electricity currents that might be caused by such activities".⁵⁸ (It should be noted that since 1999 the worst-case scenario has been revised upward.)⁵⁹

53 Q 37

54 Ev 27. A 'black start' is restoring power following a shutdown of part or all of the National Grid. One key element in this is the ability to restart some (but not all) power stations to operation without drawing power from the grid. The other power stations can then be restored using power from the grid. There are a number of other technical elements that are needed to ensure that power stations and grid come back on smoothly.

55 *Ibid.*

56 Ev 26

57 *Ibid.*

58 Q 94

59 Ev 25

63. We were also given examples of how equipment might be hardened retrospectively. While such retrospective hardening of the system might appear to be an attractive proposition, witnesses agreed that there was a risk that hardening one component of the infrastructure might simply move the problem on to another section of the system, and what was appropriate in the US might not be so in the UK. Chris Train said:

Hardening in itself is actually quite a challenge. There is talk of putting capacitance in the earth in order to block the GICs, but this is unproven. There are some difficulties peculiar to the design of the transformers in the UK compared with the US, which actually means that this would need a very close look at before such measures were considered. On the capability actually to roll that out, it would take an incredibly long period of time to do that. Once you harden an asset, all you are doing is moving the problem to the next asset.⁶⁰

He argued that the exercise was unproven in terms of effectiveness and “would need proper research to determine whether it would be effective. Intruding in the asset causes other problems as well, so you might be mitigating the potential for a very rare event and triggering a more frequent event”.⁶¹ Avi Schnurr agreed that further testing was needed.⁶²

64. 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.

65. 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.

66. 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

60 Q 37

61 Q 39

62 Q 43

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.

Telecommunications

67. It is obvious that the continued availability of telecommunications systems would be important in the event of a severe space weather event or HEMP attack causing widespread national disruption. Such evidence as we received on the effect of these on telecommunications was relatively encouraging.

68. The Government told us that while “telecommunications and electrical power distribution infrastructures are mutually dependent”, public, fixed line, systems at least were relatively robust, having arrangements “that enable them to continue to function for up to five days in the event of the loss of grid-distributed electricity”.⁶³ As with the electricity grid, “telecommunications infrastructures are owned and operated by private sector organisations who are best placed to respond to and recover from a major telecommunications incident”. It is also the case that the fixed-line structure uses optical fibre for most lines, and this is highly resistant to space weather. Nonetheless:

Government has worked closely with the owners and operators [...] through the Electronic Communications Resilience and Response Group to facilitate restoration of services in the event of a major incident affecting networks. The procedures that are in place are subjected to an extensive annual test conducted over several days.⁶⁴

And

Core telecommunications networks are highly resilient when viewed against the planning assumptions from the National Risk Assessment.⁶⁵

69. In an EMP emergency, the Government would be heavily dependent on telecommunications during mitigation and restoration measures. We were assured that, if telephone lines were down, an alternative means of communication was available to Government through hardened, military, satellites.⁶⁶

Advice to the public

70. A severe space weather event, let alone an HEMP, would severely disrupt the life of the UK, as suggested by Peter Taylor of Ethos Consultancy.⁶⁷ We asked the Government witnesses whether there was anything businesses or families could do to protect themselves. John Tesh told us:

63 Ev 24

64 *Ibid.*

65 *Ibid.*

66 *Ibid.*

67 Ev 63

The answer is that there is, but it does not yet reflect our current understanding of the possible impacts of solar weather on businesses on the ground, as it were. We have something called the national risk register, which we published for the first time in 2008, with an updated version in 2010. We intend to update it further in the next three months, by the end of January next year; at that time, we expect it will reflect new risks that have emerged, on which we did not have material to include in the last one. That will include the effects of solar weather.

The purpose of the risk register is to provide an indication to people of the kinds of things that can disrupt their lives. In the first instance, it has been designed to be readable by people who are running small and medium-sized businesses as much as by people who run the big corporate enterprises and the national infrastructure. It is also designed to provide part of the background to the Government's initiatives on community resilience, so it should include common-sense advice on the kinds of things that you need to keep in your cupboard in order to deal with the impact of the sorts of things that happen all the time and which you cannot do very much to prevent.⁶⁸

4 The MoD and EMP

MoD resilience to EMP events

71. We were concerned to establish how resilient MoD equipment and processes would be against EMP events.

72. Written evidence from the MoD indicates that there are three main capabilities that rely on space-based assets:

- **Satellite communications (SATCOM).** SATCCOM and data networks enable the command and control of deployed forces and the timely exploitation and dissemination in intelligences data.
- **Position Navigation and Timing (PNT).** Precise PNT solutions derived from the US Global Positioning System (GPS) enable the orchestration of complex military operations while reducing the risk of collateral damage and fratricide.
- **Earth Observation (EO).** Earth Observation capabilities (most of which are derived from allies and commercial providers) provide the necessary strategic indicators and warnings, and the intelligence to support operational and tactical planning.⁶⁹

The MoD told us that the majority of these capabilities are hardened or augmented “to withstand a reasonable worst case space weather event”, and that defence procurement standards require “appropriate hardening against nuclear weapon effects, including EMP” but notes that severe space weather or HEMP “could degrade the ability of [Earth Observation] satellites to collect and disseminate data in a timely manner”.⁷⁰

73. Although the MoD were confident that the satellite services and the positioning, navigation and Earth observation systems were reasonably protected, we were worried about other, terrestrial, equipment. The Minister said that generally defence equipment was more resilient and hardened than its civilian counterparts but that:

it would be unrealistic, bluntly, to seek to harden all military assets against a threat of space weather and EMP, but as the overall likelihood of a severe damaging event is relatively low in our view, we focus our attention on what we consider to be a critical subset of systems.⁷¹

David Ferbrache explained other precautions taken in case of the failure of equipment:

We also put quite a bit of time and effort into reversion modes and fall-back. GPS is the classic. It’s a military system anyway—US military satellites. It has a degree of resilience against a lot of the space weather scenarios we have talked about. But we also routinely practise reversion modes. So, yes, we do still train people in maps and compasses—good old-fashioned navigation. We also train them in how to use

69 Ev 21

70 Ev 22

71 Q 101

inertial navigation systems, and we routinely practise GPS jamming. As Mr Harvey has set out, we tend to include electronic warfare routinely in our exercises and training. We play through a lot of degradation modes and reversion modes. I am not sanguine; the threat will evolve over time.⁷²

74. HEMP is, of course, a different matter from space weather. David Ferbrache explained that hardening the equipment was the second line of defence after prevention:

We are very much focused on trying to ensure that that event does not occur in the first place, which is all about counter-proliferation action to prevent the acquisition of nuclear weapons or ballistic missile capabilities. Deterrent capability is one of the areas that we make absolutely certain is protected against EMP, in terms of our ability then to retaliate against such an aggressive act. Then we go into hardening of key strategic communication systems, too. It is a threat we are keeping a weather eye on, to use that phrase, because the concern downstream is that we may well see a proliferation of both nuclear weapons capabilities and appropriate launch systems.⁷³

75. In view of the importance of the nuclear deterrent, we sought assurance that the Nuclear Firing Chain was secure. The MoD assured us that:

As part of the UK's strategic nuclear deterrent, the Nuclear Firing Chain is designed and maintained to assure the UK's ability for retaliatory action should we be subject to a nuclear attack, and this has been the case since the days of the Cold War.

The MoD audits the integrity of the Nuclear Firing Chain regularly and acts to ensure that it maintains the highest possible standards, but it would not be appropriate to comment on specific measures here.⁷⁴

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

Responsibility in the MoD

77. It became clear in the course of our inquiry that there is some confusion within the MoD as to who has responsibility for matters relating to resilience to or development of EMP weapons, nuclear or otherwise. There was some disagreement between them and the Committee on appropriate witnesses. When we invited the MoD's Chief Scientific Adviser to give oral evidence to this inquiry we were told that he had no responsibility in this area,⁷⁵ despite his stated role being to "provide strategic advice to Defence on science and technology in support of military operations and future capabilities".⁷⁶ Subsequently, during the oral evidence session, it became clear that the Minister and Government Chief

72 Q 101

73 Q 90

74 Ev 51

75 Ev 55

76 Supplementary Memorandum from the Government to the House of Lords, Science and Technology Committee, Third Report of 2009–10, *Setting priorities for publically funded research*, HL 104-II, p 54

Scientific Adviser Sir John Beddington, and perhaps even Mark Welland himself, were of a different view, and that Mr Welland would have been an appropriate witness.⁷⁷ The Minister apologised for any misunderstanding.

78. 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.

79. We asked the MoD if, when it acquired information about a particular vulnerability in the wider infrastructure it passed the information on to those responsible for civil infrastructure. Mr Harvey said “we do share it with the rest of government. It is also the case that a lot of industries will have some direct information coming to them on this”.⁷⁸ David Ferbrache added that “we have had a reasonably good understanding of the effects of EMP for some time and that has been reflected in a complete suite of defence standards, which are taken up by respective industries as well”.⁷⁹

80. 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.

MoD role in responding to an emergency

81. The Ministry of Defence does not expect to play a primary role in the case of a national EMP event, for instance in restoring the National Grid. Nonetheless, a severe space weather or HEMP event is likely to meet the definition of an “emergency” under the Civil Contingencies Act 2004 as “an event or situation which threatens serious damage to human welfare” or “war or terrorism which threatens serious damage to security”.⁸⁰ In this case, the armed forces might be called upon to assist as with any other major emergency. Nick Harvey said:

As a national asset, defence would not expect to be called on, except in the case of very large-scale incidents. In that sense, if something did kick off, rather as Mr Tesh indicated earlier, we would expect to be brought into the equation through the COBR process. The scientific community shares information across Departments all the time. I am sure that it is keeping an eye on the evolving picture.⁸¹

82. 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.

77 Qq 100 and 105

78 Q 98

79 Q 96

80 Ev 20

81 Q 105

5 Satellite security

83. Space-based infrastructure such as satellites is particularly vulnerable to space weather events as highlighted by the evidence from Research Councils UK.⁸² ⁸³ The growing reliance on satellite infrastructure for a range of services, notably position, navigation and timing (PNT) services which provide global navigation satellite systems (GNSS) such as the US Global Positioning System (GPS) means that this vulnerability is potentially very problematic:

There are more than 600 satellites in orbit providing essential services [...]. During a space weather event the Van Allen radiation belts can intensify 10,000 fold or more resulting in satellite charging and damage to electronic components. Solar energetic particle events can also reduce solar array power and satellite lifetime. Three satellites in the radiation belts were damaged in one event in 1994, leading to serious loss of service, and satellite losses occurred in 1997, 1998 and 2003 during the last solar cycle.⁸⁴

The planned European GPS system under project Galileo, by providing an alternative satellite navigation system will provide some additional measure of protection, through redundancy to existing GNSS.

84. The importance of PNT services were highlighted by a recent report by the Royal Academy of Engineering:

A failure or loss of signal due to some outside influence can result in a range of consequences depending on the application; in a telecommunications network, a small loss in the efficiency of data handling may occur while the system “freewheels” until a signal is restored; in a surveying application where timing is not critical some delays may occur before the survey can be properly completed. In such applications, a temporary loss of GNSS signals might be considered an inconvenience. However, where systems are used in safety of life critical applications, the consequences can be more severe.⁸⁵

85. The UK Armed Forces rely on satellite services for a wide range of operational capabilities, such as communication systems, navigation etc. However, there are well established ways of reducing both the vulnerability of satellites themselves and GNSS networks to the effects of space weather. For instance, Research Councils UK suggest that “satellite operators attempt to mitigate the effects of space weather by hardening chips against radiation and by using multiple circuits so that a malfunctioning circuit can be outvoted by ones that are operating correctly.”⁸⁶

82 Ev 29

83 Our Specialist Adviser told us that in fact banking systems avoid using satellite communications because they are too slow and that only a very small proportion of internet traffic uses them. Also, internet uses satellite only where other systems are not available.

84 Ev 30

85 *Global Navigation Space Systems: reliance and vulnerabilities*, Royal Academy of Engineering, March 2011

86 Ev 31

86. 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.

6 Responsibility in Government

87. The House of Commons Science and Technology Committee held an inquiry last year into “scientific advice and evidence in emergencies”. One of its case studies for the inquiry was severe space weather. Its Report recommended that a Lead Government Department be identified specifically in relation to severe space weather. The Committee suggested this would be announced alongside the 2011 edition of the National Risk Register, which has yet to be published. It noted:

A severe space weather event could have impacts cutting across Departments’ responsibilities and therefore coordination is important in preparation for a potential emergency. We note with concern that the Royal Academy of Engineering has stated “there is little indication of any coordination across Government.”⁸⁷

88. In the course of our inquiry we have found it difficult to establish the lines of responsibility in relation to this matter. The Cabinet Office handles civil contingencies, and its Centre for the Protection of National Infrastructure (CPNI) has responsibility for providing “integrated security advice (combining information, personnel and physical) to organisations which make up the national infrastructure.”⁸⁸ However, the CPNI’s website does not list space weather or EMP threats as particular concerns. Energy security as a whole lies within the Department for Energy and Climate Change, terrorism within the Home Office, and the use of and defence against such potentially devastating weapons within the MoD. As a result our witness panels were drawn from several Departments and there was more than usual difficulty in assembling them. We are grateful to those who, like the Chief Scientific Adviser, altered their diaries at short notice to accommodate us.

89. Asked where responsibility would lie should there be a severe EMP event, Dr Kerridge of the British Geological Survey responded “the difficulty here is identifying a lead Department that would take responsibility for the overall risk. There probably not only one, because it goes across MoD, transport and, for the National Grid, DECC. That is a difficulty.”⁸⁹ He added:

In terms of the SEIEG [Space Environments Impact Expert Group] we have self-organised and said “this is an important issue”, in a sense we need a customer to tell us to do the work. At the moment we are working on the basis of “we think it is a good idea and we ought to co-ordinate”. Of course there will be difficulties to the extent to which, say, the private sector remains in something that is not driven in some way by government.⁹⁰

90. For the Government, asked which Government department would take the lead in the event of a severe electro-magnetic storm, natural or man-made, John Tesh said:

87 Science and Technology Committee, *Scientific Advice and Evidence in Emergencies*, para 40

88 www.cpni.gov.uk

89 Q 54

90 *Ibid.*

If we are talking about what we would call a level 2 crisis, which is one where the impacts are widely spread, then the action moves into the Cabinet Office Briefing Rooms—COBR—and one of the functions of the Civil Contingencies Secretariat would be to advise the Prime Minister on who he should appoint as the lead Government Minister for that crisis. Ordinarily, we would have pre-identified Government Ministers, depending on the nature of the crisis, and the main criterion is where the largest impact falls. So if this was something which largely hit the electricity generating industry and sector, then DECC would probably be the person in the frame. If it was something that affected communications rather more, then another Government Minister would be identified. If it is entirely unclear who should be in the lead, then there is a system for appointing a Minister without departmental responsibility, simply to come in and deal with that particular crisis.

The system is well rehearsed, and usually functions on the basis of pre-identified lead Government Ministers. In the case of space weather, we have yet to get to that point, because we have been doing a lot of work with SEIEG—the group that Sir John Beddington was talking about—to identify exactly what the impacts of a severe space weather event would be. When we have done that work, we will be looking to identify lead Government Ministers either overall or, as is perhaps more likely in this case, for particular aspects of the crisis. Then we will have the whole thing pre-identified. As it is, we will be working off the evidence that we have received so far to identify any Government Minister.⁹¹

He hoped that a lead Department would be identified “within the next two or three months.”⁹²

91. Scientific advice would be co-ordinated by the Chief Scientific Adviser. He said:

In the event that we move to some sort of Cabinet Office Briefing Room response, because it is of that degree of severity, I would put together a scientific advisory group in emergencies, the acronym for which is SAGE. This would involve the appropriate people from within Government, the list of Rutherford Appleton, the Met Office and so on that I referred to, and some of the chief scientific advisers—those from the MoD, DECC and arguably Transport. It would also have some independent scientists from industry and academia, who would be involved. SAGE would then convene and questions would be posed by whoever is chairing COBR at the time, and we would gather in emergency sessions. I would bring the scientific advice, either on mitigation or, if we had an alarm that a problem was coming, advice on how we would deal with it. That mechanism is in place and it is truly cross-Government.⁹³

When we suggested that the system appeared chaotic, Charles Hendry, Minister of State at the Department of Energy and Climate Change, replied “in my experience, this is one of

91 Q 83

92 Q 89

93 Q 84

the most seamless examples of Government working, rather than there being any sense of chaos in it”⁹⁴.

92. 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.

7 Conclusion

93. While successive Governments, both in the UK and elsewhere, have long been aware of the threat to national infrastructure from military EMP it is only in the last two years that there has been serious work on the risks from space weather.

94. Space weather can, to some extent, be forecast, and when it can be forecast some mitigating action can be taken. More work is necessary, both on forecasting capabilities and on establishing more exactly the likely effects. While the scientific community is doing much work on this, it is important that Government- and indeed governments, since this is an international problem- take a still more active role in driving it forward.

95. Much of the current mitigation strategy involves pre-emption and quick recovery rather than protection or prevention, but more work is also needed on how equipment may be protected, either on installation or retrospectively, to withstand the effects of severe space weather

96. While mitigation of the effects of severe space weather is, in the first instance, for the providers of the services likely to be affected, the effects of a High Altitude Electro-Magnetic Pulse Event, as a result of a nuclear weapon exploded at high altitude, would be so serious that only government action could be expected to mitigate it. We are concerned that the Government does not regard this as currently being a high risk and urge that more vigorous action should be taken to prepare for such an attack. Similarly, an urgent reassessment should be made of the risk from non-nuclear EMP attack on vital national facilities.

97. 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.

Formal Minutes

Wednesday 8 February 2012

Members present:

Mr James Arbuthnot, in the Chair

Mr Julian Brazier

Sandra Osborne

Mr Jeffrey Donaldson

Sir Bob Russell

Mr Dai Havard

Bob Stewart

Penny Mordaunt

Ms Gisela Stuart

Draft Report (*Developing Threats: Electro-Magnetic Pulses (EMP)*), proposed by the Chair, brought up and read.

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

Paragraphs 1 to 97 read and agreed to.

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

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

Written evidence was ordered to be reported to the House for printing with the Report with written evidence reported and ordered to be published on 9 and 29 November 2011.

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

[Adjourned till Wednesday 22 February at 2 p.m.]

Witnesses

Wednesday 9 November 2011

Page

Professor Richard Horne, British Antarctic Survey, **Dr David Kerridge**, British Geological Survey, **Avi Schnurr**, Chairman and CEO, EIS Council, and **Chris Train**, Network Operations Director, National Grid Ev 1

Nick Harvey MP, Minister for the Armed Forces, Ministry of Defence, **Charles Hendry MP**, Minister of State, Department of Energy and Climate Change, **Sir John Beddington CMG, FRS**, Chief Scientific Adviser to HM Government, **David Ferbrache**, Head of Cyber, Ministry of Defence, and **John Tesh**, Deputy Civil Contingencies, Cabinet Office Ev 10

List of written evidence

1	HM Government	Ev 20
2	National Grid	Ev 25
3	Research Councils UK	Ev 28
4	Avi Schnurr, Chair and CEO, Electronic Infrastructure Security Council	Ev 41
5	Professor Richard B Horne, British Antarctic Survey	Ev 44
6	International Electrotechnical Commission (IEC) Subcommittee 77C	Ev 45
7	Royal College of Physicians	Ev 46
8	Peter Taylor, Ethos Consultancy	Ev 47
9	The United States Federal Energy Regulatory Commission	Ev 48
10	Met Office	Ev 50
11	Ministry of Defence	Ev 51
12	Charles Hendry MP, Minister of State, Department of Energy & Climate Change	Ev 53
13	EMPact America	Ev 54
14	Email from Parliamentary Clerk, Ministry of Defence, to Clerk of the Defence Select Committee	Ev 55

List of Reports from the Committee during the current Parliament

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

Session 2010–12

First Special Report	The Comprehensive Approach: the point of war is not just to win but to make a better peace: Government response to the Committee's Seventh Report of Session 2009–10	HC 347
Second Special Report	The contribution of ISTAR to operations: Government response to the Committee's Eighth Report of Session 2009–10	HC 346
Third Special Report	Ministry of Defence Annual Report and Accounts 2008–09: Government response to the Committee's Fifth Report of Session 2009–10	HC 353
First Report	The Strategic Defence and Security Review	HC 345 (HC 638)
Fifth Special Report	Defence Equipment 2010: Further Government Response to the Committee's Sixth Report of Session 2009–10	HC 898
Second Report and First Joint Report	Scrutiny of Arms Export Controls (2011): UK Strategic Export Controls Annual Report 2009, Quarterly Report for 2010, licensing policy and review of export control legislation	HC 686 (Cm 8079)
Third Report	The Performance of the Ministry of Defence 2009–10	HC 760 (HC 1495)
Fourth Report	Operations in Afghanistan	HC 554 (HC 1525)
Fifth Report	Ministry of Defence Main Estimates 2011–12	HC 1373 (HC 1528)
Sixth Report	The Strategic Defence and Security Review and the National Security Strategy	HC 761 (HC 1693)
Seventh Report	The Armed Forces Covenant in Action? Part 1: Military Casualties	HC 762
Eighth Report	Ministry of Defence Annual Report and Accounts 2010–11	HC 1635
Ninth Report	Operations in Libya	HC 950

Oral evidence

Taken before the Defence Committee on Wednesday 9 November 2011

Members present:

Mr James Arbuthnot (Chair)

Mr Julian Brazier
Mr Jeffrey M. Donaldson
John Glen
Mr Dai Havard

Mrs Madeleine Moon
Sandra Osborne
Bob Russell
Ms Gisela Stuart

Examination of Witnesses

Witnesses: **Professor Richard Horne**, British Antarctic Survey, **Dr David Kerridge**, British Geological Survey, **Avi Schnurr**, Chairman and CEO, EIS Council, and **Chris Train**, Network Operations Director, National Grid, gave evidence.

Q1 Chair: Thank you all very much for coming to give evidence. We are holding an inquiry into developing threats to the electronic infrastructure. You are most welcome to the Committee.

I must begin by shaping expectations. This will be a brief evidence session, and this will be a one-evidence-session inquiry. During the course of this morning, I am afraid that several members of the Committee will have to go out to ask questions elsewhere. Nevertheless, I believe, as do several other Committee members, that this is an extremely important issue, and its importance is not limited by the amount of oral evidence we will be able to take this morning.

We will need to be crisp in our questions, and I would be grateful if you could be crisp in your answers. Do not feel you need to answer every question, unless a question is addressed to you or you have a particular knowledge of it. May I begin by asking you to introduce yourselves? Mr Schnurr, would you like to begin?

Avi Schnurr: I am Avi Schnurr. I am the co-ordinator of the electric infrastructure security summit process, which has been working to bring together a number of nations and allies—

Chair: Can I ask you to speak up, please?

Avi Schnurr: I am Avi Schnurr, the co-ordinator of the electric infrastructure security process—the international framework that has been working to bring countries together at the governmental level to consider these issues. I am also the CEO and chairman of the EIS Council.

Q2 Chair: And EIS stands for?

Avi Schnurr: Electronic Infrastructure Security.

Chris Train: I am Chris Train, Network Operations Director at National Grid. I am responsible for the real-time operation of the electricity transmission grid and the gas transmission grid.

Professor Horne: I am Richard Horne. I am a scientist at the British Antarctic Survey, which is part of the Natural Environment Research Council. I am also an honorary professor at the University of Sheffield. I am here as a scientist with particular expertise in the space aspects of space weather, and I

also lead an international project called SPACECAST, which helps forecast space weather for satellites.

Dr Kerridge: I am David Kerridge from the British Geological Survey, which is also a component body of the Natural Environment Research Council. I am a director of geoscience research there and have a particular responsibility for natural hazards. My background is in geomagnetism, where I have worked on applying science to real-world problems, including working with ScottishPower and National Grid on geomagnetically induced currents. I have been involved with two groups set up in the last year—the Natural Hazards Partnership, which is led by the Met Office, and the Space Environment Impacts Group, which has advised the Cabinet Office on the national risk assessment.

Q3 Chair: If a space weather event of the size of the Carrington event of 1859 were to occur tomorrow, what would be the likely impact on UK infrastructure, given that we are now much more reliant on electronic infrastructure than we were in the 1850s?

Avi Schnurr: I could offer a brief summary of the conclusions of the National Academy of Sciences NASA-funded study that addressed that question. It looked at the potential impact on the United States, but it is fair to say that, given its location, the conclusions about the United Kingdom would certainly not be better. The study's conclusion was that, in such an event, there would be a risk of cascading infrastructure failures, which would be caused by either immediate or short-term damage to extremely high-voltage transformers. The level of damage would be such that the study projected that there would be a risk of a black out affecting about 130 million people in the north-east of the United States. According to Joe McClelland, who is the director of the Office of Electric Reliability for FERC—the Federal Energy Regulatory Commission—his organisation has estimated, based on the study that it did to follow the NASA study, that the duration of the impact would be five to 10 years. That was associated with the long lead procurement times for these very large, expensive, extremely high-voltage transformers.

Q4 Chair: Is there anything there with which any of you disagree?

Chris Train: That is the analysis of the United States electrical infrastructure. There are some significant differences in the formulation of the infrastructure here in the United Kingdom. Having done a similar piece of modelling work following the concerns that were raised around a Carrington-sized event, we have been working along with our partners—the BGS and Manchester University and others—looking at what the potential impacts would be here in the UK.

Because of the meshed infrastructure here in the UK, we believe that the impact would not be as great here. The effort that we have been putting in has been around operation mitigations following a coronal mass ejection to understand how we might manage the system to minimise the impact of the potential in such an event. But I do not think that it would have the same catastrophic cascading effect that would happen in the United States because of the different nature of the configuration and development of the networks.

Q5 Chair: Have you worked out with the United States why you have come to such a different conclusion?

Chris Train: We have modelled the UK system. We have been in discussions. Have we finalised differences in modelling? I think that that is not the case. The second area is that there is more work to do, looking at the vulnerability of power generators and transformers. Through the Emergency Executive Committee, we are working with the power generators so that we can model the potential effects to their equipment so that we can get a better and fuller understanding of the total risk across the UK.

Q6 Chair: So that modelling has not yet been done?

Chris Train: That piece of modelling is under way at the moment.

Q7 Chair: So it has not yet been done?

Chris Train: It has not yet been done.

Q8 Chair: Mr Schnurr, do you agree with Mr Train that the impact in the United Kingdom would be less severe than in the United States?

Avi Schnurr: There is no question but that there will be differences. Incidentally, it is outstanding that this initial modelling was done. Perhaps I would be corrected if I were wrong, but, based on my conversations with some of the people who have been doing the work at National Grid, my understanding was that the modelling was done by an outside consultant based on some general assumptions that were made. That is an excellent start, and certainly in the United States similar work was done to begin thinking about the process.

A conversation similar to this occurred in the United States, which was mediated by National Labs and the Department of Homeland Security, which talked to transformer manufacturers. Again, some general assumptions were made about capability of transformers in terms of what is called GIC withstand—the capability of one of the big transformers to withstand ground-induced currents

that occur in such an event. After making some encouraging observations, the transformer manufacturer involved was asked, “Would you be willing to certify that all your transformers would survive such an event?” The response was, “To really understand what is necessary is to see whether or not there is magnetic flux leakage into support structures. What that magnetic flux leakage does in terms of its detailed thermal and electrical effects, we would have to review and model the as-built design for every transformer, the detailed electrical modelling and the very detailed finite-element thermal modelling.” At that time, they suggested it would cost \$50,000 per transformer.

Q9 Chair: I will have to stop you there. You are going into a realm of technology that we are not as fully up on as you are. I take it, though, that you do not fully agree with Mr Train that the United Kingdom would be more resilient than the United States.

Avi Schnurr: Based on my discussions with the people and their cursory review, they are concerned that the modelling that was done was sufficiently general that it would not capture the detailed transformer problems.

Q10 Chair: Thank you. That’s what I wanted to know. I need—

Chris Train: May I make some points on that? There are some—

Chair: All right, but be snappy in your points, if you would.

Chris Train: I’ll be very snappy. There are some fundamental differences in the US infrastructure. For example, it is a much larger geographical area, with long, long lines, which exacerbates the effect of the GICs.

Q11 Chair: GICs being ground-induced currents.

Chris Train: Yes, ground-induced currents, which are the thing that causes the problem with the transformers. By inducing a current into the core of the transformer, you heat the core of the transformer. Another critical aspect is the amount of loading that the transformer is under at the point where the GIC has an impact. The issues include the length of lines, size of geography and nature of the relationship within the substation. A higher frequency—60 Hz—network means a bigger impact than a 50 Hz network. Single-phase transformers are more vulnerable than multi-phase transformers. There are a number of fundamental differences in the architecture and topology of the UK infrastructure as compared with the US.

Chair: Thank you. I shall now hand over to Dai Havard, Vice-Chair.

Q12 Mr Havard: On the question of the UK’s assessment, you said earlier it’s fine. What about the recovery period, and what within that modelling takes account of the interrelationship between the UK infrastructure and supply and, say, France and what’s happening in the European countries? What’s the

9 November 2011 Professor Richard Horne, Dr David Kerridge, Avi Schnurr and Chris Train

recovery period as far as the UK assessment is concerned?

Chris Train: As far as the UK is concerned, we've looked at where our vulnerable transformers are, which is part of the detailed modelling work, along with the—

Dr Kerridge: BGS.

Chris Train: BGS. Thank you. I got my acronym and my mind the wrong way round. So we know which are our vulnerable transformers. As we've gone into solar cycle 24, we've increased our level of stockholding of transformers. If we lose a transformer, it takes in the order of two to three months to replace it, should we have a spare. Part of Avi's description concerns the need to go to manufacturers, which obviously have limited capacity.

The other aspect is that we operate to a level of resilience on the network, so we would not see the same level of disruption. We would expect that in some instances there could be minor disruptions for a number of months. In some instances, there may be no disruption at all. It depends on the size, scale and impact of the—

Q13 Mr Havard: Right, so if it's localised in the south-east of England and intense, it's one set of relationships; if it's in Scotland and more localised, it's a different thing. I understand that, but in terms of your general planning, what would be the recovery period? Could you have things back up and running normally in six months?

Chris Train: In two to three months.

Q14 Chair: How many spares do you have?

Chris Train: That is not a relevant question. The question is, what level of risk have we been assessing our spares holding against? We have modelled what we believe the level of risk to be, we have looked at the transformers that we have on the network and we have looked at our spares holding in order to manage that risk. In an integrated network, the routes and the route planning are the critical element, so if you have a problem at a node, you can move the energy flows through a different part of the network. The issue is what happens if you get a concentrated level on a particular node in the network. We believe that we have the right holding to manage that risk.

Q15 Ms Stuart: What percentage of your system is at risk?

Chris Train: Again, it doesn't work—

Q16 Ms Stuart: Single figures? Double figures? It does work—

Chair: Allow him to answer, because that may not work as a question.

Chris Train: In terms of numbers, you are talking of the order of 10 to 20 transformers out of a population of around 800 transformers on the network.

Q17 Sandra Osborne: Even so, it is quite difficult for a lay person to imagine the scenario that you are talking about. What is the likelihood of a large geomagnetic storm actually happening?

Chris Train: The others may comment on this, but obviously it is a high impact, low probability event that we are talking about. The Carrington event is believed to be somewhere around a one in 100-year or one in 150-year event.

Professor Horne: We have very big storms which occur every year; it is a question of the severity. For example, of magnetic storms of type moderate or larger, at a minimum we have something like 10 per year, which may rise to something like 60 per year during the solar maximum of the 11-year sunspot cycle. We measure the sunspot cycle—solar activity in terms of sunspots which has an 11-year cycle.

Of a storm of the size of the 1859 Carrington storm, the largest one on record, we really have no way of saying when such a large storm would occur again. The point is that something that big has occurred in the past; it can occur again in the future. That is where we are. It is perhaps more likely to occur during a period of sunspot maximum, which is what we are moving into over the next few years, but we cannot say exactly when.

Dr Kerridge: Could I add to that that we have been measuring the magnetic field happily for more than 150 years, so we have a good record of the types of event that occur? While the Carrington event is taken as the most extreme, it is in a family and the statistics of that family indicate, as Mr Train has said, that the Carrington event might be of the order of a one in 100-year or one in 200-year event, but the question we are talking about is risk assessment. We are describing the geophysical hazard there, and the other part of the risk is, of course, the change in vulnerability that we are addressing here. It is not only that Carrington can be taken as the reasonable worst-case scenario, but there is a family of other events that come into play when vulnerability increases.

Another project we are involved in involves Europe, because of the concern about the increasing interconnectedness between grids. So we have a European project looking at this.

As a point of information, GICs are geomagnetically-induced currents.

Q18 Chair: Geomagnetically-induced currents?

Dr Kerridge: Yes. In effect, we have a terrestrial transformer. There are intense currents in the magnetic storm about 100 km up, and they are linked to the ground by the magnetic field, which creates the electric field in the ground that then, when you put the conducting system on top of it, pumps the currents into that conducting system.

Chair: Thank you very much.

Q19 Sandra Osborne: What is your perception of the understanding of the risks within Government and the key industries that would be affected?

Dr Kerridge: There has been a great acceleration over the past year in the way we have addressed this problem. The event about a year ago, which Mr Schnurr led, led a few of us to sit down and say, "How can we better organise ourselves to address this problem?" As a result of that, in October 2010 we began something that we have termed the Space Environment Impacts Expert Group. At the same time,

there had been developing through the Met Office, the Ordnance Survey and the Environment Agency a natural hazards partnership. Those two things have developed quite quickly to look particularly at space weather and other hazards. Each of those has the support of the Civil Contingencies Secretariat in the Cabinet Office. So the latest development is to advise on the national risk assessment for the space weather and other hazards and to provide advice to the Government Office for Science.

Q20 Chair: Do you all agree? Okay.

Q21 Mrs Moon: I would like to move to high-altitude nuclear electromagnetic pulse bursts. What effect might one of those have on UK infrastructure?

Avi Schnurr: This is an interesting area, which is well understood. For 55 years, the United Kingdom, the United States and most of the developed world have spent an enormous amount of money on it in almost every military organisation. The United States Department of Defense has spent hundreds of billions of dollars addressing the issue over many years.

What is new about this, as you asked, is the question of the effect on civilian infrastructures. The best answer I can give is to summarise the conclusions of two different studies. The US Congress established an EMP commission, which provided an executive summary report after four years. At the end of eight years, two years ago, it provided a broader set of conclusions. Another study was done, supervised by Oak Ridge National Laboratory, with the Department of Energy, the Department of Homeland Security and FERC, with participation by review of the White House and the Department of Defense.

Both studies reached the same conclusions, basically. Even for a country the size of the United States, with one or two nuclear detonations—east coast, west coast, depending on how it was done—which could be relatively small, the impact would risk what they call cascading infrastructure failures, which would leave the United States without electrical power. We talk about severe space weather, relatively long-term, ground-induced or geomagnetically induced currents—that same effect is true with an EMP strike. There is an additional effect called an E1 pulse, which is very fast and can be thought of as equivalent to a lightning strike, but one that strikes everywhere in a broad geographic region, at higher intensity and much faster. So you cannot achieve protection with lightning rods, for example, for something like this. In the case of E1, in addition to the risk to transformers, which we have discussed, one has to try to reach conclusions, depending on the level and detail of analysis. In addition to the effect over a broad region, we would expect damage to electronics, computers and, most importantly, to command-and-control systems, because, these days, the electric grid and other critical electronic infrastructures are managed by many very complex command-and-control systems, with hundreds of computers in each.

The report from the commission and the technical report that I referred to both concluded that there would likely be sufficient damage to control systems to bring down the electronics. The scope of the

damage and the extent, relative to the labour available to go and find the problems, would be substantially more than could be resolved or recovered from in any normal sense. So we would expect the electric grid to go down and, concurrently, we would expect the failure of water supplies, fuel, transport, communications, medical care and financial services—one could go into more detail. It is not simply the control systems and the computer controls. There are also issues and concerns with relays and diagnostic systems. A small percentage of insulators on transmission lines are expected to fail, based on the research done. Unfortunately, given the number of insulators on each transmission line, even a small percentage would be expected to bring down most or all the transmission lines. There are many different kinds of failures with the electric system. Of course, you have a similar problem with computer-intensive infrastructures.

Chair: May I stop you for a moment? There may be things that one member of the panel says, with which others disagree. At the end of the session, once the evidence has gone up on the internet and you have had a chance to read it, please write to the Committee with any points of disagreement or clarification. That will save you—unless it is absolutely essential—during the course of the evidence session from saying, “That is absolute rubbish.” I did not see a facial expression indicating that what Mr Schnurr was suggesting was absolute rubbish.

Mrs Moon: Actually, I think it was a very full answer.

Q22 Mr Brazier: I have a question for Mr Schnurr that is right on the edges of what we are discussing. It seems there is an opportunity here. I remember in cold war days the importance of disconnecting the aerial from the radio, because of the threat of losing it through the electromagnetic pulse. Is this potentially a threat to all the air assets that happen to be in the air that do not have manual back-up systems? Would that include anything remotely piloted or fly-by-wire or whatever? Could an EMP simply fry the electronics of everything?

Avi Schnurr: It is a threat. I think it is less of a threat for, say, aircraft and aeroplanes than it might otherwise be, because typically you have the electronics surrounded by a conductor to some extent, due to the shell of the aircraft. Aircraft have to be protected to a degree against things such as radar signals, which are similar in extent. That said, even for aircraft and, given those considerations, there would be a risk that would have to be evaluated.

Certainly, you would expect the air traffic control system to go down. The nature of this effect is not that all electronics are destroyed or damaged; it is a percentage of electronics that will be destroyed or damaged. The problem tends to come when you have complex control systems in which, if you have a significant number of failures, the whole control system tends to fail. Our control systems were not designed as war fighters in general. Even for civilian infrastructures—aircraft and other things—if you have enough failures, everything simply stops working.

9 November 2011 Professor Richard Horne, Dr David Kerridge, Avi Schnurr and Chris Train

Q23 Mrs Moon: How much awareness of this potential risk is there among academics and key industries? Is it something that everybody is talking about, or is there only a niche interest?

Avi Schnurr: Perhaps this would be a good way to answer that. The day before yesterday I was in Brussels, where I was asked to give a briefing to the Assistant Secretaries-General of NATO. We went over this subject and one of them commented, "This is interesting, because on the one hand this is really an emerging threat, because we have not considered the impact on our civilian infrastructures. On the other hand, this is something we round this table are all familiar with, because EMP has been a military issue for a very long time."

So, there is very little awareness, unfortunately, even though—or perhaps because—it has been a military issue. The civilian sides of government and those concerned with civilian infrastructures have tended to have the luxury of simply saying, "EMP is a military issue. We'll leave it to the defence people." It is really only in the past three to four years that this has begun to be understood and discussed by the civilian sides of government as a serious threat. Incidentally, it is not so much the EMP itself; it is more the rapidly escalating vulnerability of our increasingly complex computer-controlled infrastructures.

Q24 John Glen: Given the potentially catastrophic impact, could you explain to what extent you feel these high-altitude EMP weapons could affect the UK? What is the credibility of this threat? There is a lot of analysis of what could happen, but could you explain how credible the threat is so that we can begin to understand the levels of risk that we are dealing with here? For many people it seems quite a remote and new topic, but it is this credibility of the threat that we really want to understand.

Avi Schnurr: I will point to two groups that I have mentioned previously. There was a NATO weapons of mass destruction conference in Bergen, Norway last summer. The conference opened with a statement by the Secretary-General of NATO, in which he made the point that NATO is concerned about the rapid growth in proliferation worldwide. There are several reasons why this is occurring and is expected to continue. In general, I would say, from the global perspective, that that is the risk. There was an attempt using sanctions, for example, to prevent both Pakistan and India from acquiring nuclear weapons—clearly that failed. There was such an attempt to prevent North Korea from acquiring nuclear weapons—that seems to have failed. We can see what is going on today around the world, and interest in nuclear power is a well known precursor of the development of nuclear weapons—it can be such a precursor. Interest in developing nuclear power has been increasing very rapidly around the world, including in the Gulf states and the Middle East, in states that are rather surprising because you would not expect such a need for nuclear power. In a global sense, the proliferation risk is here. In order to ignore this, I believe, from my perspective, one would have to reach a conclusion that it is unlikely that any enemy of the free world, the west, would ever elect to use this at any point in the foreseeable future. The

window to address it, to put protection in place, tends to be three to five years.

Q25 John Glen: So there isn't a credible threat now, but there could be in the near future?

Avi Schnurr: I would say that the issue to think about is: is there a possibility that in future we could have a rogue state, a transnational terrorist group or even a situation in which there is someone who may not be totally under the control of the Government? I will give you a specific example. The congressional EMP commission said that their primary concern was a ship-launched nuclear missile. They were more concerned about transnational terrorists than rogue nations. The reason, they said, is, "We know that transnational terrorist groups have ships. We know that they have missiles. Given a ship and a missile, it is a question of whether they can acquire a small warhead." We know that there are specific countries out there. Iran, for example, recently announced—I believe the announcement came from the commander of the Iranian navy—that they have already installed missile launchers on their logistics vessels and that they plan to base them in the Atlantic.

Is there a current concern? When you look at the consequence if, for example—given boats, given the potential will to use them and given missiles—a warhead somehow gets into the wrong hands, there would be a level of destruction that is referred to by the commissions that have looked at this in the United States as "affecting the continuity of the United States as a nation." If there was damage of this potential with a single bullet, or two bullets, so to speak—in the case of a country the size of the United Kingdom, I think, unfortunately, you would have to worry about one—even a short-range missile launched from a boat would be an extremely severe concern. The level of impact has to be looked at for current concerns.

Q26 Chair: The Government have given us some written evidence, which you will not have seen. In it, they say: "To generate more widespread damage from EMP, a nuclear warhead would have to be detonated at high altitude to generate the EMP from the interaction between the radiation from the weapon and the outer layers of the atmosphere. This could only be achieved by launching a device by missile to an altitude of several tens of kilometres. A limited number of States possess this capability." I think that that was intended to be reassuring. Do you believe that Iran is one of the states that possesses that capability?

Avi Schnurr: Yes. Unfortunately, the list of states and terrorist groups that possess that capability is far longer than would leave me in a state of comfort. Let's put it that way. We are talking about tens of kilometres, which is accurate. Not many tens of kilometres would provide a pulse that would cover the United Kingdom.

Q27 Chair: And Iran has that capability?

Avi Schnurr: Iran definitely has that capability. So does Hezbollah.

Q28 Chair: So does Hezbollah?

Avi Schnurr: Yes.

Q29 Chair: The Government say: “No non-State actors can currently produce an improvised nuclear device”—that I think is true—“and none are likely to be able to make a sufficiently robust warhead for missile delivery in the foreseeable future”, which I think may be true. Does Hezbollah have at least the missile delivery capability?

Avi Schnurr: It has the missile delivery capability. Al-Qaeda is believed to have ships and ship resources. There are only two things that stand right now between us—by “us” I mean the United Kingdom, the United States and other allies—and having this level of catastrophe. One is that although they have the ships and the missiles, terrorists groups and rogue nations do not today, necessarily, have access to nuclear weapons. That is a very thin boundary, because, for example, North Korea has nuclear weapons. Could North Korea sell its nuclear weapons? Could there be destabilisation in a state that has nuclear weapons? I could name a few. Those are things that could happen in the future. The other thin boundary is will. We are dependent on keeping any warhead of any size out of the hands of transnational terrorists or rogue nations and on their good will if they acquire them.

Q30 Bob Russell: Does the state of Israel have that capacity?

Avi Schnurr: The capacity to launch such a missile?

Q31 Bob Russell: You have referred to these other countries that may have or do have the capacity. Does the state of Israel have the same capacity?

Avi Schnurr: I have no unique information about Israel’s possession of nuclear warheads. In fact, I have no information. I would just depend on what is available in the public domain. In terms of missiles and boats, Israel has been reluctant to develop offensive missiles. Unlike some of the other countries, it has tended to depend on its air force. There is some talk these days, which you can see in the open press, about potentially moving more in the direction of developing such missiles, but historically Israel has not tended to develop them. I have no unique information.

Q32 John Glen: Is there not a gap in the theoretical scenario whereby all these things could come together: a rogue element within a state, which we are presumably tracking considerably all the time, acquiring a nuclear warhead and then being able to test and deliver it? To have all those things come together in one country is quite a long way away from the potential to happen. You have put together a very clear explanation of how all those things could come together, but, in practice, it would be difficult for all those things to align, given the level of scrutiny and given the technical complexity. This is not something that you can just knock together in the back yard, is it?

Avi Schnurr: I can point you to the congressional EMP commission again. The congressional EMP commission took testimony from all branches of the

US Government and elsewhere. Its conclusion is that it would not be very challenging for either a transnational terrorist group or a rogue nation to have a ship, which could look like a freighter, with a missile on board, but they would need to acquire a warhead. Unfortunately, analysts out there believe that over a number of years, given proliferation, their acquiring a warhead is not something that we can write off as a possibility. People have said, “How does one launch a missile with any accuracy from a freighter or a boat?”, but that overlooks the fact that with EMP, no accuracy is required.

Q33 Chair: Can I ask about the possibility of non-nuclear EMP weapons? They exist, do they not? How widespread are they?

Avi Schnurr: They do exist. The biggest issue with non-nuclear EMP weapons is that the complexity and threshold required to produce them is minimal, to say the most. At the summit meeting in Washington DC, for example, there were two Assistant Secretaries of Defence, a Deputy Under-Secretary and the Pentagon’s chief lawyer, all of whom expressed grave concerns over this risk—the non-nuclear EMP risk in particular, but the risk of EMP in general. The non-nuclear EMP risk is much shorter-range. However, that range, which could be 100 metres, a fraction of a kilometre or a kilometre—under certain circumstances, which I could discuss separately, it could be multiple kilometres—includes the risk of having a field strength that would be even greater, although limited in extent, than a nuclear EMP.

To summarise the capability, let me put it this way. We had a speaker at that summit who described, to the extent he was allowed to describe it, a device that he built from hardware he acquired from retail stores in the United States, which he had built into a van. As he put it, “I brought it on to an army base to test it, because it would not have been a good idea to test it in my garage where I built it.” The result of the testing was quite disturbing. The capability simply amounts to, again, the will on the part of a terrorist group—

Q34 Chair: But at shorter range.

Avi Schnurr: Much shorter range. It also depends on the will of an electronics engineer. There are such devices that exist; they were used recently by North Korea against South Korea to suppress communications. South Korea is developing very advanced non-nuclear EMP weapons, and it has agreed to convey the technology to the United Arab Emirates. China is suspected now to be looking at such devices, and one could go on.

Q35 Ms Stuart: Mr Schnurr has told us about his views on the commission that was set up in the United States to assess the risk from electromagnetic pulse attack, and I wonder what Messrs Train, Kerridge and Horne think the benefits of a similar study in the United Kingdom would be.

Chris Train: From the grid perspective, we understand the electronic threat through naturally occurring space weather. We have no assessment as to what the overall threat is, but you have to remember that there is a trade-off of costs, mitigations and

9 November 2011 Professor Richard Horne, Dr David Kerridge, Avi Schnurr and Chris Train

probability, so we would need an assessment of what level of threat we should be taking into account and whether, in the scheme of managing the threats to the infrastructure, that is actually a credible threat to attempt to mitigate.

Q36 Ms Stuart: I still bear the scars of being the duty Minister on the millennium change, when I spent years preparing for the disaster that never happened. Dr Kerridge.

Dr Kerridge: What we are doing and are capable of doing at the moment is describing the natural hazard. That means that we can run scenarios that are applicable to work that we can do with National Grid to look at the possible consequences of a range of events.

Another aspect of this is the ability to forecast events and to monitor the progress of natural events that take sufficient time from the sun to the Earth, and there is certainly a great deal of scope for improving our ability to forecast and to predict the impact of events. That is something that is currently being taken up through a US and UK collaboration, and there was a recent meeting in Boulder about it.

In operational terms, the National Oceanic and Atmospheric Administration's Space Weather Prediction Center is now co-operating with the UK Met Office on operational delivery, but behind that we have a great body of expertise in the UK that can be brought to bear to improve the skill of the predictive models and observations that are needed to make better forecasts. In the case of natural events, there are things that we can certainly do.

Professor Horne: I think there is another dimension here as well, which touches on both space weather and the effects of a nuclear detonation at high altitude, and that goes back to the 1960s when the USSR and the USA did their nuclear tests at high altitude. One thing that was found was that when they had an injection of high-energy electrons up into the earth's magnetic field, those electrons were trapped and then circulated all the way around the earth, and they presented an additional radiation hazard to spacecraft. Now, that was back in the early 1960s, and it also caused the damage and loss of something like three satellites at that time. So I think there is another dimension here—assessing the risk to satellites from a high-altitude nuclear detonation. In the same way, there is a need to do more work to assess the risk to satellites from natural space weather events.¹

Q37 Mr Havard: Can I ask you about preparedness, particularly in relation to the United Kingdom and where we are in this, for such an electromagnetic event—intentional or otherwise? What do you have to say about our preparedness? There is a lot of discussion about hardening different parts of the infrastructure and hardening various different things. Where are we in terms of our current preparedness?

Chris Train: In terms of naturally occurring space weather, we have a set of operational mitigations in place, which start with the better forecasting of space weather and increased understanding about the likelihood and any timing of impacts. We have a

number of operational measures that we can put in place, such as de-loading vulnerable transformers, spreading generation around the network and manning particular sites.

Hardening in itself is actually quite a challenge. There is talk of putting capacitance in the earth in order to block the GICs, but this is unproven. There are some difficulties peculiar to the design of the transformers in the UK compared with the US, which actually means that this would need a very close look at before such measures were considered. On the capability actually to roll that out, it would take an incredibly long period of time to do that. Once you harden an asset, all you are doing is moving the problem to the next asset.

Q38 Mr Havard: We have had quite substantial evidence from the Government, which will be published—you have not had the opportunity to see it—and it addresses some of these things and the processes and structures to try and co-ordinate and address them. It talks about defence and says, "Defence procurement standards direct that military equipment must have an appropriate hardening against nuclear weapon effects." This level of protection against space weather is involved in that assessment. But that is not necessarily true of the civil infrastructure that we are talking about, is it? So what is the position as far as retrospective hardening is concerned? This is an expensive exercise, is it?

Chris Train: It is an unproven exercise in terms of the technology.

Q39 Mr Havard: Therefore is it worth doing?

Chris Train: This first thing is that it would need proper research to determine whether it would be effective. Intruding in the asset causes other problems as well, so you might be mitigating the potential for a very rare event and triggering a more frequent event. So it needs very careful consideration.

Q40 Mr Havard: Professor Horne, what do you reckon?

Professor Horne: I can really only speak on the space side of things and the satellites.

Q41 Mr Havard: The space weather effects?

Professor Horne: And the space weather effects.²

Q42 Mr Havard: There are these 1, 2 and 3 categories—there is the initial thing that might come from a nuclear explosion, and then there is the second wave and the third wave. I cannot remember the exact terms at the minute. I am not a scientist. What do the standards that would be required terrestrially need to be to protect against natural causes, not necessarily category 1?

Chair: I think you have moved off the point about hardening.

Q43 Mr Havard: Well I want to know what the hardening is for and up to what standard you are going to harden things. How much money will you spend here in hardening infrastructure and against what?

¹ Ev 44

² Ev 44

Chair: Mr Schnurr?

Avi Schnurr: Perhaps I could add some elements to this. I very much agree with what Chris said. The current blockers, as they are often called, are an example of an approach that can be used for hardening, but testing is needed. We need to understand how well it works and we need to be sure that there are no undesirable other effects. I know that, for example, in the United States there are growing plans to do such testing. Some testing has already occurred on the part of developers. For example, ABB, I believe the largest transformer company in the world—certainly one of the largest transformer companies—has recently completed a prototype current blocker that it is proposing could be used to protect transformers. As a matter of fact today in Atlanta at a meeting of NERC, the capability of that prototype is being reviewed.

Q44 Chair: But what do you say about Mr Train's point that by hardening something you just move the problem on to the next asset?

Avi Schnurr: That is exactly the point. There are two things that need to be looked at. First of all, one needs to be sure of the transformer itself, so that while one blocks the current, one will not have a negative effect on the transformer. Secondly, in the United States this particular point that you made, Chris, is taken very seriously. As officials at FERC, the Department of Energy and Congress look at protecting the US electric grid, they are looking at doing it in a co-ordinated, planned fashion, so that as you begin to put hardening in place, you put it in place without temporarily increasing the risk to some components while you protect others. So when hardening is done it has to be done with that in mind, based on modelling that tells you, "Okay, if I'm going to harden the grid, this is the way to do it so as not to put at risk component A, which might be more sensitive than component B, when I first protect component B."

Q45 Mr Havard: This is a discussion about hardening the electricity supply, if I can describe it that way. Does this have effects on other forms of electronics? What are the things that need to be done by the telecommunications industry, for example? It uses electricity to do transmission, and there are other forms of electronics. Where are things being done other than the main grid as far as hardening is concerned? What is being done? Do we have resilience there and what do we need to do for that?

Avi Schnurr: There are many different areas in society where critical, even life critical, infrastructures depend on electronics.

Q46 Mr Havard: Yes, does this knock them out? I want to know what we are doing in the UK about dealing with our own infrastructures, whether it is telecommunication companies or all the people who use communications of various sorts in terms of our own utilities and others.

Chris Train: I can only comment on the electricity transmission network and the gas transmission network. We have talked about the transformer issues

in an EMP environment. Understanding the issues around the control systems would be quite critical.

Avi Schnurr: I could offer an example of some things that are going on in the United States. On the one hand, you have federal regulators and the Government level looking at this issue, but you also have some companies beginning to take independent action. For example, some companies, one in particular, have already made the decision that their next spare controller for their portion of the electric grid will be EMP and severe space weather-proof. Looking at that, I asked them, "What do you anticipate to be the cost impact on that particular installation?" They said, "Well, it looks like something in the neighbourhood of 5%."

Q47 Mr Havard: Are these technology advances introduced into the regular maintenance, repair and change programmes going to achieve what we want and provide us with the extra protection we require—the extra-hardened systems to protect us over time? Is that what we are doing?

Chair: It has not been said that we are doing anything.

Mr Havard: Maybe that is what we should be doing.

Chris Train: The first thing is to assess the threat, isn't it?

Q48 Bob Russell: Following on from that line of questioning, are those working on the national grid sufficiently informed of the risks we have been discussing to be able to cope with an unexpected event?

Chris Train: In terms of space weather, we have a set of procedures. We actively monitor space weather, we are doing all the work in terms of understanding the risks and impacts I was talking about earlier, and we have a set of procedures in place, which are well known and tested in the control room environment, to ensure that we can respond appropriately should we get a warning of a space event.

Q49 Bob Russell: So you feel you are sufficiently informed?

Chris Train: Yes.

Q50 Bob Russell: Is there sufficient awareness of this issue within Government? This is your opportunity to let the Government know.

Professor Horne: I think there is a growing awareness. As David said earlier, when we formed the Space Environment Impacts Expert Group last year, we approached and talked to the Cabinet Office. It welcomed the formation of the group, and it was very much aware of space weather as a developing threat. We also had great support from the Government Office for Science at that time. The awareness has really grown over the last few years. The research councils are also developing a much greater awareness. On the research front, there is now discussion between the Natural Environment Research Council and the Science and Technology Facilities Council to try to put together funding for research into space weather.

9 November 2011 Professor Richard Horne, Dr David Kerridge, Avi Schnurr and Chris Train

Q51 Bob Russell: That is obviously encouraging. To what extent, if any, is the work done by industry, the Government, research institutions and so on co-ordinated? Or is it not co-ordinated?

Professor Horne: I think we would say there needs to be more co-ordination. We have made a really good start. Last year, we had our get-together for the Space Environment Impacts Expert Group, and that was one of the first times we were able to bring people from the MoD together with people from the Met Office, scientists, the research councils and private industry—in this case, the aviation industry.³

Q52 Bob Russell: That is a good start. Are you saying there is room for improvement, or have you got a utopian situation already?

Professor Horne: I think that is something that needs to be built on, developed and guided. We need to develop more of a strategy in this country.

Q53 Bob Russell: Okay. That is the United Kingdom. How is this work being co-ordinated with that being done by other nations?

Avi Schnurr: Perhaps I could address that. I have two brief comments. I would measure awareness in the Government in terms of the actions that are taking place. There are two sides: severe space weather and EMP. In terms of severe space weather, I believe that things have begun to occur. Someone will need to make a decision on, for example, whether there should be a much more detailed level of analysis to go forward for the electric grid than what has already occurred, which strongly supports what has occurred. I think that is an excellent start, and maybe that is sufficient, but I feel that you may want to consider looking into a much more detailed level of analysis. That would be one measure of awareness.

A second example, moving on to EMP, would be: is there a process, a plan or workbooks that are being developed for different industries to look at what they would need to do to protect themselves against an EMP, either non-nuclear or nuclear? Certainly, in the United States, there is talk about that; that has not yet occurred. I do not know if that has happened here.

The assessment of cost impacts to do this kind of thing for EMP, for example, is again fairly modest, I think, based on the discussions we have had with some of the bulk power companies in the US. For example, we have asked them if they would be interested in cost recovery and if they would like Congress to provide for cost recovery. An example of their reactions is that these kinds of cost tend to fit within their existing logistics budgets.

Q54 Bob Russell: I suspect that one of the conclusions of this inquiry is that the Committee will be seeking to get a clear understanding of where the responsibility lies for protecting UK infrastructure from the hazards that we have been discussing. Are there any thoughts that you might like to put into that? For example, do you think that there should be one specific Minister to take a clear lead on these matters?

I am intrigued to know what title he or she would have.⁴

Dr Kerridge: If I may go back to an earlier point, you asked at what level in Government the awareness is. An announcement on space weather was made as part of the Cameron-Obama announcement following the recent visit, so it has reached and gained attention at the highest level.

On the question that you are asking now, when we looked at the national risk assessment as a group, we broke down the natural effects into 12 or 13 categories. The difficulty here is identifying a lead Department that would take responsibility for the overall risk. There probably not only one, because it goes across MoD, transport and, for the National Grid, DECC. That is a difficulty.

In terms of the SEIEG, where we have self-organised and said, “This is an important issue,” in a sense we need a customer to tell us to do the work, because it is an important issue, rather than being self-generated. At the moment, we are working on the basis of, “We think it’s a good idea, and we ought to co-ordinate.” Of course there will be difficulties to the extent to which, say, the private sector remains engaged in something that is not driven, in some way, by Government.

Chair: I hope that we can help you on that.

Avi Schnurr: If I may, I would just make the comment that sometimes it is helpful to step back. What we are talking about here are threats that are based on a large number of commissions, organisations—in the United States certainly—and some very impressive scientists. In terms of EMP, 55 years of work and many, many hundreds of billions of dollars spent all yielded the same conclusion: there is potential for an impact that would interfere with the continuity of modern society as we know it today.

When we are dealing with a threat and a risk of that magnitude, what level of assurance do we want to arrive at? We could sort of hope for the best, but I would recommend against that approach. If the approach is not to be, “Let’s hope for the best. It may destroy our society or damage it in a way that will take decades to recover, but we’ll be okay,” we have a very serious problem. That problem, as I think you mentioned, is that this cuts across all branches of Government. It will therefore be quite challenging to find a way to come to grips with it, because there will be so many other challenges from every Department where this has any impact that it may tend to be pushed aside.

The challenge will be to find some way for the Government to build within themselves some strong advocacy to address this in a way that takes cognisance of the level of risk. Certainly, if I am facing a risk that many scientists believe could be devastating, I would want to reach a level of insurance or assurance that I am handling it properly that rises much, much higher than for other events, which might be less devastating. There are governmental management issues to be addressed.

Chris Train: My response to that question is that it does start with a national risk assessment. From an

³ Ev 44

⁴ Ev 44

9 November 2011 Professor Richard Horne, Dr David Kerridge, Avi Schnurr and Chris Train

industry perspective, we have had a very good relationship and interaction and dialogue with the DECC officials as we have moved along this journey of developing the risk assessment around space weather and, alongside that, working with partners such as BGS on assessing what that risk means in terms of the infrastructure, and then through the E3C, the Energy Emergencies Executive Committee, collaborating with industry to understand what the wider effects are on it. For me, we have those mechanisms in place.

Q55 Chair: You have the assessments beginning to take place rather than the mechanisms in place?

Chris Train: The mechanisms for efficient dialogue. The full mitigations would follow on from those risk assessments.

Q56 Mr Havard: On the mechanism question, do you think that this should be part of the national security strategy discussion as much as anything else, and perhaps part of the considerations at the National Security Council? It should be in that stream as much as it is in civil discussions?

Chris Train: What I am saying is that from the energy industry perspective, our dialogue through DECC is an efficient dialogue.

Dr Kerridge: We are talking about the UK. I will just emphasise that within the UK there is an immense resource and experience in these questions in Government Departments, Government-funded agencies, the university sector and the private sector. There is an opportunity to provide leadership beyond the UK. Working together with the US on this matter is one strand; another important strand is in Europe, through the European Space Situational Awareness programme. It is quite important that we should be involved—which we are not currently—in the space weather component of it, because it will bring a great deal to bear on the wider problem.

Q57 Chair: I am afraid that we are going to have to bring this to a close. I am sorry, Professor Horne, but we have some more witnesses from the Government to tell us what they are doing. Thank you all very much indeed for your evidence this morning. I am sorry it has been so brief, but it may be the first of more inquiries. You never know.

Examination of Witnesses

Witnesses: **Nick Harvey MP**, Minister for the Armed Forces, Ministry of Defence, **Charles Hendry MP**, Minister of State, Department of Energy and Climate Change, **Sir John Beddington CMG, FRS**, Chief Scientific Adviser to HM Government, **David Ferbrache**, Head of Cyber, Ministry of Defence, and **John Tesh**, Deputy Director, Civil Contingencies Secretariat, Cabinet Office, gave evidence.

Q58 Chair: Welcome to this evidence session on developing threats to electronic infrastructure. I am sorry that this is all so truncated, but we are grateful to you all for coming. I must say to both Ministers that we will not be able to call you Minister because we will get confused, so we will call you Mr Harvey and Mr Hendry. Will you all introduce yourselves?

Nick Harvey: I am Nick Harvey, Minister of State for the Armed Forces.

Charles Hendry: I am Charles Hendry, Minister of State for Energy.

Sir John Beddington: I am Sir John Beddington, Government Chief Scientific Adviser.

John Tesh: I am John Tesh, Deputy Director, Civil Contingencies Secretariat, Cabinet Office; National Risk Assessment.

David Ferbrache: I am David Ferbrache, Ministry of Defence lead on Cyber and Space Policy matters.

Q59 Chair: Thank you all for coming. As you can see, there are as many witnesses as there are members of the Committee. Inevitably, we clash with other activity in Parliament, which means that we will need to be brief. You don't have to answer every question. In fact, I would rather you didn't. I thank you, Sir John, in particular for changing your arrangements today to be able to make it to this evidence session. I shall start with the recognition of whatever threat there is, and with the higher altitude nuclear electromagnetic pulse weapon event. What estimation has been made of the potential impact on the UK infrastructure of such an event? We are talking about

nuclear weapons, so it might seem appropriate to go to—well, whichever of you would you like to begin. Mr Harvey, would you like to begin?

Nick Harvey: Yes, by all means. We have addressed this somewhat in our written evidence to you. Clearly, we recognise the threat both of a nuclear attack and high-altitude electromagnetic effects. We take these very seriously, and in threat terms, we view them in more or less equivalent terms. It is certainly viewed as a top-level threat, and recognised as such in the security strategy. I do not know whether David Ferbrache would like to add anything.

David Ferbrache: I am happy to. One of the keys for us is to actually put the threat in context. We probably need to separate the elements a little as well. The event that is likely to have the greatest impact is an extra-atmospherical high-altitude nuclear burst generating an EMP. To achieve that, certain things have to happen. Obviously, you need to have a country with nuclear weapons capability, able to “ruggedise” that nuclear weapon for delivery by the ballistic missile system, and to have a ballistic missile—

Q60 Chair: Ballistic missile?

David Ferbrache: A ballistic missile, which is capable of putting that into high-altitude detonation at over 30 km above the earth's service, and even then, it has relatively localised hundreds of kilometres' effect. To have an effect over a large area like the continental United States or all of Europe, you need to get it to 400 km in altitude. At the moment, we

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

assess that very few states—that is, well-established nuclear weapons powers—have that capability. If we took a country such as Iran, they would have to have ballistic missiles with the appropriate range. They do not currently. They would have to have a credible nuclear weapon capability and they would have to have the ability to marry those two together and detonate them at altitude.

Q61 Chair: You said 400 km.

David Ferbrache: Up to 400 km.

Q62 Chair: Whereas in your written evidence you say that that could only be achieved by launching a device by missile to an altitude of several tens of kilometres.

David Ferbrache: As your altitude increases, the area of the earth you can impact using that electromagnetic pulse also increases, so at lower altitude you may only be talking of hundreds of kilometres of effect. As you get up to 400 km, you are talking potentially thousands of kilometres.

Q63 Chair: So a bad effect could be achieved by, say, 30 km.

David Ferbrache: Yes. The second category of your threat is when you start looking at terrorist use or, alternatively, the ability to explode a nuclear weapon at ground level. That is a very different scale of effect. You are talking short-range EMP and in most cases the blast and thermal radiation fallout is actually a greater concern.

Q64 Chair: Could such a weapon be launched from a ship?

David Ferbrache: It could be, but, again, it detonates at low altitude; hence the effect is actually quite localised compared to the worst-case scenarios of the high-altitude nuclear weapon exploding.

Q65 Chair: Why would it detonate at low altitude?

David Ferbrache: Because, again, unless you had a ballistic missile that was capable of reaching those sorts of altitudes—

Q66 Chair: So 30 km.

David Ferbrache: Exactly.

Q67 Chair: Could, say, Iran, launch a ballistic missile from a ship up to 30 km?

David Ferbrache: No, not currently.⁵

Q68 Chair: When you say this could only be achieved by launching a device by missile to an altitude of several tens of kilometres, a limited number of states possess that capability. Is Iran one of those states?

David Ferbrache: Our assessment at the moment is that Iran does not possess the capability to detonate a nuclear weapon at altitude.

Q69 Chair: No, that was not what I asked. Could Iran launch a device by missile to an altitude of several tens of kilometres?

David Ferbrache: We do not believe so. We keep that threat under assessment, so our defence intelligence works with allies to monitor Iran's programme in terms of both nuclear weapons and ballistic missile capabilities.⁶

Q70 Chair: Could North Korea?

David Ferbrache: We do not believe that is the case.

Q71 Chair: Mr Harvey, would you like to add anything to this?

Nick Harvey: No. I think that covers our reading of the threat.

Q72 Chair: Is there a possibility of a non-nuclear EMP attack? Is it considered a genuine threat?

Nick Harvey: It is certainly considered a potential threat. It is not considered a particularly likely one, certainly in the foreseeable future; but we keep that constantly under review. It is a material risk that we need to consider, but we do not think there is any imminent likelihood or threat from it. Again, Mr Ferbrache may want to add to that.

Q73 Chair: Mr Ferbrache, how long do you think, before Iran has the capability that you say it does not have at the moment, to launch a weapon to the relevant height?

David Ferbrache: I am cautious about speculating, as you might expect, Mr Chairman, because there are a number of different elements to that intelligence assessment. We keep it under track, and over the next decade, we can see that it might have the capability to do so, both in terms of ballistic missile programme development and the imponderable for us, which is how close is Iran to the development of a nuclear weapon at this stage. When the Foreign Secretary made his statement to the House on 29 June, he referred to his concerns about the development of Iranian ballistic missile capabilities, which might arrive at a point where they could deliver such a nuclear weapon.

Q74 Chair: One other thing you said in your written evidence, which I want to pick up, is that no non-state actors can currently produce an improvised nuclear device and none are likely to be able to make a sufficiently robust warhead for missile delivery in the foreseeable future, but states have been known to provide non-state actors with weapons, have they not?

Nick Harvey: At the moment, the MoD is not aware of any state or non-state actor intent to attack us in that way, but there is certainly evidence of growing awareness of non-nuclear EMP—

Q75 Chair: Sorry; I've changed the subject. States have been known to provide non-states with weapons, yes?

Nick Harvey: Yes.

⁵ Ev 51

⁶ Ev 51

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

Q76 Chair: So if a state developed a nuclear weapon, it could provide it to a non-state.

Nick Harvey: It could.

Q77 Mr Havard: Mr Harvey, you were going to say something about whether non-nuclear technology is in the hands of non-state actors.

Nick Harvey: We do not believe at the moment that there is anyone with both the intent and the capability to do this, but we are aware that there is a growing interest in it and a growing awareness of it. As with the risk of cyber-attack by terrorists, we keep a watching brief for any intelligence that indicates a terrorist intent to adopt new methods of attack; but, frankly, our main concern remains terrorist use of conventional explosives or their possible acquisition of CBRN weapons. Those things are a more immediate concern.

Q78 Chair: Why?

Nick Harvey: Because it would be more straightforward for them to wreak havoc with either of those than it would be for them to get into these other realms.

Q79 Chair: You estimate that the likelihood of a space weather event in the next five years is moderate to high. Do I gather that you feel it would have the same effect or much the same sort of effect as a high-level nuclear event? Sir John Beddington, do you want to answer that?

Sir John Beddington: Yes. First, may I go back to that frequency estimate? These estimates are pretty uncertain. What that estimate is saying is that it's not likely to be once in 10 years or once in 1,000 years; it's somewhere between those. It is quite an uncertain estimate, because all we have to go on essentially is historical information on the frequency of these events. Some of the information comes from, as it were, secondary sources, such as ice cores and so on. So the inference is not brilliant. We have had pretty good records since the middle of the 19th century and we know roughly the frequency. That gives you an idea of the answer.

In terms of severity—perhaps Mr Tesh will expand on this—the way we have been trying to look at this risk has been to ask what a reasonable worst case is. We feel that a reasonable worst case in this context is probably something similar to the so-called Carrington event, which occurred at the tail end of the 19th century. We are using that event in terms of our assessment of a reasonable worst case. That involved a combination of things. We generally feel it's a relatively low probability, but not to be discounted. The effects are similar, but are likely to be significantly lower in scale than a nuclear device exploded at altitude, as David has indicated.

I'll describe the sort of analysis that we've been doing. I believe you had some of the National Grid people in front of the Committee. We asked them to look at the issue from the point of view of our having this reasonable worst case of a space weather event, and they are indicating—I guess this is well known to you now—that in the UK, something of the order of eight or nine transformers might be affected.

In terms of the satellite industry, part of it will depend on whether you get reasonable early warning of the event, so that you can make some adjustment, and indeed that is the same for the National Grid, but perhaps, John, you want to expand on the way you actually assess that reasonable worst case.

John Tesh: The reason we chose the Carrington event was that it seems to be representative of the most extreme manifestation, according to the records that exist, of all three aspects of the solar weather risk, which is partly the electromagnetic side, partly solar radiation storms and partly solar flares. They all affect different parts of different types of infrastructure in different ways, so we set up a group of scientists—I think you've been talking to some of them; the leader of them is Mike Hapgood from the Rutherford Appleton Laboratory—to work with industry to try to work out what the impacts would be of each of those different effects of solar weather, and to start by confirming that it's reasonable to work off the Carrington event as the reasonable worst-case manifestation of it.

Sir John Beddington: I might add that there is a rather awkward acronym SEIEG, which stands for the Space Environment Impacts Expert Group, led by Rutherford Appleton Laboratory, with the British Geological Survey, British Antarctic Survey, QinetiQ, SolarMetrics and the Met Office as members. That group is working closely within the Cabinet Office's orbit. In my role as Chief Scientific Adviser, I have met the group and provided a critical-friend challenge to some of these things. It is fair to say that there is a fair bit of work in progress.

I will also allude to some of the co-operation with the USA. I visited a meeting on this issue at the White House earlier this year. We met most of the key agencies in the USA, and the European Space Agency was also present. Following that, we agreed there was a need to enhance the co-operation on space-weather effects between ourselves and the USA. I discussed it with John Holdren, who, as chief scientific adviser to President Obama, has a similar role to mine in the US Government. We wrote an op-ed piece in *The New York Times* on the issue in general terms, saying that it was something to be taken seriously on both sides of the Atlantic, which I firmly believe.

Following President Obama's visit, there was a joint statement from the Prime Minister and the President indicating that we were going to enhance the collaboration on space weather in all aspects: monitoring, prediction, assessment of mitigating measures and so on. That is active at present. In particular, one of the things that has been taken forward is an agreement between the Met Office and NOAA, the National Oceanic and Atmospheric Administration, to co-operate on providing 24/7 cover for prediction and warning of space events. That is active. The aim is to enhance that; that is very much the view of the Prime Minister and the President that it should be done. That is active engagement, primarily at official level at the moment, but also for our organisations. I am sorry, Chairman, I answered too fully for that, but I think that may have covered some of the issues.

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

Q80 Chair: No, not at all. I am looking at an article in *The Guardian*, headed “Solar storms could create \$2 trillion ‘global Katrina’, warns chief scientist”. So, it is clear that you do take this extremely seriously.

Sir John Beddington: Yes, though I do not think the 2 trillion comes from anything I have said. I take it seriously; it is an issue that we should have out there in our minds. It should be part of our national risk assessment that is actively in progress. We need to think in the risk assessment what is a reasonable worst case. I am confident—and American colleagues have the same view—that a Carrington event is something like a reasonable worst case. It is likely that we might get something significantly less than a Carrington event that nevertheless can do damage. The last serious events we have had in space have been at times when, it is arguable, our vulnerability was less; there was less reliance on electronic control of many of our life support systems. Our vulnerability is increasing through massively increased use of satellites for communications and so on. In terms of basic time clocks, we are very reliant on satellite information.

Q81 Chair: It is more than arguable that our vulnerability was less. Our vulnerability is much, much greater, isn't it?

Sir John Beddington: Absolutely, yes. I may have misstated.

Q82 Chair: You used the word arguable; that was what I was questioning.

Sir John Beddington: I won't take issue with that.

Charles Hendry: With the National Grid, we have also identified what we would consider a worst-case scenario. That again has been based on the Carrington event. That is about ten times worse than the event we saw in the UK in 1989. In 1989, two transformers were knocked out, and that did not have any impact on the grid, which was able to continue to function properly. In terms of the work taken forward, we are looking at a much more significant event than that. The National Grid presented a paper to E3C, which is the Energy Emergencies Executive Committee, in July. Based on that paper, more work is being done now to look at the issues relating to generator transformers, and that work will be concluded in the early months of next year. We have also jointly written, with the National Grid, to all the major players in this sector, saying that we require them to co-operate actively in this work, because of the impact which it could have. That is a significant stepping up of the level of activity in order to understand what the full implications could be and what will be done, if necessary, to mitigate that.

Q83 Mrs Moon: This is an issue that cuts across Departments, as we can see by your presence here today. In the event of a severe electromagnetic event, whether it was natural or international and intentional, which Department would take the lead?

John Tesh: It would depend on what the origin of the event was. If we are talking about a nuclear EMP event, then we are talking about war and the Prime Minister would be in charge of a meeting of his

national security Ministers straight away; that is very straightforward. If we are talking about a terrorist event, then the Home Secretary is the Government Minister for terrorist events by default—in other words, the assumption is that she will be in charge for the moment, until something else happens that alerts you that there is some other aspect of the crisis that means that someone else needs to take the lead.

If we are talking about a solar weather event, it would rather depend on the level of the crisis. If we are talking about something which had an effect largely on one sector or Government Department, then that Government Department would take the lead. So if this was something that affected the national grid, then the lead Government Department for that would be the Department of Energy and Climate Change. Probably, if it was limited to that sector, they would run the crisis from DECC itself, and we would send officials from the Cabinet Office to assist in the linkages to other Government Departments that might be necessary.

If we are talking about what we would call a level 2 crisis, which is one where the impacts are widely spread, then the action moves into the Cabinet Office Briefing Rooms—COBR—and one of the functions of the Civil Contingencies Secretariat would be to advise the Prime Minister on who he should appoint as the lead Government Minister for that crisis. Ordinarily, we would have pre-identified Government Ministers, depending on the nature of the crisis, and the main criterion is where the largest impact falls. So if this was something which largely hit the electricity generating industry and sector, then DECC would probably be the person in the frame. If it was something that affected communications rather more, then another Government Minister would be identified. If it is entirely unclear who should be in the lead, then there is a system for appointing a Minister without departmental responsibility, simply to come in and deal with that particular crisis.

The system is well rehearsed, and usually functions on the basis of pre-identified lead Government Ministers. In the case of space weather, we have yet to get to that point, because we have been doing a lot of work with SEIEG—the group that Sir John Beddington was talking about—to identify exactly what the impacts of a severe space weather event would be. When we have done that work, we will be looking to identify lead Government Ministers either overall or, as is perhaps more likely in this case, for particular aspects of the crisis. Then we will have the whole thing pre-identified. As it is, we will be working off the evidence that we have received so far to identify any Government Minister. I hope that is not too long-winded.

Q84 Mrs Moon: It sounds slightly chaotic, I have to say.

Sir John Beddington: In terms of providing scientific advice in emergencies, the ball tends to land in my court. In the event that we move to some sort of Cabinet Office Briefing Room response, because it is of that degree of severity, I would put together a scientific advisory group in emergencies, the acronym for which is SAGE. This would involve the

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

appropriate people from within Government, the list of Rutherford Appleton, the Met Office and so on that I referred to, and some of the chief scientific advisers—those from the MoD, DECC and arguably Transport. It would also have some independent scientists from industry and academia, who would be involved. SAGE would then convene and questions would be posed by whoever is chairing COBR at the time, and we would gather in emergency sessions. I would bring the scientific advice, either on mitigation or, if we had an alarm that a problem was coming, advice on how we would deal with it. That mechanism is in place and it is truly cross-Government. The habit of SAGE is that, after an appropriate time delay, all the advice that it has received and all the advice that it has actually presented is made public.

Q85 Mrs Moon: Are you telling us that you take overall responsibility for the co-ordination of, and the various responsibilities associated with, an electromagnetic event, or is that someone else? I still do not get a picture of who is actually leading this.

Sir John Beddington: Taking overall responsibility is a little bit above my pay grade, but co-ordinating the appropriate science and engineering advice for Government is my responsibility.

Q86 Mrs Moon: Above your pay grade, who is it then?

Q87 Chair: As a matter of interest, if all the telephones are down how would you co-ordinate things?

John Tesh: We have rehearsed that scenario and we have alternative means of communicating in a crisis, which rely on military satellite communication and not on—

Q88 Chair: So the satellites are not down? Is that right?

John Tesh: As I am sure Mr Harvey is going to tell you, those satellites are hardened, so they are reasonably robust. That is why we have relied on them for crisis communication in the event that all other forms of communication are down.

To answer your original question about the chaotic nature of the process, Mrs Moon, it is not that chaotic. It is spelled out in a document that I can easily make available; it is on the website. It is about the concept of operation for central Government in a crisis, and the roles and responsibilities are very clearly laid down, including the duty and responsibility right up-front in a crisis—it is almost the first responsibility—to provide advice to No.10 and the Prime Minister on who he should appoint as the lead Government Minister.

To put it simply, we can prepare as much as we like for most kinds of contingencies and we do prepare—we have a long list of lead responsibilities—but there are some types of contingencies that impact in a rather unpredictable way. Space weather is a classic case, and we would have to match the recommendation to the way that it looked the impacts were going to fall. The process is well rehearsed and I would argue that it works quite well.

Charles Hendry: In my experience, this is one of the most seamless examples of Government working, rather than there being any sense of chaos in it. Where there is a clear lead in terms of which Government Department is suffering the most impact, that is the Department that would lead this process. Where there is not clarity, then the process is co-ordinated, as has been discussed, through the Cabinet Office, although potentially with a lead Minister.

Let me give you an example, although it is on a very different scale from the issues that we are looking at today. Last winter in the very bad weather, the immediate impact was evidently in the transport system—airports being brought to a halt, the rail infrastructure and the motorways too—so it was the Transport Secretary who took the lead, as Transport was the lead Department in that process. As that issue started to be mitigated, there was a risk that it could become an energy issue—that people would not get their heating oil and that grid connections might be down. Had that scenario materialised—in fact, it did not—the lead would have transferred across to DECC. Where there is clear departmental responsibility and lead in terms of the overall impact, that is the Department that would lead that work.

Q89 Mrs Moon: The Science and Technology Committee recommended that there should be a lead Government Department in relation to space weather. Has a lead Department been identified; and if it has been identified, would it be the same Department that would lead if there was a HEMP attack?

Charles Hendry: The work is still going on, I understand. Mr Tesh will elaborate, but it is dealt with in terms of identifying where the impact would be felt most acutely. In the event that it cannot be established which sector is affected most acutely, the formula of having a lead Minister who is supported by the Cabinet Office would be the model adopted.

John Tesh: We said that we would make that decision when the results of all the work that has been done on the impacts of extreme space events is much more clearly known, clearly because it is the Department where the impact is felt most heavily that is most likely to be the lead Government Department for dealing with the situation. We have not yet got to that point, but we would hope to be able to do so in the next two or three months.

Q90 Mrs Moon: How ready are we for an event tomorrow, be it a geomagnetic storm or a HEMP attack? Would we be able to cope? Are we prepared? Are we that far down the line?

John Tesh: As far as solar weather is concerned, we are a lot better prepared than we were about two years ago. An enormous amount of work has been done since 2008, when this was first identified as a potential risk, first, to identify exactly what type it was in terms of probability and predictability, and secondly, to see how the impacts would be felt in different areas. I think you heard earlier this morning about the work that National Grid has been doing to prepare. Similar work is being done, or will be done over the coming months, in other sectors where there is an effect, but first of all they need to understand how the effects of

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

space weather would differ from the sorts of disruptions that they already have planning for and whether they therefore need to put additional measures in place, or can rely on existing resilience of the sector.

In the last few months, we have spent time briefing the Space Leadership Council and talking to people who represent telecommunications and so forth. We have been promoting the concept of a sector resilience plan, which is a plan for each sector that looks at all the risks—not just a particular one—that affect the operation of that sector. We have been inviting those people to review their contingency plans and resilience arrangements and upgrade them as they see the need. The answer is: we are better off than we were, and we will, I hope, be better off still in the next few months as work on the impacts comes to maturity. A high level EMP event, I think—I probably have to defer to other witnesses on this—is a truly catastrophic event, not just because of the EMP, but rather more because of the burst effects. You are talking about a different kettle of fish.

David Ferbrache: It is fair to say our approach to that is rather different. We are very much focused on trying to ensure that that event does not occur in the first place, which is all about counter-proliferation action to prevent the acquisition of nuclear weapons or ballistic missile capabilities. Deterrent capability is one of the areas that we make absolutely certain is protected against EMP, in terms of our ability then to retaliate against such an aggressive act. Then we go into hardening of key strategic communication systems, too. It is a threat we are keeping a weather eye on, to use that phrase, because the concern downstream is that we may well see a proliferation of both nuclear weapons capabilities and appropriate launch systems.

Sir John Beddington: I can add briefly that, given the organisations that are already in place and working on it, we would have some degree of prediction, depending on the type of solar event—something of the order of an hour or two, or almost a day. It is not that it would just happen; there would be some early warning, because there are mechanisms for providing one. In terms of providing the scientific advice on how we would react, I have a sort of “Yellow Pages” of people who would be contacted and brought in. Almost certainly, depending on the situation, we would directly use the phone system, or military back-up, and we would be able to pull that team together pretty quickly.

Charles Hendry: May I expand on that? There is daily monitoring of the space environment. That is primarily done through two satellite systems, one called SOHO, which gives a 24-hour indication of what is happening, and one called ACE, which is much more accurate in terms of the intensity, but is perhaps a half hour ahead. There is clearly a pattern to this: the next solar maximum is expected in 2013; the current expectation is that it will not be particularly strong, but we are aware that the period pre-Carrington in 1859 was not one of very strong solar activity, so one cannot take that as a prediction of what is going to happen subsequently.

The National Grid has in place what is called an all-in system, so in the event that any issue emerges, it has an ability to bring on the entire network immediately, or within a very short period of time, to respond and to ensure that the risk of a problem being transported from region to region in the country can be minimised.

Q91 Mrs Moon: Will any advice or guidance be issued to business and to families on what they can do to protect themselves in such an event? Is there anything they can do, or will it be a case of only a Government-level response?

John Tesh: The answer is that there is, but it does not yet reflect our current understanding of the possible impacts of solar weather on businesses on the ground, as it were. We have something called the national risk register, which we published for the first time in 2008, with an updated version in 2010. We intend to update it further in the next three months, by the end of January next year; at that time, we expect it will reflect new risks that have emerged, on which we did not have material to include in the last one. That will include the effects of solar weather.

The purpose of the risk register is to provide an indication to people of the kinds of things that can disrupt their lives. In the first instance, it has been designed to be readable by people who are running small and medium-sized businesses as much as by people who run the big corporate enterprises and the national infrastructure. It is also designed to provide part of the background to the Government’s initiatives on community resilience, so it should include common-sense advice on the kinds of things that you need to keep in your cupboard in order to deal with the impact of the sorts of things that happen all the time and which you cannot do very much to prevent. The answer to your question is yes. I would love to say that we have a lot of people in the country reading this all the time. That is an obstacle that we still have to overcome. I think we have to market it more effectively than we are at the moment.

Q92 Mrs Moon: From which Department is this resilience strategy coming?

John Tesh: The resilience strategy comes out of the Cabinet Office—my Department.

Q93 Mr Havard: On the question of strategy as opposed to response—you have described the architecture for response very adequately—there is a national risk assessment, and the register thing you have just spoken about, at that level, and there is also the National Security Strategy, the NSC, and so on. What is the interrelationship between them in deciding a strategic view, which suggests a longer-term outlook—not doing it in a panic when the response is required, but doing it before? How do those two things get together? How does this get fed into and monitored through the security strategy and the work of the NSC?

John Tesh: The National Resilience Strategy is subordinate to the National Security Strategy. The National Security Strategy takes all our security interests from the point of view of prevention and the

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

pursuit of our national security interests, security in the sense of hardening and protection, and also response. In the resilience strategy, we define resilience as being the ability to anticipate emergencies before they arise, being prepared for them, being able to respond effectively to them and being able to recover effectively from them. We have, as part of the National Security Strategy, a resilience strategy that sets out our approach to that. It was basically incorporated in the same document as the National Security Strategy and the Strategic Defence And Security Review. If you look in there, beyond the material about defence and so forth, there is material about our ability to improve the resilience of the country to common types of emergency.

Q94 Sandra Osborne: What consideration has been given to making it a legal requirement for civilian electricity companies to protect their equipment in the event of electromagnetic disturbance and damage?

Charles Hendry: It is wrong to suggest that activity is not really happening in this area. Clearly a tremendous amount of the impact here would be on the national grid infrastructure. Since 1999, all the transformers purchased by the National Grid have been ones that can stand the high electricity currents that might be caused by such activities. The grid is constantly being upgraded. Part of the process is to try to localise any impact that happens. We are perhaps less at risk than the United States because we have shorter distances of cabling without interruption, so this can be contained more readily here. The purpose of the letter that one of our directors in the Department wrote to the energy companies and others at the beginning of October—it was a joint letter with National Grid—was to increase greatly their active engagement in this work, to make sure they understand the urgency we attach to it and to say that we need their active engagement in ensuring that the strategy being prepared for early next year reflects their needs.

Q95 Sandra Osborne: You do not feel that there has to be a legal requirement?

Charles Hendry: The issue links more to National Grid than to the individual companies. This work will be spread through the grid infrastructure. The important element is that National Grid understands what needs to be done, and I am very satisfied that that is the case. The EEEEC committee is chaired by Chris Train of National Grid, and the focus throughout is on how one stops an incident spreading and on how one contains it. As the grid is upgraded—we are going through a £30 billion process of upgrading the national grid—that will be done in a way that builds in resistance and resilience.

Q96 Sandra Osborne: We took evidence previously from National Grid. In attempting to mitigate the risks associated with electromagnetic activity, to what extent is knowledge shared between Departments and key businesses? For example, where the MOD becomes aware of a particular vulnerability that could be exploited—perhaps in developing its own networks or capabilities—is that knowledge passed on to protect military and civilian infrastructure?

Nick Harvey: Certainly, the military monitor these things through our own sources and those, principally, of the Americans. We use that information for our own reasons. Yes, we do share it with the rest of Government. It is also the case that a lot of industries will have some direct information coming to them on this. I do not know whether John or David want to add to that.

David Ferbrache: In the case of electromagnetic pulse, we have had a reasonably good understanding of the effects of EMP for some time, and that has been reflected in a complete suite of defence standards, which are taken up by respective industries as well. Those are publicly available, and they give indications of the threat wave forms and potential protective measures.

Charles Hendry: On the civil side, this is at the heart of what we are trying to achieve. The letter sent in October includes the sentence, “We see the need for a collaborative approach, which will require the sharing of data, especially transformer design, construction and configuration information.” We are expecting businesses in the sector to be sharing good practice and good design.

Q97 Chair: Could we have a copy of that letter?

Charles Hendry: Yes, certainly.⁷

Q98 Sandra Osborne: Do you think the UK would benefit from a study similar to that carried out in the US by the Commission to Assess a Threat to the United States from an Electromagnetic Pulse (EMP) Attack?

Sir John Beddington: The answer is that the more we co-operate, and the more information and sensible discussion and critical debate you have in the scientific community, the better. There is a lot of work currently going on, as John Tesh has explained. For example, there is a great deal of work going on between NOAA and the Met Office in trying to improve predictability by using satellite information of an event that may reach us from space weather. In terms of defence, that is more in the purview of Sir Mark Welland and the MoD.

On the civilian side and the space weather issues, there is a great deal of work already ongoing with the US. The North American Electric Reliability Corporation (NERC) has been particularly useful. The things it has been suggesting are terribly similar to the operation and mitigation procedures that National Grid already has in place. So I can give you some degree of reassurance on that.

In terms of the electric infrastructure security partnership, there was a meeting in Westminster Hall in September last year, I think, to look at the framework. The UK has had discussions with members of the EIS Council. You had Mr Avi Schnurr in front of you just before us. I have met him, and we speak regularly. My officials attend—I know appropriate scientific personnel do this too—events as they occur. It is interesting that, beyond being instructed by both President Obama and Prime Minister Cameron to enhance this co-operation, which is a work in progress and I will be going to the USA

⁷ Ev 53

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

in February to explore that, I will be seeing John Holdren. We have a meeting in Cape Town on Friday. One of the discussions bilaterally will be on how we can enhance the instruction that we have got from the President and the Prime Minister. We are active in it. The aim is to understand it much better and understand the impacts much better. As John Tesh indicated, that is very much a work in progress, which has to involve industry.

We are looking very carefully at ways in which we can improve the predictability. As Mr Hendry indicated, there is an issue to do with how we are using satellites to predict weather events. For some, you have of the order of eight minutes warning, depending on the event, but for others you can have up to two or three days. That needs to be bottomed out. The Met Office is working closely with NOAA on this and the scientists are meeting. The group that we have, with British Government input, as well as inputs from the appropriate universities, is working pretty well on this.

Q99 Chair: You have twice mentioned NOAA, so can you remind us what it stands for?

Sir John Beddington: Yes. NOAA is the National Oceanic and Atmospheric Administration.

Q100 Chair: Thank you very much. Mr Harvey, in view of what Sir John has just said about the responsibilities of Mark Welland in this area, why did the Ministry of Defence refuse to send somebody who could give evidence, on the basis that he had no responsibility in this area?

Nick Harvey: Candidly, I was not aware that we had done. There would be no objection in principle to his appearing before you.

Chair: We asked.

Nick Harvey: I can only apologise. I was not aware of that. From my point of view, I certainly have no objection to his appearing.

Chair: This is one of the problems that we have had with this inquiry: trying to work out who on earth will accept some responsibility for what appears to be a relatively large threat.

Q101 Mr Havard: Perhaps I can come on to that, because one of my questions will be about responsibilities and who is responsible for co-ordination and so on. Clearly the threats are real, whether they are natural or otherwise induced, and there is an effect and everyone knows that we have to put in place protections. That is a given. We are told that, of the sorts of effects there may be to power networks, satellite services, aviation, digital control systems, wireless and mobile communications, satellite communications, positioning, navigation and timing, and Earth observation, the last three in particular are the Ministry of Defence's responsibility. We are trying to delineate what responsibility should properly lie where in all this. What is said to us is that those last three things are already hardened against the problems. Some of the others are not, and we are describing how that might be done.

The Ministry of Defence may be confident that the satellite services and the positioning, navigation and

Earth observation may well be protected, but what about all of the other things that the Ministry of Defence uses that fall into the less protected areas? What is the Ministry doing about extending that protection beyond the space environment to the things that it uses in the terrestrial environment?

Nick Harvey: Generally, defence equipment is more resilient and hardened than its civilian counterparts. The responsibility for ensuring appropriate resilience for individual military equipment and systems lies with the Defence Equipment and Support organisation. As a solution is developed for a new capability, whatever that might be, including planned future upgrades, the requirements are managed to ensure that the solution will meet the need of whatever the military application is. It would be unrealistic, bluntly, to seek to harden all military assets against a threat of space weather and EMP, but as the overall likelihood of a severe damaging event is relatively low in our view, we focus our attention on what we consider to be a critical subset of systems.

David Ferbrache: We tend not to look at space systems in isolation. So, the way we tend to approach it is actually to talk about the overall system. For us, that would include, for instance, the nuclear firing chain and our strategic command and control, and that includes therefore the hardening of the terrestrial infrastructure that goes with it—not just the space segment.

With the nuclear EMP threat, we are currently putting that in a context namely that, “we judge that to be a low-probability threat,”—for all the reasons I have set out in terms of nuclear weapons—capability linked to ballistic missiles and detonated at high altitude. We therefore have taken the decision to trade out some elements of that protection, based on our assessment of the threat, and that is something we keep under review.

So my point is that this threat may evolve over the next decade—we fully expect it may do—and that will lead us to change the risk balance decisions we make. We also put quite a bit of time and effort into reversion modes and fall-back. GPS is the classic. It's a military system anyway—US military satellites. It has a degree of resilience against a lot of the space weather scenarios we have talked about. But we also routinely practise reversion modes. So, yes, we do still train people in maps and compasses—good old-fashioned navigation. We also train them in how to use inertial navigation systems, and we routinely practise GPS jamming. As Mr Harvey has set out, we tend to include electronic warfare routinely in our exercises and training. We play through a lot of degradation modes and reversion modes. I am not sanguine; the threat will evolve over time, and it is something we need to keep a careful watch on—

Q102 Chair: The title of this inquiry is “Developing threats to electronic infrastructure,” and that is therefore what you say this is.

David Ferbrache: It is, yes.

Chair: We will write you a letter, Mr Harvey, asking for further details about the nuclear firing chain that Mr Ferbrache just mentioned.⁸

⁸ Ev 51

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

Q103 Mr Havard: The Chief Scientific Adviser MoD is the person who would clearly advise the Ministry of Defence on what should be happening with the development of new equipment and other things, and replacement programmes and extra hardening and so on. So do they have responsibility for the co-ordination of seeing that those activities take place in all these other areas of the MoD? If not them, who in the Ministry of Defence has that responsibility to ensure that these considerations are fed into the various aspects of the Ministry's broader defence policy as well as its equipment acquisition? Who is that person? Is it you, Mr Harvey? Who has the responsibility to process within the MoD to ensure that that happens both day to day and in terms of policy?

Nick Harvey: It would be the capability owners acting on the advice of the Chief Scientific Adviser and then working, as I said, in co-operation with the Defence Equipment and Support organisation. Certainly Ministers would oversee this, but in terms of resilience of equipment it would be through the capability function, and providing that would be the responsibility of Defence Equipment and Support, but acting in both cases, very much, on the advice of the Chief Scientific Adviser.

Q104 Mr Havard: The Ministry of Defence is doing its thing, and we also have, as you have referenced, work with allies. Who is responsible for ensuring that those considerations work, what we can offer in that debate and what we can gain from others' experience? Who co-ordinates the relationship with allies on this issue?

Nick Harvey: I think it goes on at many different levels. The scientists liaise with their scientific counterparts, and operations people very much with their operational counterparts. At the most basic level, we have our own arrangements to monitor space and developments, and we share that information with American counterparts. We also have some procedures in place to share that with our European counterparts. It will all be done at the appropriate level.

Q105 Mr Havard: Can I ask you about military support for the civil environment, utilities and others? Clearly, at some point there is a crossover in relation to those two things. Also, in terms of the development, there is presumably an R and T strategy, or some sort of science strategy, coming through in terms of the Ministry of Defence. Where is the prioritisation of development activities and science research technology that is appropriate to the Ministry of Defence? How does it relate to those things that are appropriate to other people—not the Ministry of Defence—seeing the hardening of their equipment? How does that interface work? To me, it is not all your responsibility, Mr Harvey; equally, it is not all your responsibility, Mr Hendry. How does that work?

Nick Harvey: I agree with you: it is not all our responsibility. You correctly identify that the military aid to the civil authorities mechanism would be the means by which we would expect to give this assistance. Certainly, the Civil Contingencies Act

2004 lays out systems by which this would be done. As a national asset, defence would not expect to be called on, except in the case of very large-scale incidents. In that sense, if something did kick off, rather as Mr Tesh indicated earlier, we would expect to be brought into the equation through the COBR process. The scientific community shares information across Departments all the time. I am sure that it is keeping an eye on the evolving picture.

Sir John Beddington: Yes, I spoke to Mark Welland about this yesterday. I said that I was a bit puzzled that I was to be here, rather than him.

Mr Havard: So were we.

Sir John Beddington: There seem to be some crossed wires. He has indicated that, of course, he works in this area, and that some of it is extremely sensitive, but that he would be more than happy to answer questions about it. What he also said to me, to spare Mr Ferbrache's blushes, is: "David Ferbrache knows a great deal about this," so in a sense he is there.

In terms of cross-government, we have a group of chief scientific advisers in all Departments. We meet once a week. We meet formally five or six times a year, and we have informal meetings once a week. I probably talk to Mark Welland twice a week on the telephone. The chief scientific adviser at DECC—David MacKay—Mark Welland and I would have conversations about some of the issues, and we have had probing discussions with the advisory committee that we referred to earlier. I think we are reasonably joined up. In the event, for example, of an emergency with COBR, probably the very first person I would call would be Mark Welland, and we would network and cascade out whom we would want at the SAGE meetings.

Q106 Mr Havard: The reason why we are interested in some of this has to do with prioritisation and how much consideration is given to it at the appropriate levels. Everyone might be interested in it, but where is the co-ordination of it to make it a priority within the other systems? The issue is the relationship between defence and security. This is a newer area for us. Some people are involved in this—not just the Home Office, or the Ministry of Defence; it is not the usual, obvious people. We are trying to figure out where that is co-ordinated, so that each of the responsibilities is appropriate to those who have it, but equally so that they come together to make an appropriate equation that deals with the problem. Is it the Ministry of Defence's responsibility to ensure that the issue is prioritised, in terms of security, national security, security strategy, and NSC consideration, or is it a Cabinet Office issue? Where does it rest, in terms of prioritisation and therefore ensuring that the appropriate money is spent by the appropriate Department to achieve the result?

Nick Harvey: The National Security Council is the answer. I do not know whether Mr Tesh wants to elaborate.

John Tesh: It is just that; the National Security Council was set up by the Government to bring together all the different interests in security. It has both a main council and a subordinate committee that deals with threats, hazards, resilience and

9 November 2011 Nick Harvey MP, Charles Hendry MP, Sir John Beddington, David Ferbrache and John Tesh

contingencies, which has an even wider membership than the top-level National Security Council. The council is chaired by the Prime Minister and so, I believe, is the THRC—the subordinate committee.

Q107 Chair: I know what the answer to this will be, but do you think that there is enough resource devoted to this developing threat?

John Tesh: Are you talking about space weather?

Q108 Chair: Since there seems to be a pretty similar effect from both space weather and a high-level electro-magnetic pulse, I do not think that it really matters, does it?

John Tesh: It matters because if you are talking about nuclear weapon-generated EMP, the resource that has been put into it is, as David said, the deterrent, the Government's counter-proliferation strategies and so forth, and also a certain amount of preparedness—

Q109 Chair: As opposed to resilience?

John Tesh: There is work on resilience, but the priority is to prevent the thing happening in the first place, because we are talking about a malicious event, and you can work on human intentions and capabilities. In terms of space weather, the resource going into this is much more a Government-industry partnership because of the main impacts. You cannot do a lot to prevent it, and it is the impact management and the hardening of selected sites that you have to deal with, and that, frankly, is with the industry. The Government are working with the industry to ensure that the right level of resource is going into resilience against both space weather events and other events that have similar impacts.

Q110 Chair: Sir John, I would be interested to hear from you. Following our conversation yesterday with Mark Welland, it seems that you were both as bewildered as the Minister, but he is not in front of us today.

Nick Harvey: I believe he is out of the country today, but from what you are saying, that was not the issue in question.

Chair: No, it was not.

Sir John Beddington: I just wanted to add something on the question about resources. As Mr Tesh has explained, this is seen in the space weather world as Government-industry co-operation. There is a lot of work going on in National Grid, as there properly should be. On what I think of as a Government responsibility, prediction, the work that is going on at the Met Office with NOAA is really quite substantial. There is a slightly silly description of it. The idea is to get sun-to-mud prediction capability, which is fairly obvious and explains what it is. We have a great deal more expertise in nearer-earth capability, in terms of prediction and modelling, than NOAA does. NOAA is better nearer the sun. That work is going on fairly well.

The expectation that I am getting from the Met Office chief scientists and other advisers is that there is

potential at the moment to get a coronal mass ejection to a predictive capability of somewhere between one and four days, which would be enormously helpful. I am pretty confident that appropriate levels of resources are going into what is arguably purely the Government's responsibility—prediction. That I am comfy with. It will be enhanced. As I have mentioned, we are exploring ways of enhancing that co-operation with the Americans.

Q111 Chair: I have two final questions. First, we keep the development of non-nuclear EMP technology under a considerably higher degree of security classification than other countries do. Does that make it difficult to share some of the information, best practice and development with our allies, and, given the amount of stuff that is available on Wikipedia, is it viable?

David Ferbrache: There are two questions in there.

Chair: That was only meant to be one.

David Ferbrache: The one on R and D collaboration with NATO is worth picking up on. We collaborate with our allies on non-nuclear EMP effects, including research and development into countermeasures, through the NATO research and technology organisation which has a working group looking at those issues—so that is quite a close linkage.

In terms of classification, there is quite a bit of material on the internet. We routinely monitor that and assess it. Some of the devices are potentially viable; some are not. Most of them are rather short-range; for instance, with modified microwave sources, you are talking about ranges in the category of hundreds of metres. We keep an eye on those threats. Is it classified? There are some classified areas. We do not want to share our view on what viable devices might be at the high end of non-nuclear EMP, so we protect that very sensitive area, because we do not wish to see further proliferation of those competent devices. That is the classification reason.

Q112 Chair: The final question is this: can you confirm what the Ministry of Defence said in the written evidence? It said: "cruder devices with limited ranges of effects may be achievable by non-States. There is evidence of the proliferation of such technology, which may lead to its acquisition by countries and/or non-state actors of concern to the UK in future years." Can you put a timing on that concern? It is obviously possible that terrorists could make use of such equipment.

David Ferbrache: Again, my judgment would be that viable devices with a short range could be readily produced in the next—well, actually now, frankly, from the information available from public sources, but they would be short-range.

Chair: Okay, thank you. Unless there are further questions, I would like to say thank you very much indeed for coming this morning. It has been helpful, and we will produce our Report in due course, but in the meantime, many thanks to all our witnesses.

Written evidence

Written evidence from HM Government

This paper sets out the Government evidence to the House of Commons Defence Committee inquiry on Developing Threats to Electronic Infrastructure. It has been prepared by the Ministry of Defence in consultation with officials from other Government Departments and the National Security Council (Threats, Hazards, Resilience and Contingencies).

SUMMARY

The electromagnetic pulse (EMP) effect of a nuclear weapon detonated at ground level would be limited but one detonated at high altitude would generate a widespread effect. A limited number of States are considered to be capable of detonating a nuclear device at high altitude.

Non-nuclear EMP devices have a much more localised effect, and we continue to track the threat posed by such devices whether employed by state or non-states.

Space weather has the potential to generate EMP like effects. The UK has access to space weather data through close military and civilian links with the US allowing warnings to be issued of extreme events.

Space Weather and EMP have the potential to impact a range of civil infrastructure including: power networks; satellite services; aviation; digital control systems; and, wireless and mobile communications.

A three pronged approach is taken to mitigate the effects of EMP: prior warning is given, either through forecasting or the collection of intelligence, which enables appropriate action to take place, for example switching off vulnerable satellite systems; infrastructure is hardened where appropriate, this is especially the case for critical military infrastructure; and we prepare for these events although the Government's approach to civil resilience management is to plan for the consequences of potential civil emergencies no matter what the cause. Contingencies are in place to react to large scale loss of electronic infrastructure with the restoration of the National Grid being a priority.

The UK has significant research resources available. The civil sector focuses on the effects of space weather whereas the military sector covers both space weather and its possible EMP effects.

WRITTEN EVIDENCE

Q1. The extent of any threat posed to UK electronic infrastructure by electromagnetic pulse (EMP) events caused by space weather events, nuclear weapons detonated at high altitude or other EMP weapons

1.1 The Government considers risks to national security, such as an EMP event, on the basis of the likelihood of the event as well as its potential impact. This is to ensure that investment in security and resilience remains proportionate to the risk. Risks of civil emergencies,¹ both malicious and non-malicious, affecting the UK mainland over the next five years are assessed in an annual classified National Risk Assessment (NRA), while areas of global risks to UK national security are weighed over a five and 20 year horizon in the National Security Risk Assessment (NSRA), first published in 2010 under the Government's National Security Strategy (NSS).²

1.2 The impact of EMP events caused by nuclear devices would be very severe but the likelihood is currently considered to be low. Non-nuclear EMP devices exist and the risks are being kept under review but are not currently considered to be sufficient to warrant recognition as a national security risk. Severe space weather, which might cause geomagnetic storms impacting the Earth's magnetosphere, has been the subject of extensive research over the past year. The likelihood of a severe space weather event is assessed to be moderate to high over the next five years, with the potential to cause damage to electrically conducting systems such as power grids, pipelines, and signalling circuits.

Q2. The likelihood that a viable EMP weapon can or will be used by either state or non-state actors

2.1 A nuclear weapon (whether state or a terrorist improvised device) activated at ground level would cause a direct EMP but its range of effect would be of limited extent, and arguably less significant than the blast, thermal radiation, and fallout from any such device.

2.2 To generate more widespread damage from EMP, a nuclear warhead would have to be detonated at high altitude to generate the EMP from the interaction between the radiation from the weapon and the outer layers of the atmosphere. This could only be achieved by launching a device by missile to an altitude of several tens of kilometres. A limited number of States possess this capability.

¹ Emergency is defined by the Civil Contingencies Act 2004 as an event or situation that threatens serious damage to human welfare in a place in the UK, an event or situation which threatens serious damage to the environment of a place in the UK, or war or terrorism which threatens serious damage to the security of the UK. It must also be a threat or hazard of sufficient scale and nature that it is likely to seriously obstruct a Category 1 responder in the performance of its functions, or require the Category 1 responder to exercise its function and undertake a special mobilisation.

² Cabinet Office, *A Strong Britain in an Age of Uncertainty: The National Security Strategy*, Cm 7953, October 2010.

2.3 The use of such a nuclear device against the UK would be considered to be a nuclear attack and an act of aggression. The EMP would also be likely to cause damage to a number of other nations beyond the target country, leading to the possibility of a collective response.

2.4 No non-State actors can currently produce an improvised nuclear device and none are likely to be able to make a sufficiently robust warhead for missile delivery in the foreseeable future.

2.5 State development of non-nuclear EMP devices would require advanced engineering, although cruder devices with limited ranges of effects may be achievable by non-States. There is evidence of the proliferation of such technology, which may lead to its acquisition by countries and/or non-state actors of concern to the UK in future years.

Q3. The extent to which space weather is forecasted and the effectiveness of early warning systems that may be in place

3.1 The US National Oceanographic and Atmospheric Administration (NOAA) Space Weather Prediction Centre (SWPC) is the global centre for space weather services into the civilian community and is the dominant source of data and predictions for the UK. The US Air Force Weather Agency (AFWA), provides prediction services to UK military operations. UK infrastructure operators receive warnings via subscription services with NOAA or AFWA.

3.2 The Meteorological Office is currently developing a space weather prediction capability in partnership with NOAA and a number of UK organisations including British Geological Survey (BGS). Future space weather collaboration is also under discussion between the Met Office and AFWA. The European Space Agency (ESA) Space Situational Awareness (SSA) programme is defining ESA's requirements for space weather services. The global space weather community is dependent on a small number of solar environment observation satellites, many of which were launched for scientific purposes and not for operational observation to support prediction.

3.3 The MoD UK Space Operations Co-ordination Centre (SpOCC), based at RAF High Wycombe, receives 12-hourly updates from the US Joint Space Operations Centre of any solar activity expected within the next 72 hours. The SpOCC also receives automated alerts from the AFWA. These alerts provide details of any space weather phenomena observed in the previous 24 hour period and any solar activity expected in the next 24 hours. Where the level of solar activity is expected to impact on military operations, warnings are sent to the Permanent Joint Headquarters at Northwood and the Global Operations and Security Control Centre at Corsham. AFWA space weather products are also embedded within routine outputs from the Joint Operational Meteorology and Oceanography Centre at Northwood.

Q4. The potential impact of such events for both civilian and military infrastructure

4.1 Space weather comprises a range of solar phenomena including solar flares, solar radiation storms, and coronal mass ejections (CME), which are likely to impact upon a wide range of systems including:

- (a) *Power networks:* Severe geomagnetic storms caused by fast-moving CME, can generate large geomagnetically induced currents (GIC) through long, electrically conducting systems such as power grids, pipelines and signalling circuits. High levels of GIC can permanently damage transmission, distribution, and generation assets in electricity networks potentially leading to power failure.
- (b) *Satellite Services:* Severe space weather can interrupt satellite services including Global Navigation Satellite Systems, communications, and Earth observation and imaging systems by damaging the space-based hardware, distorting the satellite signal, or increasing the errors in ground-based receivers.
- (c) *Aviation:* Airlines rely on High Frequency (HF) radio and satellites to maintain communications both of which can be disrupted by space weather. Cosmic rays and energetic particles from solar radiation storms can adversely affect microelectronic components in aircraft. The elevated levels of radiation exposure at flight altitude can be of concern for airline passengers and flight crews.
- (d) *Digital control systems:* High levels of neutron flux produced by the atmosphere by solar radiation storms can greatly enhance error rates in these components.
- (e) *Wireless and mobile communications:* The Sun can produce strong bursts of radio noise over a wide range of frequencies that can interfere with wireless systems including mobile phone telecommunication and the internet.

4.2 The Ministry of Defence relies on space based assets to provide:

- (a) *Satellite Communications (SATCOM).* SATCOM and data networks enable the command and control of deployed forces and the timely exploitation and dissemination of intelligence data.
- (b) *Positioning Navigation and Timing (PNT).* Precise PNT solutions derived from the US Global Positioning System (GPS) enable the orchestration of complex military operations while reducing the risk of collateral damage and fratricide.

- (c) *Earth Observation (EO)*. Earth observation capabilities (most of which are derived from allies and commercial providers) provide the necessary strategic indicators and warnings, and intelligence to support operational and tactical planning.

4.3 Defence procurement 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.

- (a) *SATCOM*. 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 nuclear explosion (HANE). 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.
- (b) *PNT*. Ionospheric disturbances caused by space weather are the single largest contributor to single-frequency GPS errors. However, military receivers use two frequency bands and enhanced signal processing techniques, which make them less susceptible to signal errors caused by EMP effects in the ionosphere.
- (c) *EO*. It is possible that a severe space weather event or HANE could degrade the ability of these satellites to collect and disseminate data in a timely manner.
- (d) *Military Ground Infrastructure*. Much of the military ground infrastructure in the UK is connected to the National Grid, the Public Switching Telephone Network, and other utilities, which may be susceptible to artificially generated EMP or GIC caused by space weather. Critical military infrastructure is designed to operate independently of nationally-provided utilities, with many facilities having back-up power generators and bulk fuel reserves.

4.4 The consequences of an attack by non-nuclear EMP can be temporary or permanent. The effect can be achieved either by the generated electromagnetic energy directly coupling to the victim communication wires, links and/or sensors, or coupling indirectly via metallic structures, cables, or network architectures. Equipment hardened to withstand nuclear generated EMP, may be susceptible to aspects of non-nuclear EMP. Commercial-Off-The-Shelf electronics are known to be vulnerable to non-nuclear and radio-frequency electromagnetic pulse attack.

4.5 The success of a non-nuclear EMP attack is, however, dependent on the level of access to and knowledge of the target as acquired by the attacker. Fixed targets such as land based devices, units, and centres that use IT, electronic and/or computer control systems are considered to be more vulnerable to an attack than moving targets such as air systems.

Q5. *Ways of mitigating electromagnetic pulse events, either targeted or naturally occurring*

5.1 DECC and National Grid have been working closely over the past year to gain a better understanding of the potential impacts of a severe space weather event on electricity assets and networks. Scientific advice suggests that most of the risk from severe space weather arises from short lived extreme events that are not well correlated with longer term trends in solar activity. Historical records suggest that the so-called “Carrington event” of 1859 is a reasonable worst case scenario. Evidence indicates this event was about ten times more intense³ than the most severe recent event that occurred in 1989 and led to a major power system disturbance in Quebec, Canada.

5.2 The main risk the Sun poses to electricity networks is CME. The components of the British electricity system most at risk are the high-voltage transformers that are used to enable power to move from one network voltage to another (eg from the 400kV grid network to a 132kV distribution network). Transformers at the edges of a large network and those on ground/rock with high electrical resistance are particularly susceptible. Transformers connected to transmission networks (including those connecting power stations) are at greater risk than those on distribution networks because the networks couple to the ground over greater distances and provide a lower resistance to the GIC. If damaged, the transformers connected to the transmission system would either need to be replaced or returned to the factory for repair. National Grid has around 800 high-voltage transformers installed and holds a number of strategic spares to cover for individual faults.

5.3 There is substantial redundancy within the design of the grid allowing demand to be met in full unless there are multiple transformers out of service in a particular locality. Failure of substantial number of transformers would complicate the restart of the grid. As the normal demand for very large transformers is small (they have a life of around 50–60 years) such an event could cause substantial delay in restoring full connectivity due to the time taken to manufacture replacement transformers. There has yet to be a recorded case in which damage has been sufficient to cause such a delay in service restoration.

³ Although this depends on what effect is being measured.

5.4 To date, the most severe damage on National Grid's network was in 1989 when two transformers had to be returned to the manufacturer with damage that was believed to have been caused by the same space weather event that affected the Hydro-Quebec electricity network. Although two transformers were damaged, the redundancy within the design of the system enabled demand to be met in full. Since that time National Grid have taken actions to mitigate the risk to their network against a storm of similar intensity: altering the specification of their transformers, monitoring warnings of potential problems, and developing operational strategies.

5.5 National Grid has instituted a GIC warning system with Metatech and EPRI. Scottish Power have commissioned an independent warning and monitoring system with BGS. These processes enabled warnings to be issued for at least five events including the major "Halloween" storm in October 2003 that caused some issues in South Africa. This storm was detected in the UK but did not have any detrimental effects. The monitoring part of the current system, which records GICs flowing in selected transformer neutrals, has been integrated into the Smart Asset Management monitoring system and US Solar Shield system. A visual warning and modelling system is currently being developed with BGS with a full GB transmission model.

5.6 On 20 September 2010 the Electric Infrastructure Security Summit (EISS) at Westminster Hall was attended by HMG Officials. This was the first in a series of summits intended to promote cooperation on assessing the risks of space weather and taking appropriate action. National Grid agreed to investigate the implications of various scenarios on the British transmission system and have reported their initial findings to the Energy Emergencies Executive Committee (E3C), where government and industry work together to mitigate threats to gas and electricity supplies. E3C have been tasked with conducting further work across the electricity sector to fully understand the risks posed by severe space weather to generators and distribution network operators. An initial report is expected in early 2012.

5.7 The second EISS in April 2011 in Washington had wider industry attendance and particularly highlighted the severe effect on the US of a Carrington type event as well as EMP. Further work following the Washington Summit has determined which transmission networks or regions are particularly susceptible to geomagnetic disturbance. Increased risk is experienced in highly loaded systems with long high voltage lines over highly resistive geology and old design five limb or single phase transformers. Historically the GB transmission system has had a relatively low failure rate of less than 0.3% per year from 1952 to 2004 (five solar cycles) and random failure modes.

5.8 National Grid continues to review its approach to space weather compared to the US, European, and other transmission systems. The National Grid has six monitoring sites that, along with two on the US National Grid, will provide key inputs to the Electric Power Research Institute SUNBURST collaborative project (which the National Grid has been a member of since 2000), which in turn supports NASA's Solar Shield project. Other collaboration is taking place with the University of Manchester for transformer modelling, the University of Lancaster for space environment modelling, as well as BGS, Rutherford Appleton Laboratories, the EURISGIC project, DECC, E3C, and the Cabinet Office. NERC in the US has been particularly useful as its operational mitigation procedures are similar to National Grid.

5.9 Mitigation arrangements are in place to reduce the threat to military infrastructure. These have been detailed in response to Q4, together with the supporting space weather forecasting arrangements detailed in response to Q3.

Q6. The resources available in respect of research and development in the field

6.1 The UK has significant civil sector expertise in space weather spread over Research Council institutes, universities, industry, and the Met Office. This includes:

- (a) provision of targeted space weather services for users in the public and private sectors;
- (b) development and operation of instruments that are the UK contribution to the global space weather monitoring;
- (c) key roles in European programmes and proposals to improve space weather forecasting (eg improved modelling of threats to spacecraft and power grids; improved international coordination and integration of space weather data resources and measurements); and
- (d) collaboration with US space weather forecasters in the provision of services, the development of advanced modelling and better methods for the detection and tracking of space weather threats.

6.2 A UK-US workshop in October 2010 explored the development of a roadmap for research collaboration to address key gaps in the science needed to deliver accurate space weather forecasts.

6.3 The MoD has expertise on space weather and EMP effects within its Defence Science and Technology Laboratory (Dstl) that is complemented by industry expertise gained through practical hardening and assessments of electronic systems.

Q7. Contingencies in place to react to a large scale loss of UK electronic infrastructure, and the role of the military in such an event

7.1 Successful management of a major electricity supply emergency requires effective communication and cooperation between industry and government. The wider consequences of an incident could be mitigated by the choices that industry is able to make, and some of the practical aspects of managing an incident could be assisted by the activities of government. *The National Emergency Plan for Downstream Gas and Electricity (NEP-DG&E)* sets out a framework for industry and government to work together to manage a major supply emergency.

7.2 Should a severe space weather event cause sufficient damage to the British electricity system that a prolonged electricity shortage is experienced in a specific region, or, exceptionally, the whole country, electricity rationing may be necessary until such time as repairs are completed or sufficient mobile generation installed. The NEP-DG&E provides an option to implement electricity rationing through existing arrangements contained within the Electricity Supply Emergency Code. This aims to ensure the fair distribution of available electricity regionally/nationally to all consumers whilst protecting supplies to those who require priority treatment, using a process known as "Rota Disconnections". Electricity distribution network operators maintain lists of priority customers within their networks and in emergencies, as Category 2 Responders under the Civil Contingencies Act 2004, are experienced at working closely with Local Responders to ensure that vulnerable customers are cared for.

7.3 In the unlikely event that a severe space weather event causes a total or partial shutdown of the British transmission system, National Grid as the System Operator, would declare a Black Start. This is the industry procedure to recover from a total or partial shutdown of the transmission system which has caused an extensive loss of supply, and entails isolated power stations being started individually and gradually being reconnected to each other to form an interconnected system again. National Grid run a regular inspection and testing regime of all Black Start stations to ensure that the capability to start-up independently is robust.

7.4 Telecommunications and electrical power generation and distribution infrastructures are mutually dependent. Public, fixed line, telecommunications infrastructures in the UK have arrangements in place that enable them to continue to function for up to five days in the event of the loss of grid-distributed electricity. Telecommunications infrastructures are owned and operated by private sector organisations who are best placed to respond to and recover from a major telecommunications incident.

7.5 Government has worked closely with the owners and operators of telecomms infrastructures through the Electronic Communications Resilience and Response Group to facilitate restoration of services in the event of a major incident affecting networks. The procedures that are in place are subjected to an extensive annual test conducted over several days. This is augmented with more frequent tests of the mustering arrangements for participants.

7.6 Core telecommunications networks are highly resilient when viewed against the planning assumptions from the National Risk Assessment. While the resilience of core networks is largely the concern of the Network Service Provider, since there is a significant incentive to efficiently route traffic, the resilience of access to these networks is largely a concern for the customer. Customers for telecommunications services can undertake a range of measure to enhance resilience.

7.7 The High Integrity Telecommunications System provides a strategic communications network linking Central Government to Strategic Co-ordination Centres, from where the response to civil emergencies are co-ordinated. The network achieves an exceptionally high level of resilience through the use of both military hardened satellite capabilities and terrestrial links.

7.8 Industry has an established procedure in place (the National Emergency Alert for Telecoms) for dealing with emergencies. In both real and exercise scenarios, this procedure has proved to be a highly effective process for ensuring resilience.

7.9 In the case of a national EMP event Defence does not expect to play a significant role in the primary response,⁴ for example, restoring the National Grid. Under the provision of Military Aid to the Civil Authorities, MoD may, however, have capacity to augment any civil response, if capabilities are overwhelmed by the scale of the emergency. Defence personnel are likely to be available in the UK, and if requested should be able to provide general duties support to the emergency services and others dealing with the knock-on effects of an EMP event. Such support can be requested by any government department at the strategic level and at the local level this is facilitated through a nationwide network of Joint Regional Liaison Officers who work with local resilience fora and others to enable access to military aid.

Q8. The broader security of UK electronic and space infrastructure, particularly satellites and satellite navigation systems and the risk posed by space debris

8.1 The Strategic Defence and Security Review of 2010 committed the Government to develop a National Space Security Policy, which would coherently address all aspects, both military and civil, of the UK's dependence on space; assure access to space; help mitigate risks to critical national infrastructure; focus future

⁴ Defence may have a small number of specialists who can be deployed.

investment and research on national priorities, opportunities, and sovereign capability requirements; and encourage co-operation with UK industry and with international partners. We expect this policy to be published in 2012.

October 2011

Written evidence from National Grid

KEY MESSAGES

- Severe Geomagnetic Disturbances (GMD) resulting in Geomagnetically Induced Currents (GIC) in high voltage transmission systems are a category of what is known as High Impact Low Frequency (HILF) events.
- Severe GMD events can be as a result of natural causes from solar activity and space weather or artificial causes such as High Altitude Electromagnetic Pulse (HEMP) from a nuclear detonation or other man made activity such as Intentional Electromagnetic Interference (IEMI).
- Space weather is the term for changes in the sun-earth environment analogous to the atmosphere and terrestrial weather. While the weather on earth is well understood, space weather forecasting is in its infancy.
- The effects of space weather on transmission systems has been known for some time and National Grid is a world leading transmission operator in understanding the effects and developing operational mitigation actions.
- HEMP is a more recent perceived risk raised particularly in the US and has resulted in the Shield Act legislation being progressed.
- HEMP effects are not well understood, there is almost no experience to estimate the effects but it is probable that they will be unforeseen, extreme and affect much more than transmission systems. For this reason mitigation policy for HEMP is extremely difficult to develop.

The extent of any threat posed to UK electronic infrastructure by electromagnetic pulse (EMP) events caused by space weather events, nuclear weapons detonated at high altitude or other EMP weapons

1. National Grid is fully aware of the threat of disturbance to the Electricity Transmission System from the effects of space weather and take this very seriously.
2. National Grid first realised the seriousness of the problem after the Solar Storm of March 1989, during which two transformers were damaged by overheating.
3. As a result of discussions with DECC at the Space Weather: Energy Partners Meeting on 21 September 2010, National Grid raised the level of its Worst Case Planning Scenario from a storm of size 500 nT/min to 5000 nT/min.
4. National Grid's operating procedures propose to deal with the effects of severe Geomagnetic disturbance (GMD) by operational mitigation strategies, as outlined in National Grid BP1832. This includes daily monitoring of the space environment, principally using information provided by NOAA and NASA.
5. We also work with key partners to understand threats. This includes the British Geological Survey, Met Office, SUNBURST, EURISGIC, University of Manchester and NASA, and National Grid maintains regular contact with NERC (UK), NERC (US) and the Solar Shield project.
6. As a result of concern in the US, National Grid has considered the threat from a high altitude nuclear device and the corresponding electromagnetic pulse (HEMP). If such an event were to occur, significant damage could occur to both the Electricity and Gas Transmission Systems.
7. The United States Congress commissioned a report, Commission to Assess the Threat to the United States from EMP Attack, to assess the threat from EMP. It concluded that "It is not practical to try to protect the entire electrical power system or even all high-value components from an EMP event..." Widespread collapse of the electrical power system in the area affected by EMP is virtually inevitable after a broad geographic EMP attack.⁵ Also, "Industry is responsible for assuring system reliability, efficiency and cost effectiveness...." Government is responsible for protecting the society and its infrastructure, including the electric power system.⁶
8. HEMP produces a short lived (nanoseconds) E1 phase, an intermediate (milliseconds) E2 phase similar to a widespread lightning storm, and a longer lived (tens of seconds) E3 phase. All are capable of disrupting or damaging the Transmission Network over a distance encompassing the whole UK.
9. Supervisory Control and Data Acquisition Systems (SCADA) are susceptible to the E1 pulse. Control Systems, Protection Systems and System State Monitoring equipment can either malfunction or be irreparably

⁵ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 45.

⁶ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 53.

damaged by the pulse. Combined with concomitant disruption to communication systems this could leave control engineers effectively blind and unable to act.

10. The E3 pulse is similar to a severe Geomagnetic Storm, except that the quasi-DC currents that flow are many times greater, of the order of 10s to 100s of Amps. This disruption would be an order of magnitude greater than National Grid has planned for.

11. Research to investigate options to harden the UK system, rather than relying on operational procedures as is appropriate for solar events, would be needed to mitigate this threat. But given the size of the undertaking, and the subsequent cost of procurement and installation, this is beyond the resources of any one commercial organization, or group of organizations, and would need to be pursued at national level.

The extent to which space weather is forecasted and the effectiveness of early warning systems that may be in place

12. According to the director of NOAA's Space Weather Prediction Center "Space weather forecasting is still in its infancy".⁷ An expert at the Met Office likened the current state of Space Weather forecasting to terrestrial weather forecasting techniques a hundred years ago.⁸

13. Space Weather forecasting requires information gathered by spacecraft and satellites: principally the two STEREO spacecraft, SOHO, GOES, and ACE.

14. ACE is particularly important as it sits at the L1 point, a million miles from Earth, and is able to detect the polarity of incoming Coronal Mass Ejections (CMEs). ACE was launched in 1997 for an operational mission of three years. It is now well beyond its original operational life, although it has fuel capacity to take it to 2024. Crucially, it is a single point of failure in our ability to forecast Space Weather.

15. CMEs can take from 18 hours to three days to reach Earth. Forecasting models are used to decide on their trajectory and timing. NASA issue forecasts of arrival time giving a six hour window. However these forecasts are frequently inaccurate, with the actual arrival being many hours early or over a day late.

16. Models for what happens once the CME starts to interact with the Earth's magnetosphere are far less advanced. There are models that describe the interaction in high polar regions. These models can predict fluctuations in the magnetic field at ground level with 50% accuracy. However, the models run ~300 times slower than real time, so are not useful for practical forecasting.

17. There are currently no models that can predict the effect of a CME at the latitudes occupied by the UK.

18. National Grid relies on rough estimates of the size of the CME impact issued by NOAA at the time the CME is ejected from the sun; the size and polarity of the magnetic field disturbance at the ACE spacecraft, with a lead time of 25–45 minutes; modelling of generic scenarios using the BGS/NG modelling tool.

The potential impact of such events for both civilian and military infrastructure

19. Geomagnetic disturbances from naturally occurring solar storms cause quasi-DC Geomagnetic currents to flow in long transmission lines, and to pass through neutral earthing connections in supergrid transformers (SGTs). The size of these currents depends on the exact dynamics of the CME interaction with the magnetosphere, the position of the jet stream above the UK and the geological makeup of the rock beneath the surface of the UK.

20. Direct current, superimposed on top of the AC current that transformers are designed for, can cause the core of the transformer to saturate, and this in turn leads to flux leaking out using routes such as transformer bolts. This then leads to overheating and potentially catastrophic damage to the transformer.

21. Evidence for transformer damage comes from: the UK experience of 1989, when, anecdotally, two transformers overheated after being exposed to GIC of ~30 A; the failure of a transformer at Salem, USA during the same storm; and failures of six transformers in South Africa in the 12 months after the Halloween storm of 2003.

22. Based on the most severe event that National Grid plans for, a storm of 5000 nT/min, 10 times greater than the 1989 storm, National Grid expects that, without mitigation strategies, its worst case scenario is of the order of nine transformer failures in England and Wales, the location of these transformers being at the edge of the network. This number of failures is within the capacity of National Grid's spares policy (even before the recent review of that policy).

23. If all transformers at a node are damaged then, depending on the location of the node within the network, this could result in a local area being disconnected until replacement transformers could be installed. Replacing a transformer can take two or more months depending on the availability and location of spares. In this extreme event scenario National Grid estimates that the probability there would be a disconnection event is 62% for England and Wales, and 91% for GB as a whole.

⁷ http://science.nasa.gov/science-news/science-at-nasa/2010/04jun_swef/

⁸ Personal communication from Mark Gibbs, Met Office.

24. The number of nodes expected to fail is 0.9 in England and Wales and 1.1 in Scotland. There are four locations in England and Wales where the failure is most likely to occur, and three in Scotland. None of these locations has a high population density.

25. Because of their design and heavier loading National Grid believes that generator transformers are at more risk than SGTs. National Grid is working with DECC and the generator operators to include generator transformers in its modelling and mitigation plans.

26. A secondary effect is the creation of harmonics in the saturated core of the transformer. These propagate out and can cause malfunction of protective relay equipment, switching out hardware needed for stabilisation of the network. It was this type of event that caused the blackout of the Hydro-Quebec system in 1989, and the blackout of Malmö, Sweden, in 2003.

27. The effect of E1 and E3 pulses from HEMP would be considerably more extreme. For these effects we have no practical experience to fall back on,⁹ although the Commission to Assess the Threat to the United States from EMP Attack did conduct a number of experiments on E1 and its effect on SCADA. They concluded that “Large-scale load losses in excess of 10% are likely at EMP threat levels,”¹⁰ and that “widespread collapse of the electrical power system.....is virtually inevitable”.¹¹

28. Although National Grid recognizes the threat from other sources of deliberate EMP generation, given the localised nature of the effects we do not believe that the consequences would be severe. For instance, if a localised EMP pulse were able to penetrate the National Control Centre, the system is capable of being run from alternative locations without loss of load.

Ways of mitigating electromagnetic pulse events, either targeted or naturally occurring

29. For GMD caused by naturally occurring Space Weather events, National Grid has a set of operational strategies to mitigate the effects. These include routine daily monitoring of the space environment. In the event of a serious storm being likely National Grid would operate an all-in policy, where all available lines and all transformers would be brought into service (reducing load on individual units), power transfers between regions would be reduced, increased reactive power would be instructed to help stabilise voltage swings, and all generators would be instructed to generate. In addition, a simultaneous tap change on transformers could be instructed to lower system voltage, which reduces the risk to transformers.

30. In the event that the storm was so large (a superstorm) that it exceeded National Grid’s worst planned-for scenario, then, in conjunction with Government, National Grid would consider a controlled shut-down of the network. National Grid has a well developed Black Start Policy. Training exercises are regularly held on Black Start, and generating units are at all times scheduled for Black Start capability.

31. National Grid is developing in conjunction with BGS a tool for monitoring of GIC current flows based on real-time magnetometer data. This tool will also be able to be used as an analytical tool for assessing various possible scenarios.

32. National Grid has recently reviewed its spares policy and has increased the number of spare transformers that it holds.

33. As explained in the National Grid consultation document *Operating the Electricity Transmission Network in 2020*, managing the Transmission System with much higher penetration of intermittent generation will require greater resiliency and higher reserve requirements. The effect of this will be to harden the system and make it less susceptible to the effect of GMD.

34. National Grid is actively considering the introduction of series capacitance on the long lines connecting England and Scotland. These are capable of blocking the flow of GICs.

35. National Grid has considered the use of devices for providing permanent or switchable resistance to ground. It may be that the design characteristics of UK transformers make them unsuitable for such devices so further work is needed to assess the efficacy of such measures. At present National Grid is not planning to install these devices to counter the effects of GIC. In the event of HEMP, and an E3 pulse it is not clear that switchable devices would work, as the control mechanisms would be affected by the earlier E1 pulse.

36. With regard to HEMP, National Grid agrees with the Commission to Assess the Threat to the United States from EMP Attack that “it is not practical to try to protect the entire electrical power system or even all high-value components from an EMP event,”¹² and that “the key to minimizing catastrophic impacts from loss of electrical power is rapid restoration”.¹³

37. Rapid restoration of communication systems is vital. The recommendations of the US report suggest that in the US responsibility for this falls on the Department of Homeland Security.

⁹ Metatech Report Meta-R-320, The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the US Power Grid.

¹⁰ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 36.

¹¹ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 45.

¹² Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 45.

¹³ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 47.

38. Again, from the US report: “To better understand EMP-related system response and recovery issues, conduct in-depth research and development on system vulnerabilities”. The objective is to identify cost effective and necessary modifications and additions in order to further achieve the overall system performance. Specifically there should be government-sponsored research and development of components and processes to identify and develop new consequential and cost effective approaches and activities.¹⁴

October 2011

Written evidence from Research Councils UK

BULLETED SUMMARY

- Major space weather events have been recorded in the past but had relatively minor societal impact. Equivalent events today could be dangerous due to our greater reliance on technology.
- Examples of the hazards and risks associated with space weather include: damage to space-based infrastructure (satellites) by energetic particles and radiation; disturbance of the ionosphere degrading communication and navigation signals (including GPS) with particular impacts on aviation and shipping; blackouts and damage to electricity distribution grids extending over long distances caused by geomagnetically induced currents.
- Our ability to predict space weather and the severity of particular events is currently limited. The US Space Weather Prediction Center is the major agency providing space weather services. The UK has the potential to contribute further via research and capability supported by the UK Research Councils, services provided by the Met Office and via the European Space Situational Awareness Programme.
- Warning and prediction of space weather events is one of the most important ways of mitigating impacts. In addition, a variety of engineering and other approaches exist and are being developed to mitigate impacts of space weather across the range of infrastructure it affects.
- The UK has over 100 years’ leadership in the science underpinning our understanding of space weather. This continues today with UK Research Councils as significant funders of research and capability relevant to understanding, forecasting and mitigating the impacts of space weather.

INTRODUCTION

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 on behalf of the Research Councils listed below and represents their 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).

Natural Environment Research Council (NERC)¹⁵

Science and Technology Facilities Research Council (STFC)

3. This evidence focuses on the threat posed by space weather to civilian infrastructure. Further information of relevance to this inquiry can be found in several relevant POSTnotes¹⁶ and evidence for the House of Commons Science and Technology Committee inquiry into Scientific Advice and Evidence in Emergencies.¹⁷

Question 1. *The extent of any threat posed to UK electronic infrastructure by electromagnetic pulse (EMP) events caused by space weather events, nuclear weapons detonated at high altitude or other EMP weapons*

4. Space weather creates conditions potentially hazardous to assets in space and on the ground, detrimental to a range of the services they provide.

5. Space weather is underpinned by solar activity. The sun is a continuous source of electromagnetic radiation over a wide spectrum and of charged particles that stream through space forming the solar wind with embedded solar magnetic fields. Solar flares, radio bursts, solar energetic particle (SEP) events and coronal mass ejections (CME) are examples of impulsive solar release events where electromagnetic energy, particles and solar magnetic fields are ejected at high speed from the sun. CME’s are one of the most important types of space weather disturbances. The frequency of impulsive release events is modulated by the solar activity cycle of around 11 years commonly characterised by sunspot numbers with the next solar maximum currently estimated

¹⁴ Report of the Commission to Assess the Threat to the United States from EMP Attack: Critical National Infrastructures, p 55.

¹⁵ Views were sought from experts based at NERC’s centres: British Antarctic Survey and British Geological Survey.

¹⁶ <http://www.parliament.uk/business/publications/research/post/physics/>

¹⁷ Science and Technology Committee, Third Report of Session 2010–12, *Scientific Advice and Evidence in Emergencies*, HC 498 <http://www.parliament.uk/business/committees/committees-a-z/commons-select/science-and-technology-committee/inquiries/scientific-advice-in-emergencies/>

to be in 2013. Threats occur throughout the solar cycle, however, and levels of cosmic radiation are highest during solar minima.

Threat to space based infrastructure

6. Solar release events can result in high energy charged particles which penetrate the Earth's magnetic field directly, and cause magnetic storms which rapidly increase the number of high energy charged particles trapped in the Van Allen radiation belts. These particles threaten satellite operations by accelerating cumulative damage to the solar arrays providing power and by their effects on electronic systems. High energy particles can penetrate chips in digital electronic systems causing Single Event Effects (SEE), flipping memory and changing the state of software. Modern developments in microelectronics are leading to equipment with increasing chip density and increased vulnerability to SEEs.¹⁸ Electrons in the radiation belts can penetrate satellites and cause build-up of charge in insulating materials. Discharges can permanently damage electronic components or generate false signals to which the satellite may respond.

Upper atmosphere and ground level derived threat

7. At the Earth, solar ultraviolet and X-ray emissions are absorbed in the atmosphere creating the ionosphere, which affects the transmission of radio waves and supports the flow of electric currents which generate magnetic fields. When a CME encounters the Earth's magnetic field it can cause a severe magnetic storm lasting from a few hours up to several days. The rapidly changing magnetic fields during magnetic storms induce electric fields in the solid Earth and oceans. These can drive Geomagnetically Induced Currents (GIC) through earthed conductors, including electrical power grids and pipelines.

8. Some SEP events, through the production of neutrons from collisions in the atmosphere, lead to increases in radiation at ground level and with higher intensity at aircraft altitudes. The risk is higher in the polar regions where there is less protection from the Earth's magnetic field. SEP events result in increased radiation dose to aircrew, electronic upsets in aircraft avionics and disruption to air traffic communications on polar routes.

Question 2. *The likelihood that a viable EMP weapon can or will be used by either state or non-state actors*

9. Nil response.

Question 3. *The extent to which space weather is forecasted and the effectiveness of early warning systems that may be in place*

10. The UK has a long and successful heritage in relevant solar observations and there are a number of UK-led instruments on major international space missions. However, forecasting space weather is very difficult and is still at an early stage often considered comparable to weather forecasting in the 1960s.

11. Disturbances such as CMEs take 15–72 hours to travel from the sun to Earth. Particularly key to the prediction of Earth-impacting CMEs are the UK-led Heliospheric Imagers flying aboard the twin NASA STEREO¹⁹ spacecraft, which have been developed by the Rutherford Appleton Laboratory and the University of Birmingham. These UK instruments are the only systems able to image Earth-impacting CMEs, from out of the Sun-Earth line, enabling tracking of CMEs from the Sun to the Earth. This pioneering work is central to current research into CME arrivals at Earth and is funded by STFC and the UK Space Agency.

12. Despite this technology, it is only possible to provide a reliable warning of the extent of impact of the CME within an hour or so, as we need to measure the direction of the interplanetary magnetic field as it passes the Earth. More research to understand the basic physics and to develop better models is required to improve the reliability of forecasts.

13. The US Space Weather Prediction Center (SWPC), part of the National Oceanic and Atmospheric Administration (NOAA) is currently the major agency providing space weather services. The UK Met Office has agreed to a request from the NOAA to "mirror" the services provided by SWPC recognising the Met Office's strengths in reliable 24/7 operational service delivery.

14. The European Space Agency's (ESA) Space Situational Awareness (SSA) Programme²⁰ objectives are to support Europe's independent utilisation of, and access to, space through accurate information about the space environment, with particular regard to hazards including space weather, posed to infrastructure in orbit and on the ground.

15. NERC strategy is focussed around seven science themes,²¹ one of which, Natural Hazards, recognises the importance of space weather.²²

¹⁸ Dyer, C S, Lei, F, Clucas, S N, Smart, D F, & Shea, M A, 2003. Solar particle enhancements of single event effect rates at aircraft altitudes, IEEE Trans. Nucl Sci, vol 50, No 6, pp 2038–2045.

¹⁹ http://www.nasa.gov/mission_pages/stereo/main/index.html

²⁰ http://www.esa.int/esaMI/SSA/SEMYTICKP6G_0.html

²¹ <http://www.nerc.ac.uk/research/themes/>

²² <http://www.nerc.ac.uk/research/issues/naturalhazards/>

16. The NERC funded British Antarctic Survey (BAS) has worked with a consortium of UK insurance companies to forecast periods of high risk to satellites. BAS now leads an international project called SPACECAST to develop European modelling and forecasting capabilities in order to protect satellites on orbit from high energy particle radiation. This is a research project that will also deliver an initial forecasting capability from March 2012 onwards via a public web site, and issue warnings and alerts for stakeholders who sign up to the service. The forecasting will be provided on a best efforts basis and will lay the foundation for an operational service. The project is funded by the EU under Framework 7 and involves 7 European partners and 4 collaborations with the USA. SPACECAST is funded for three years up until the end of February 2014.

17. The NERC funded British Geological Survey (BGS) has developed a suite of space weather monitoring and forecasting services over a number of years following work for the ESA and Scottish Power. For example, BGS has access to real-time data from the UK and many other magnetic observatories around the world and is able to estimate measures of geomagnetic disturbance in near real time. BGS has worked closely with Met Office in the Natural Hazards Partnership (NHP). Since March 2011 BGS has been delivering daily magnetic activity forecasts and real time data, indicating UK and global magnetic activity conditions, for inclusion in a pilot daily hazards report issued by the Met Office as part of NHP activities.

18. Another important ground based technology of relevance is the LOw Frequency Array (LOFAR),²³ a multi-purpose sensor array whose main application is astronomy at low frequencies (10–250 MHz). LOFAR supports UK and international efforts to demonstrate interplanetary scintillation as a complementary method to monitor CMEs and other heliospheric transients, thereby improving resilience of the global space weather monitoring capability, particularly if space based technologies were to fail. The first LOFAR station to be built in the UK was opened at STFC's Chilbolton Observatory in September 2010.²⁴

19. Appendix 1²⁵ provides an audit of potential UK based space weather assets including those supported by NERC and STFC, prepared recently (November 2009) as an input to ESA's SSA programme. It can be seen as one measure of the UK's "preparedness" to predict, monitor and analyse the effects of space weather, or the UK's "National Capability" in respect to space weather and solar storms. The extent of the UK commitment to the SSA programme, via UKSA, will need to be determined as part of the wider UK strategy for engagement with ESA.

Question 4. *The potential impact of such events for both civilian and military infrastructure*

20. The largest space weather event on record occurred in 1859. A number of reports have examined the impacts of a similar event today,²⁶ with the US National Research Council giving an estimate of \$1–2 trillion for the wider societal and economic costs of a severe geomagnetic storm scenario.²⁷ The Lloyds and RAL²⁸ Space Weather Report explores the threat to business and included input from BGS.²⁹ The Space Environment Impacts Expert Group (SEIEG) chaired by member of staff from STFC and including BAS and BGS representation has helped the Civil Contingencies Unit of the Cabinet Office to evaluate potential impacts of space weather.

21. There are more than 600 satellites in orbit providing essential services including TV, banking, internet, remote sensing, navigation, and security. During a space weather event the Van Allen radiation belts can intensify 10,000 fold or more resulting in satellite charging and damage to electronic components. Solar energetic particle events can also reduce solar array power and satellite lifetime. Three satellites in the radiation belts were damaged in one event in 1994, leading to serious loss of service, and satellite losses occurred in 1997, 1998 and 2003 during the last solar cycle. Many other satellites have been damaged or lost over the years but it is not clear if those losses were due to space weather. Past experience shows that the highest space weather risk to satellites will occur two years after the peak in the sunspot cycle, sometime in 2015.

Impact on positioning, navigation and timing services

22. An important space-based infrastructure is positioning, navigation and timing (PNT) services delivered by Global Navigation Satellite Systems, predominantly the US Global Positioning System (GPS). Navigational applications of GPS are now commonplace and the use of GPS-derived time has become integral in areas as diverse as scientific monitoring, telecommunications, and financial transactions and services. Implications of loss of PNT services caused by space weather have been highlighted in a report by the Royal Academy of Engineering.³⁰ PNT services may be degraded by direct effects of space weather on satellite infrastructure.

23. Disturbance to the ionosphere may also impact PNT services. On the ground, GPS receivers rely on receiving radio signals from the GPS satellites. During magnetic storms the ionospheric density profile changes,

²³ <http://www.lofar.org/astronomy/solar-ksp/solar-physics-and-space-weather>

²⁴ <http://www.lofar-uk.org/index.html>

²⁵ Appendix 1—UK space weather assets as published by ESA in tender 2010.pdf

²⁶ <http://www.nerc.com/files/HILF.pdf>

²⁷ <http://www.nap.edu.catalog/12507.html>

²⁸ Based at STFC's Rutherford Appleton Laboratory, RAL Space is at the forefront of UK Space Research—<http://www.stfc.ac.uk/ralspace/default.aspx>

²⁹ <http://www.lloyds.com/News-and-Insight/360-Risk-Insight/Research-and-Reports/Space/Space-Weather>

³⁰ Royal Academy of Engineering (2011). *Global Navigation Space Systems: reliance and vulnerabilities*, ISBN 1–903496–62–4. (<http://www.raeng.org.uk/gnss>)

affecting the propagation time of the radio signals, which leads to positional errors. Magnetic storms can also result in loss of signal lock by receivers. In addition, solar radio bursts can overwhelm GPS satellite signals leading to loss of service for periods of several hours.³¹

Impact on aviation and shipping

24. Disturbance of the ionosphere can have particular impacts on aviation and shipping. SEP events can lead to loss of high frequency communications in the polar-regions for 24 hours or more requiring aircraft on polar routes to be re-routed, adding considerably to the flight costs. Solar flares can also produce communications blackouts for a few hours. A space weather event disrupted trans-Atlantic aviation in 2005. See also paragraph 28.

Impact on power supply

25. GICs pose a threat to electricity distribution grids extending over long distances which can cause blackouts and damage. Permanent damage to transformers caused by GICs is a major concern. Transformers are costly, not available as “off-the-shelf” items, and replacing one is a major exercise. The consequences of a prolonged loss of electrical power are potentially catastrophic as the infrastructures and services that modern developed societies rely on are entirely dependent on electricity. Examples include heating, lighting, refrigeration, communications, pumping of fuel, water and sewage.

26. It has been estimated that if a magnetic storm that occurred in May 1921 was repeated today then 130 million people in the US would lose their electricity and more than 350 transformers would be at risk of permanent damage.³² A large space weather event caused power blackouts across North-Eastern Canada in March 1989. Quebec was blacked out for 9 hours, millions of people without electricity. During the same storm a large step-up transformer at the Salem Nuclear Power Plant in New Jersey was damaged.

Question 5. *Ways of mitigating electromagnetic pulse events, either targeted or naturally occurring*

27. Warning and prediction of space weather events is one of the most important ways of mitigating effects. Essential systems can then be put into a safe mode, but this may not always ensure survival.

28. There are a number of mitigating possibilities to help protect satellites in the aftermath of an EMP or severe space weather event. Scientific research at the BAS on natural radiation belts has shown that various types of electromagnetic waves can remove energetic charged particles so that they are deposited down into the atmosphere. Once in the atmosphere they are quickly absorbed. A potential mitigation process is to increase the rate of scattering and particle loss by these waves. This might be done by:

- Injecting very low frequency and extremely low frequency waves into space from ground based transmitters;
- Transmitting very low frequency waves from satellites in orbit;
- Releasing chemicals from rockets which generate waves in space by natural wave-particle interactions.

29. These ideas are at the research stage and are led by the USA. The UK has considerable expertise in wave-particle interactions through its research on space weather and radiation belts at BAS.

30. Satellite operators attempt to mitigate the effects of space weather by hardening chips against radiation and by using multiple circuits so that a malfunctioning circuit can be outvoted by ones that are operating correctly. However, during the so-called Halloween magnetic storm in October/November 2003 more than 47 satellites reported anomalies and one scientific satellite was a total loss.

31. The use of dual-frequency receivers can help overcome the effect of magnetic storms on the propagation time of the radio signals from GPS satellites to GPS receivers.

32. Aircrew on long-haul flights are classified as radiation workers by the European Union and frequent flyers are also at risk.³³ The only mitigation strategies to reduce exposure during a radiation event are to fly at lower altitude to increase atmospheric shielding or re-route to lower latitudes.

33. ISIS pulsed neutron and muon source at Rutherford Appleton Laboratory³⁴ is in the build phase of Chipir,³⁵ a new experimental facility which will study how microchips’ operations are severely disrupted by cosmic radiation, one of the first dedicated resource of its kind outside the US. Chipir will be world leading with unique capabilities for screening microchips with neutrons and will enable the development of more

³¹ Cerruti, A P, P M Kintner Jr, D E Gary, A J Mannucci, R F Meyer, P Doherty, and A J Coster. 2008. Effect of intense December 2006 solar radio bursts on GPS receivers, *Space Weather*, 6, S10D07, (doi:10.1029/2007SW000375)

³² US National Academy of Sciences, 2008. Severe Space Weather Events—Understanding Societal and Economic Impacts, Workshop Report. ISBN: 0-309-12770-X. (<http://www.nap.edu/catalog/12507.html>)

³³ Hapgood, M A & Thomson, A W P. 2010. Space weather: its impact on Earth and implications for business. Lloyds 360° Risk Insight Briefing.

³⁴ <http://www.isis.stfc.ac.uk/>

³⁵ <http://www.isis.stfc.ac.uk/instruments/Chipir/>—including detailed technical specifications.

resilient electronic systems. The project received funding in March 2011³⁶ from the UK Large Facilities Capital Fund.³⁷

34. Possible mitigation strategies to reduce the threat to electrical power distribution systems include fitting blocking capacitors to the earth connections of transformers and management of the distribution of load throughout a grid system to protect the components most at risk. Risk assessments require the identification of a “reasonable worst case” that a system should be designed to be resilient to, or for which an adaptation strategy should be developed. The statistical distribution of extreme events is required, but for a number of the space weather effects the available data are limited. This is not the case for magnetic disturbances as magnetic observatories have been in operation for more than 160 years. Analyses on data from European magnetic observatories to estimate the size of major geomagnetic storms using extreme statistics methods have been carried out.³⁸

35. NERC/BGS and STFC/RAL Space were co-sponsors of a workshop on Geomagnetically Induced Currents in National Power Grids held at Lancaster University on 30–31 March 2011. This workshop was led by Lancaster University using impact funding from EPSRC. It brought together UK and international experts from science, industry and government to discuss the space weather threat to power grids and was a welcome opportunity to exchange ideas and develop links between experts from different communities.

36. In partnership with National Grid, BGS has developed a range of scenarios and modelled the effects on a simplified representation of the UK high voltage grid to identify transformer “hot spot” locations. National Grid has, in parallel, been considering the engineering and supply consequences of these scenarios. BGS has been commissioned by National Grid to provide a geomagnetic hazard monitoring and analysis service and is working with National Grid to improve models of the high voltage system, to enable more accurate assessments of space weather impacts on the UK grid system. BGS is also a partner in the EU Framework 7 project EURISGIC, carrying out research into the generation and impacts of Geomagnetically Induced Currents on power distribution networks.

37. The adoption of optical cables for most telephone and internet communications makes them largely immune to space weather effects. Transoceanic cables have electronic systems to amplify signals which introduce a potential but relatively minor vulnerability. The ability of relatively recent and rapidly developing wireless technologies including mobile phones, wireless internet and device controllers to reject interference from radio bursts has not yet been established by exposure to significant events as their widespread adoption has been recent and during a quiet period in solar activity.

Question 6. *The resources available in respect of research and development in this field*

38. The UK has over 100 years’ leadership in the science underpinning our understanding of space weather. This continues today with the UK Research Councils, in particular NERC and STFC, acting as the significant funders of relevant research programmes.³⁹ Research Council commitment is broadly split between ground-based and space-based studies with NERC funding Earth orientated solar terrestrial physics and STFC funding space based activities. There are many inter-relationships between the various areas of research. UK scientists are world leaders at combining data from ground-based and space-based studies.

39. SEIEG provides a forum for developing research plans and the Met Office, which is one of the founder members of SEIEG, is playing an important part in work being carried out by the World Meteorological Organisation (WMO) on space weather.

40. The following are examples of significant recent Research Council activity:

- STFC is currently finalising negotiations with the EU Commission for a 5M Euro FP7 project to establish an advanced data system to facilitate scientists’ access to databases essential for research across all aspects of space weather. The project, which involves 22 partners from the UK, the rest of Europe and from the US, will be led by a team in RAL Space.
- STFC is leading preparation of a bid for up to 10M Euro FP7 funding to coordinate and improve the networks of European ground-based sensors that provide measurements critical to space weather research. If successful, this bid will enable instrument groups in the UK and the rest of Europe to provide high-quality ground-based measurements that are an essential complement to space-based measurements, such as those being developed by ESA. This mix of ground-based and space-based measurements is critical to advancing the quality of space weather forecasts.

³⁶ <http://www.isis.stfc.ac.uk/news/2011/speech-by-david-willetts-minister-for-science-at-isis11743.html>

³⁷ <http://www.rcuk.ac.uk/research/Infrastructure/Pages/CapitalFund.aspx>

³⁸ Thomson, A W P; Gaunt, C T; Cilliers, P; Wild, J A; Opperman, B; McKinnell, L-A; Kotze, P; Ngwira, C M; Lotz, S I. 2010. Present day challenges in understanding the geomagnetic hazard to national power grids. *Advances in Space Research*, 45 (9). 1182–1190. (doi: 10.1016/j.asr.2009.11.023)

³⁹ From 2008 responsibility for ground based research transferred from STFC to NERC and amounted to approximately £2.7 million per annum. The space-based research programme funded by STFC currently amounts to approximately £1 million per annum, but is difficult to accurately define given the many crossovers. These figures do not include spend on post-launch support or new mission development (eg ESA’s Cosmic Vision Solar Orbiter mission) and this aspect is now managed by the UK Space Agency.

-
- STFC/RAL Space was a key part of the organising team for Space Weather and Society workshop that took place at NASA Ames Research Centre in California over the weekend of 15/16 October 2011. This workshop aimed to establish a plan for linking space weather expertise with societal and economic needs. STFC provided the key international input to complement internal US expertise in the organising team. The UK attendees included representatives from STFC, NERC, industry and Government.
 - NERC are developing significant collaborations with research groups across Europe and the USA on space weather (eg via three Framework 7 projects at the British Antarctic Survey and through another involving the British Geological Survey). It is also developing an integrated approach where BAS and BGS are co-operating to develop computer models to forecast space weather which utilise a variety of ground and space based data.
 - A UK-US workshop on space weather research coordination in Boulder, Colorado on 11–14 October was sponsored by the FCO Global Partnership programme. The workshop involved experts from STFC, NERC, the universities and Met Office, plus their counterparts from the US, and will result in a roadmap for future collaboration on science to advance the mitigation and forecasting of adverse space weather.
 - See also responses to Q3 including reference to assets.
 - Also with reference to Q3 (paragraph 11), the STEREO Heliospheric Imager data are being made available to the public through a project known as Solar Stormwatch,⁴⁰ and this has enabled thousands of people worldwide to identify and track CMEs. This is a successful and on-going pilot study for crowd-sourcing techniques, mobilising effort that cannot be duplicated otherwise, and it is consistent with a UN approach for crowd-sourcing as a tool for hazard mitigation and which is being applied to a number of disaster planning scenarios.

Question 7. *Contingencies in place to react to a large-scale loss of UK electronic infrastructure, and the role of the military in such an event*

41. Nil response.

Question 8. *The broader security of UK electronic and space infrastructure, particularly satellites and satellite navigation systems and the risk posed by space debris*

42. Nil response.

October 2011

⁴⁰ <http://www.solarstormwatch.com/>

APPENDIX 1

UNITED KINGDOM				
<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Merlin Radiation Detector	QinetiQ	QinetiQ	Sensor(s)	Small space environment monitor capable of being fitted to various spacecraft to provide wide ranging environmental information
Real time space weather data	STFC	STFC	Data	Access to real time data from the NASA STEREO mission via the SSTD ground station
Real time space weather data	STFC	STFC	Data	Access to real time data from the NASA/NOAA ACE mission via the SSTD ground station
Skynet 5 comms facilities	Paradigm	Paradigm	Other	Extensive ground infrastructure for networking comms with ability to serve overseas sites and link to all UKK SSA related facilities
Ionosonde in Slough, Falklands, South Georgia			Sensor(s)	
GPS station network			Sensor(s)	
SAMNET magnetometer network		Lancaster University	Sensor(s)	Stations in: UK, Faroe islands, Iceland & Russia
Magnetometers		BGS	Sensor(s)	
EISCAT (UK support)		STFC/RAL	Expertise	Located at Eskdalemuir, Hartland, Lerwick
Ionospheric modelling		Leicester University, Lancaster University	Expertise	Supports and coordinates UK related EISCAT activities
IRIS: imaging riometer		Lancaster University	Sensor(s)	Located in Finland
CUTLASS (Co operative UK Twin Located Auroral Sounding System)		Lancaster University	Sensor(s)	HF radars at Pykkvibær, Iceland, and Hankasalmi, Finland .Part of global international Super Dual Auroral Radar (SuperDARN) .Group also has several scientific instruments located in the arctic. The CUTLASS data are made available in real time via website .SuperDARN cross polar cap potential maps for the northern hemisphere, to which the CUTLASS data contribute, are also available in real time from APL website
Expertise in solar s/c instrumentation		University College London/MSSL	Expertise	Flown relevant instrumentation on SOHO, Yohkoh, Hinode + others
Expertise in solar s/c instrumentation		STFC/RAL	Expertise	Flown relevant instrumentation on SOHO, STEREO + others
EGSO		Hosted at UCL/MSSL	Service	GRID test bed aimed towards simplifying access to heterogeneous solar data. Currently operating at pilot
SOARS: Spaceweather Operational Air-lines Risks Service		University College London/MSSL	Service	Pilot service, part of the ESA space weather applications pilot project & member of SWENET
Solarmetrics		Commercial	Expertise	Startup geared towards providing space weather information and services to airlines

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
CEDEX radiation monitor Expertise in space plasma s/c instrumentation		Surrey University University College London/MSSL	Sensor(s) Expertise	Flown relevant instrumentation on eg Cluster
Incoherent radar Malvern DIFS: Daily Ionospheric Forecasting Service	Bae Systems	Bae Systems (UK)	Sensor(s) Service	Nowcast and forecast HF and SATCOM signal propagation conditions
BINCASTS: Index Nowcast and Forecast	BGS	BGS (UK)	Service	Indices now and forecast
SWIMIC: Solar Wind Monitoring and Induction Modelling for GIC	BGS	BGS (UK)	Service	Nowcast and forecast GIC in Scottish power grid
SOARS: Spaceweather Operational Airlines Risks Service	MSSL/UCL	MSSL/UCL (UK)	Service	Service for airlines focussing on radiation and communication issues
GEOSHAFT	QinetiQ	QinetiQ (UK)	Service	Radiation hazard nowcast and alert at GEO
STIF	STFC/RAL	RAL (UK)	Service	Ionospheric propagation parameters for European region
ASAP	Bradford University	Bradford University(UK)	Service	Forecast solar flare activity
EDAM	QinetiQ	QinetiQ	Service	3D electron density model
HOTRAY		British Antarctic Survey	Software	Ray tracing code for calculating the path, amplification and absorption of electromagnetic and electrostatic waves in hot magnetised plasmas. Potential applications to Galileo signals
PADIE		British Antarctic Survey	Software	Computer code for calculating pitch angle and energy diffusion rates for wave particle interactions in connection with radiation belts. Potential applications to space weather modelling
BAS dynamic global radiation belt model		British Antarctic Survey	Software	Computer code for dynamic modelling of the Earth's radiation belts in 3d. Potential applications to space weather modelling
Global magnetic field models (eg scientific, International Geomagnetic Reference Field and World Magnetic Model)		British Geological Survey	Expertise	Leadership role in International Geomagnetic Reference Field
UK regional magnetic field model		British Geological Survey	Service	
Magnetic index forecast codes		British Geological Survey	Service	Includes services that contribute to SWENET
GIC analysis code for UK		British Geological Survey	Software	
Atmospheric radiation model		QinetiQ	Expertise	

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Synthetic Aperture Trans Ionospheric Radio Propagation Simulator (SAR TIRPS)		QinetiQ	Software	
Kinetic modelling of coronal mass ejections		STFC/RAL	Expertise	
Integration of UCL GCMs with lower atmosphere GCMs		UK Met Office	Expertise	
Terrestrial thermosphere/ionosphere models		University College London	Software	CMAT2 goes from 15km to 500km plus plasmasphere and high latitude connection into the magnetosphere
Thermosphere/ionosphere models for other planets, eg Mars, Jupiter		University College London	Software	
MIDAS ionospheric tomography/data assimilation software for ionospheric specification		University of Bath	Software	
Automated Solar Activity Prediction Tool		University of Bradford	Service	Used for detection and classification of sunspot groups, and solar flare prediction. It is online and near real time. http://spaceweather.inf.brad.ac.uk/ Contributes to SWENET
SHARE radar—now called the Halley SuperDARN radar. Measurements of winds, tides and waves in the mesosphere and ionosphere. Part of global international Super Dual Auroral Radar		British Antarctic Survey	Sensor(s)	Operated by BAS from 1988 to 2008 . Will resume operations at Halley 6 in Jan 2012.
New Falkland Islands radar—to start about 2010		British Antarctic Survey	Sensor(s)	
Meteor radar at Rothera		British Antarctic Survey	Sensor(s)	
Imaging riometer, being moved to Halley 6		British Antarctic Survey	Sensor(s)	
AARDDVARK network of radio receivers for measuring electron precipitation		British Antarctic Survey	Sensor(s)	
Search coil magnetometer, Halley 6		British Antarctic Survey	Sensor(s)	

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Pulsation magnetometer, Halley 5, will move to Halley 6.		British Antarctic Survey	Sensor(s)	
VELOX at Halley, for whistler detection and substorms		British Antarctic Survey	Sensor(s)	
Low power magnetometer network, poleward of Halley		British Antarctic Survey	Sensor(s)	
AIRIS riometer in Norway/ALOMAR		Lancaster University	Sensor(s)	
Ny Alesund imaging Riometer		Lancaster University	Sensor(s)	In collaboration with China (PRIC)
Rainbow all sky camera network in Iceland and Faroes		Lancaster University	Sensor(s)	During darkness and clear sky
Ionosonde at Tromsø		QinetiQ	Sensor(s)	Real time data goes to SWPC Boulder
GPS receivers		QinetiQ	Sensor(s)	
CREDANCE monitor to fly with NASA Living with a Star		QinetiQ	Sensor(s)	Will monitor accumulated dose, energetic protons, heavy ion LET spectra, electron fluxes and charging currents. Approx launch date 2012
Space Environment Testbed				
EMU monitor to fly on Galileo.		QinetiQ	Sensor(s)	Similar capabilities to CREDANCE but additional proton channels
QDOS aircraft radiation monitor		QinetiQ	Sensor(s)	To fly regularly on high latitude flights
Ionosondes at Chilton and Port Stanley		STFC/RAL	Sensor(s)	Real time data supports DIAS system and hence SWENET services. Real time data goes to SWPC Boulder and hence to end users including MOD
Ground station: 12m S band uplink/downlink antenna system		STFC/RAL	OT	Past space weather use: STEREO beacon mode (now too far away); ACE real time solar wind (superseded by DLR service in Sep 2009)
2.4m S band downlink antenna system				
4.5m S band/X band downlink antenna system				
Heliospheric Imager on NASA STEREO spacecraft		STFC/RAL	Sensor(s)	
Fabry Perot measurements of thermosphere winds and temperatures in Svalbard and Scandinavia		University College London	Sensor(s)	During darkness and clear sky

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Scanning Doppler Imager (SCANDI) measurements of thermosphere winds and temperatures		University College London	Sensor(s)	During darkness and clear sky
GPS receivers		University of Bath	Sensor(s)	
LEO beacon receivers		University of Bath	Sensor(s)	
Meteor radars		University of Bath	Sensor(s)	
Meridian chain of GPS scintillation receivers, jointly run with Bath:		University of Nottingham	Sensor(s)	
operational: Tromsø, Trondheim, Nottingham, Dourbes, Lagos (Nigeria) to be deployed: Kiruna, Lerwick, Aberdeen, Shrewsbury, Cyprus, northern Nigeria				
Magnetic field		Imperial College	Sensor(s)	Cluster, Rosetta, Ulysses, Cosmic Visions, cubesat
Thermal electrons (<1 eV to 30 keV)		MSSL	Expertise	Cluster, CRRES, Cassini, Cosmic Visions, miniaturisation studies
EUV spectroscopy		MSSL	Expertise	Hinode
Radiation dose		QinetiQ	Expertise	Shuttle, Concorde, Giove,
High res space cameras		STFC/RAL	Expertise	STEREO (HI, EUVI, COR), SDO (AIA, HMI), SMEI, GOES
EUV spectroscopy		STFC/RAL	Expertise	SOHO
Medium energy (30 keV - 1 MeV) particle detectors		STFC/RAL	Expertise	Cluster, Cosmic Visions
Radiation dose		Surrey	Expertise	Giove
CRRES satellite wave and particle database			Data	
World Data Centre for Geomagnetism			Service	
CHIANTI			Expertise	Atomic Database for Spectroscopic Diagnostics of Astrophysical Plasmas
ADAS			Expertise	Atomic Data and Analysis Structure
GAIA-VXO			Service	Global Auroral Imaging Access
UK Solar System Data Centre			Service	Data & models for solar and STP studies
PROMPT ionospheric database			Data	World Data Centre C1 for STP Developed as UK input for COST-271

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Solar archives CSDSweb STPDF			Service Service Software	Data from SOHO, STEREO and TRACE Magnetospheric near realtime conditions using Cluster Data access system for STP/space weather data. Key data access component of ESA's SEDAT system
Clustran Database of Fabry Perot measurements of thermospheric winds and temperatures Daily Ionospheric Forecasting Service		BAE SYSTEMS Advanced Technology Centre British Geological Survey	Software Data Service	Library for coordinate transformations. Used in ESA's SEDAT system 30 years data, mostly over Scandinavia but also occasionally elsewhere Contributes to SWENET
Commercial applications of geomagnetic data and science, eg for oil and gas exploration and recovery and in navigation Geomagnetic hazard modelling and analysis, eg for power system operators AuroraWatch UK		British Geological Survey	Expertise	Includes services that contribute to SWENET
Space Weather Operational Airline Risks Service Spacecraft Hazard And Anomaly Forecasting Tool EDAM533 real time HF propagation prediction service Space-based auroral imagers, primarily at UV but also possibly at X ray wavelengths TRIO CINEMA—3 cubesat mission with US and Korea.		Lancaster University MSSL QinetiQ QinetiQ University of Leicester Imperial College London	Service Service Software Service Sensor(s), Expertise Sensor(s)	Over 25,000 subscribers Contributes to SWENET Contributes to SWENET Web service that provides HF propagation information based on the EDAM real time ionosphere. Access if controlled. Derived from systems on XMM and Swift Imperial College to supply magnetometer. Launch early 2012. http://mstl.atl.calpoly.edu/~bklofas/Presentations/DevelopersWorkshop2009/2_Science/4_GlaserCINEMA.pdf GIOVE A plus other Galileo GPS
Proton, electron fluxes, ion LET spectra, total dose, charging currents		QinetiQ	Sensor(s)	

<i>Asset name</i>	<i>Owner</i>	<i>Operator</i>	<i>Type of asset</i>	<i>Brief description of the asset</i>
Particle fluxes, aircrew ambient dose equivalent Solar wind physics		QinetiQ Imperial College London	Expertise Expertise	Various regular airflights

Supplementary written evidence from Avi Schnurr, Chair and CEO, Electronic Infrastructure Security Council

During the oral evidence session that took place before the Defence Select Committee on 9 November 2011, Committee Chair Rt Hon James Arbuthnot MP requested that witnesses follow up after the session with any comments relating to witness testimony. This letter is submitted in response to that request.

The Defence Committee's investigation into electromagnetic threats to infrastructure seems both important and timely, and could provide leadership in an area increasingly recognized as vital to the continued health and wellbeing of developed nations world-wide.

In the discussion below I attempt to provide additional information, especially in regard to comments made by other witnesses that seem to require clarification. Please let me say, at the outset, that it is clear that all the witnesses are committed to assuring the security and resilience of the UK grid. It was an honor to testify along with these government officials and corporate representatives, and I am confident that any divergence in testimony is simply an expression of differences in opportunities to study this field. With detailed studies, extensive modeling and laboratory testing on grid vulnerability to EMP beginning in the United States more than ten years ago, and corresponding detailed evaluation of grid vulnerability to Carrington-class severe space weather beginning three years ago, the U.S. institutions referenced in my testimony have had time and resources to become deeply involved in studying this issue. I count myself privileged to represent their findings, and doubly privileged to have the opportunity to provide evidence to the Defence Committee.

In his testimony, Chris Train made reference to two factors as principal reasons for the National Grid Electricity Transmission (NGET) assessment of substantially lower risk from severe space weather for the United Kingdom than for the United States: The United Kingdom, he indicated, has shorter transmission lines, and its grid is run with less loading than in the United States. There was also a reference to the lower frequency used in the U.K. grid, and an assessment of the vulnerability of individual transformers.

As Chris Train mentioned in his testimony, co-validation or finalization of the differences between U.K. and U.S. modeling is incomplete. It is hoped that the following discussion can help shed some light on the above considerations, and will have utility for follow-on work.

1. *The risk factors for power grid exposure to severe space weather are complex*

The risk factors that cause Ground-Induced Currents (GIC) in Extra High Voltage power grids are complex and diverse, and cannot be meaningfully expressed as simply a function of the lengths of the longest transmission lines. Important factors include:

- The geomagnetic field threat environment, typically worse for higher latitude countries such as the U.K.
- Geological coupling and extent of coastal boundaries.
- The design and density of the power grid network and its operating voltages.
- The design and present condition of specific equipment, such as large transformers and generators.

With no design codes, to-date, that have taken severe electromagnetic threats into consideration, the trend of changes in network designs in modern nations has been, unknowingly, to cause exponential increases in vulnerability.

2. *On the impact of shorter transmission lines in the U.K. vs the U.S.*

The idea that shorter individual transmission lines would act to minimize electric grid risk is a not-uncommon misconception in the electric power industry, when trying to understand how geomagnetic storm disturbance environments couple with electric power grids.

Since individual lines are all interconnected, GIC flows couple across an entire regional network. To understand this coupling GIC flow must be computed on the complex network topology as a whole. In the UK, even across just England the grid extends as much as 500 km north to south and over 400km east to west, and the grid has multiple lines interconnected in all directions across the country, including interconnections and extensions across all of Scotland. Projections of GIC flow and coupling to the storm environment must address the larger interconnected network, not just the length of individual lines, even the longest lines, within that interconnected network.

U.S. example: As an example, a similar misunderstanding characterized earlier discussions of this issue by electric utility companies in the densely configured power grid of the U.S. mid-Atlantic region, where lines are much shorter than in other more sparsely populated regions. In fact, based on detailed grid modeling, the dense, concentrated regions of the US grid have the highest GIC problems, and are at the greatest risk.

European example: In other European power grids of similar design to those in the UK, very large GIC's have been observed for relatively minor storm events. For example a GIC of over 300 amps was observed in the 400kV system of southern Sweden on 6 April 2000 at the Simpevarpe nuclear plant, in a region where the east-west distance is only ~270km.

GIC levels can, in any case, be quite large even for individual lines: Even simple, “back of the envelope” calculations can illustrate this. For example, using the typical resistances for 400kV transformers and transmission lines on the NGET network, a single 100km line would typically see 65 Amps of GIC in the neutral of each transformer for a small storm, with just 1 V/km geo-electric field. Increasing the storm environment to just 5 V/km increases the GIC to ~330 Amps in each transformer. Multiple lines and increased network density add multiple GIC flows in exposed transformers.

Possible follow-up questions: Was a complete model of the U.K. electric grid developed and run? Were the non-NGET grid transformers associated with large generators included? If such a comprehensive model was developed and run, it would be helpful to see the actual estimated GIC and the estimated geo-electric field intensity that was used for the severe storm scenarios examined.

3. The UK grid is run with less loading than typical in the US

While load levels can play some role, typical transformer load levels are not a key factor in predicting grid vulnerability: even unloaded transformers can be driven beyond over-excitation specifications with long duration, minimal GIC levels. Today’s transformer design standards do not allow for long duration over-excitation of even 10%, even for transformers with no load on them. Driving a transformer to 10% over-excitation requires only a very small GIC, and there are processes from storm events that can produce low level GIC’s for long duration. Indeed it is this process that is believed to be the cause of the transformer failures in South Africa’s grid during the Oct 2003 storms.

Even unloaded transformers can be driven beyond over-excitation specs for moderate level GICs of very short duration. Present standards only allow a level of 40% over-excitation for as little as 10 seconds even on an unloaded transformer. Even moderate levels of GIC can produce 40% over-excitation.

Possible follow-up questions: If full-grid GIC models were run, did scenarios include long duration, low level or moderate level GIC levels? Were comparison statistics developed, based on measurements and computations, for the typical load levels of the U.K. and U.S. grids? If so, these levels, and their measurement and computational basis would be helpful and instructive.

4. The UK grid operates at a lower frequency than the US grid

Grid operation at 50 Hz in the U.K. and Europe requires a proportionate increase in transformer core steel vs. the 60 Hz US operation frequency. However, at 50 Hz the pulse of GIC-caused half cycle saturation is also proportionately longer than at 60 Hz. As a result, the net impact is that the advantage of the larger volume of core steel is offset by the longer duration core steel exposure to half-cycle saturation. These two effects would act to largely offset each other: the net difference between 50Hz and 60 Hz operation may not be significant. Other design factors such as resistance of lines and efficiency of the transformers and operating voltage are the most important factors in determining GIC risk for a network design.

5. NGET has determined which of its transformers are vulnerable, as part of its detailed modeling

Given today’s technology, most or all transformers installed in power grids remain vulnerable: The issue of transformer vulnerability to GIC has been reviewed extensively over the past year within the North American power industry, with the active engagement of major transformer manufacturers. To summarize, to-date there has been no acceptance that GIC-invulnerable transformers can be manufactured. For example, in a proposed new, GIC-invulnerable design recently submitted by a manufacturer, heating in core and tank areas indicated they would exceed design standards for levels of GIC at ~90 Amps per phase. Of course, the North American power industry discussion also recognized an expected decay in GIC Withstand due to age, heating damage from ongoing GIC exposure, and other aging processes. This makes the effort to even assess the GIC-withstand of existing transformers (planned to remain in the network for several decades longer) exceedingly difficult. Finally, to the knowledge of the U.S. community, existing transformers, world-wide, have not been purchased to any GIC Withstand specifications.

Since most transformer failures due to moderate level GIC are understood to have resulted from difficult-to-predict effects, such as magnetic flux leakage into support structures, accurate assessment of transformer vulnerability requires detailed electromagnetic modeling and thermal finite element modeling for the as-built, current condition of each individual transformer. Even where thermal issues are understood, evidence also was noted for internal arcing processes that occurred during the March 1989 storm that have not been well-modeled and understood.

Possible follow-up questions: There is no known basis for general, grid-wide assumptions as a tool to identify at-risk transformers. Has the above-mentioned detailed, transformer-by-transformer modeling been performed? If not, on what modeling basis does NGET feel the vast bulk of their transformers are not vulnerable to GIC? Were most transformers purchased with GIC Withstand standards? If so, what GIC design ratings were used? How many have actually been purchased and what percentage of the existing network would that represent?

To my knowledge and the knowledge of U.S. power industry experts, no present industry standards have ever been approved or adopted in regard to GIC-Withstand for transformers, including both the IEC and IEEE

standards organizations. However, if in fact such standards were specified, were the transformers tested and demonstrated at the required conditions? Did manufacturers provide a warranty against such standards?

6. *Iran's and North Korea's ballistic missile capabilities*

While David Ferbrache indicated, in response to a question, that he does not believe either Iran or North Korea possess the capability to launch missiles to altitudes of “tens of kilometers,” it seems clear that the question must have been misunderstood.

According to physical law, to reach targets beyond about 160 km ballistic missiles must fly above the earth's atmosphere. A typical maximum range ballistic trajectory is an arch about one fourth as high as it is long. Thus, even a missile with a range of only 160 km would reach an altitude of around 40 km.^{41,42} This is a function of the basic physics of ballistic objects. For more information, physics and mechanics/dynamics texts may be referred to (or, for example, see the below on-line references to the physics of ballistic objects).⁴³

Thus, all ballistic missiles with a range more than around 120 km can meet the conditions for reaching the minimum altitude necessary for an EMP strike. Even the first ballistic missile to reach space, the German V-2, reached an altitude of 97 km, on October 3, 1942.⁴⁴

Iran possesses a variety of missiles such as the Shahab 3 (range 1,200 km) and the Ashura (range 2,000 km), both of which reach altitudes of hundreds of kilometers. In fact, according to many sources, Iran successfully launched the Safir space launch vehicle (SLV), which was used to launch the Omid satellite into space on 2 February 2009.⁴⁵ According to the same Massachusetts Institute of Technology report, North Korea's Taepodong missile achieved even longer ranges, and thus associated higher altitudes, than Iran's missiles.⁴⁶

Dr. William Graham, former Presidential Science Advisor and Chair of the Congressional EMP Commission, noted in testimony to the Senate Armed Services Committee, “Iran, the world's leading sponsor of international terrorism, has practiced launching a mobile ballistic missile from a vessel in the Caspian Sea. Iran has also tested high-altitude explosions of the Shahab-III, a test mode consistent with EMP attack, and described the tests as successful. Iranian military writings explicitly discuss a nuclear EMP attack that would gravely harm the United States.”⁴⁷

In fact, even Hezbollah, possessing the single stage, solid fuel Fateh 110 missile, now has delivery systems that could be used for an EMP strike from a boat. With its 300 km class range,⁴⁸ it can reach a 75 km altitude at maximum range, or over 100km at reduced range. A 100km altitude nuclear detonation, launched from an offshore freighter in the mode referenced by the U.S. Congress EMP Commission,⁴⁹ would create a circle of electric infrastructure damage or destruction slightly larger than a circle containing the United Kingdom and Ireland.

CONCLUDING REMARKS

Even without the clarifications I summarize above, NGET's modeling and projections to-date are, like any such efforts, less than 100% certain. Similarly, given the world's turbulent military history and, for example, the very recent IAEA report on evidence of Iran's nuclear warhead development, leaving one's country open to unprecedented, catastrophic destruction from a single, poorly targeted nuclear “bullet” does not seem to be prudent policy.

If cost effective protection can in fact be demonstrated, installing protection for transformers and gradually upgrading other grid assets against EMP E1 would seem to be an unarguable, obvious course to take.

If this understanding is correct, it suggests a good course of action would be to begin implementing cost effective critical asset E1 protection, and to work toward testing and validation of the various new current blocker technologies that have now been developed.

With some GIC current blocker prototypes now completed, and with one in particular now already developed and tested by one of the world's largest extra high voltage transformer manufacturers, a positive outcome of this process might be for the UK to consider participation in the upcoming, definitive testing now undergoing

⁴¹ Trajectory of a projectile, http://en.wikipedia.org/wiki/Trajectory_of_a_projectile

⁴² Physics of Ballistic Missiles, <http://www.missilethreat.com/overview/pageID.155/default.asp>

⁴³ See, for example: Physics 001: The Science of Ballistics, Gable, Hurley, Chojnicki, Wyka and Hopkins, class.phys.psu.edu/p001/projects/.../48%20%20FinalPresentation.ppt; Physics Tutorial: Projectile Trajectory. <http://www.physics247.com/physics-tutorial/projectile-trajectory.shtml>; Understanding Projectile Motion, Douglas Black. <http://www.helium.com/items/1175843-what-is-projectile-motion-how-does-projectile-motion-work-explaining-projectile-motion>

⁴⁴ Germany's V-2 Rocket, Kennedy, Gregory P.

⁴⁵ *A Technical Assessment of Iran's, Ballistic Missile Program*, by Theodore Postol*, Professor of Science, Technology, and International Security, Massachusetts Institute of Technology.

⁴⁶ Op cit.

⁴⁷ Dr. William Graham Senate Armed Services Testimony, <http://www.empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf>

⁴⁸ Lt. Gen. Ashkenazi, on Fateh 110 capability. <http://dover.idf.il/IDF/English/News/today/09/11/1001.htm>

⁴⁹ U.S. Congress EMP Commission Report, <http://www.empcommission.org/docs/GRAHAMtestimony10JULY2008.pdf>

early planning in the U.S.—ensuring that such testing addresses the full range of UK concerns, sufficient to allow integration of these protective measures into the grid.

Finally, as the Defence Committee's process goes forward, I would be happy to help as much as desired, with the Defence Committee as well as with NGET and other U.K. stakeholders, in providing information and connections to the growing body of evaluation work occurring in the United States and elsewhere.

14 November 2011

Supplementary written evidence from Professor Richard B Horne, British Antarctic Survey

During the oral evidence session of the Defence Select Committee on the 9 November 2011, you invited witnesses to write to the Committee after the meeting with any points of disagreement or clarification. I would like to offer the following points.

Electromagnetic pulse (EMP) has been known since the high altitude nuclear tests in the early 1960s, and the UK defence sector has had 50 years to plan and protect. However, space weather has only recently been put onto the national risk register in 2011. Thus a severe space weather event, such as the Carrington event, is where the emerging risk lies and which is, as yet, unquantified.

The discussion focussed very much on the effects of a nuclear EMP on the power grid. However, I would like to clarify the point I made under question 36 in the transcript. Both high altitude nuclear detonations and severe space weather events release high energy particle radiation, many times the background level, which damage satellites. This radiation is long lived. It remains trapped in the radiation belts for years, reduces the operational life of satellites passing through it, and has caused the sudden loss of satellites. Changes in the radiation levels during space weather events can be more than a hundred times greater than those from a nuclear test, depending on location, and extend over a far greater volume of space. Since we rely so much on satellites, with increasingly small electronic circuits, in my view this is where the new risk lies and where better assessment is essential.

Mr Havard asked about space weather effects under question 41. The Space Environment Impacts Expert Group (SEIEG) has chosen a Carrington event as the "reasonable worst case" to define an extreme environment, the impacts, and thus what is needed to protect infrastructure. I agree with this initial start. But the truth is we do not know how big a space weather event can be. That is because we do not understand the physical processes that set the upper limits, on the sun, the interplanetary medium, the radiation belts, magnetic field or elsewhere, and these systems are all coupled. This is where we must target research. While I believe we must have some initial assessment in place very quickly, we must improve the assessment, and this will require challenging research that will take time.

Mr Russell asked how well the work done by Government, research institutions, and others is co-ordinated under question 51. I do believe that the Government is making real efforts, and I said so. But the Government can do more to utilise resources. One would not dream of going to war without using the Intelligence Services, and in the same way we should not battle space weather without utilising the scientific expertise in the Research Council Institutes and Universities. They are the intelligence service in this arena. Defining an extreme space weather event and its impact is absolutely critical to all the risk assessments, the protection measures and the level and appropriateness of response. The expertise to do this lies with research scientists in the Research Council Institutes and Universities, working with Government and industry. But the research is challenging, requires funding and a strategic approach. At present members of the SEIEG offer their support without additional funding, but this has been at the level of a few days per year and is very limited compared to what is required.

The Government has a very difficult problem to define the impact of a severe space weather event. They need research scientists to help them. However, research on solar terrestrial physics, which underpins space weather, is in competition with other areas of funding and there is no guarantee that projects on space weather will be funded. If the Research Councils do approve a space weather research programme in 2012 it would be 2013 before any research grants were awarded and results would normally follow two to three years later. In my view we cannot afford to wait this long.

Mr Russell also asked who should take responsibility for the emerging risk under question 54. To me this is straightforward. Since space weather can affect nearly all areas of Government, including Transport, Security, Defence, Business and Education there should be a higher authority that takes responsibility and coordinates. To me that is the Cabinet Office. Otherwise, if an event is in progress, how one decides which Department is most affected and should take responsibility is not clear, especially when events can unfold very quickly—in a matter of hours.

I am sorry I was not able to make these points during the witness session, but I enjoyed the experience greatly. Thank you for the opportunity to write to you.

11 November 2011

**Written evidence from officers of the International Electrotechnical Commission (IEC)
Subcommittee 77C**

The authors of this letter are officers of the International Electrotechnical Commission (IEC) Subcommittee 77C and have been leading the effort within the IEC to develop standards and other publications to protect the civil infrastructures of the world against man-made attacks from different types of “EMP”. This work began in 1989 and has focused on two particular “EMP” threats: the high-altitude electromagnetic pulse (HEMP) produced by nuclear detonations in space and Intentional Electromagnetic Interference (IEMI) produced by electromagnetic weapons used by criminals or terrorists. In addition a few of the IEC publications deal with low-frequency HEMP environments that are very similar to the environments created by space weather or more particularly geomagnetic storms, which are natural, but severe threats to the power infrastructure.

The title and scope of IEC SC 77C are:

High Power Transient Phenomena

“Standardisation in the field of EMC to protect civilian equipment, systems and installations from threats by man-made high power transient phenomena including the EM fields produced by nuclear detonations at high altitude. Note—high power conditions are achieved when the peak incident EM field exceeds 100 V/m.”

This committee produces international civil standards and technical reports on protection and test methodologies against high power transients. They are available for use by any country wishing to protect its civil systems against such transients. At the present time the IEC SC 77C is supported by 18 “P” or participating (voting) member countries (including China, Germany, Republic of Korea, Russian Federation, UK, USA) and 16 “O” or observing member countries. As with all IEC standards, they are voluntary until they are adopted by national or regional standards organizations or when they are referenced in contractual documents.

The publication set encompasses 20 documents, which is in fact the most complete set of high power electromagnetic standards available for defining the threats and designing protection measures and test methods to ensure that the protection elements perform according to their specifications. The most recent of these publications deal mainly with IEMI aspects, and these were published over the past five years. Many of the older publications deal specifically with HEMP, and some deal generally with the protection methods available for high-level EM fields at frequencies above 10 MHz, which covers both HEMP and IEMI.

It is important to note that the publications of IEC SC 77C are basic standards that need to be applied to specific products and industries. In recent years the publications of IEC SC 77C have been adapted to the needs of the telecommunications industry by the International Telecommunication Union (ITU-T Recommendations K.78, and K.81) and to the needs of the international power industry in Cigré (WG C4.206 where work is underway).

In order to aid the Defence Committee, we have attached in an annex, the complete list of publications prepared by IEC SC 77C.

26 September 2011

Annex

PUBLICATIONS DEALING WITH THE PROTECTION OF CIVIL EQUIPMENT AND SYSTEMS FROM
THE EFFECTS OF HEMP AND HPEM (IEMI)—ISSUED BY THE INTERNATIONAL
ELECTROTECHNICAL COMMISSION (IEC) SC 77C

IEC/TR 61000-1-3 Ed 1.0 (2002-06): Electromagnetic compatibility (EMC)—Part 1-3: General—The effects of high-altitude EMP (HEMP) on civil equipment and systems. *Basic EMC publication.*

IEC/TR 61000-1-5 Ed 1.0 (2004-11): Electromagnetic compatibility (EMC)—Part 1-5: High power electromagnetic (HPEM) effects on civil systems. *Basic EMC publication.*

IEC 61000-2-9 Ed 1.0 (1996-02): Electromagnetic compatibility (EMC)—Part 2: Environment—Section 9: Description of HEMP environment—Radiated disturbance. *Basic EMC publication.*

IEC 61000-2-10 Ed 1.0 (1998-11): Electromagnetic compatibility (EMC)—Part 2-10: Description of HEMP environment—Conducted disturbance. *Basic EMC publication.*

IEC 61000-2-11 Ed 1.0 (1999-10): Electromagnetic compatibility (EMC)—Part 2-11: Environment—Classification of HEMP environments. *Basic EMC publication.*

IEC 61000-2-13 Ed 1.0 (2005-03): Electromagnetic compatibility (EMC)—Part 2-13: High-power electromagnetic (HPEM) environments—Radiated and conducted. *Basic EMC publication.*

IEC 61000-4-23 Ed 1.0 (2000-10): Electromagnetic compatibility (EMC)—Part 4-23: Testing and measurement techniques—Test methods for protective devices for HEMP and other radiated disturbances. *Basic EMC publication.*

IEC 61000-4-24 Ed 1.0 (1997-02): Electromagnetic compatibility (EMC)—Part 4: Testing and measurement techniques—Section 24: Test methods for protective devices for HEMP conducted disturbance. *Basic EMC Publication*.

IEC 61000-4-25 Ed 1.0 (2001-11): Electromagnetic compatibility (EMC)—Part 4-25: Testing and measurement techniques—HEMP immunity test methods for equipment and systems. *Basic EMC publication*.

IEC/TR 61000-4-32 Ed 1.0 (2002-10): Electromagnetic compatibility (EMC)—Part 4-32: Testing and measurement techniques—HEMP simulator compendium. *Basic EMC publication*.

IEC 61000-4-33 Ed 1.0 (2005-09): Electromagnetic compatibility (EMC)—Part 4-33: Testing and measurement techniques—Measurement methods for high power transient parameters. *Basic EMC publication*.

IEC/TR 61000-4-35 Ed 1.0 (2009-07): Electromagnetic compatibility (EMC)—Part 4-35: Testing and measurement techniques—High power electromagnetic (HPEM) simulator compendium. *Basic EMC publication*.

IEC/TR 61000-5-3 Ed 1.0 (1999-07): Electromagnetic compatibility (EMC)—Part 5-3: Installation and mitigation guidelines—HEMP protection concepts. *Basic EMC publication*.

IEC/TS 61000-5-4 Ed. 1.0 (1996-08): Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guidelines—Section 4: Immunity to HEMP—Specification for protective devices against HEMP radiated disturbance. *Basic EMC Publication*.

IEC 61000-5-5 Ed 1.0 (1996-02): Electromagnetic compatibility (EMC)—Part 5: Installation and mitigation guidelines—Section 5: Specification of protective devices for HEMP conducted disturbance. *Basic EMC Publication*.

IEC/TR 61000-5-6 Ed 1.0 (2002-06): Electromagnetic compatibility (EMC)—Part 5-6: Installation and mitigation guidelines—Mitigation of external EM influences. *Basic EMC publication*.

IEC 61000-5-7 Ed 1.0 (2001-01): Electromagnetic compatibility (EMC)—Part 5-7: Installation and mitigation guidelines—Degrees of protection by enclosures against electromagnetic disturbances (EM code). *Basic EMC publication*.

IEC/TS 61000-5-8 Ed 1.0 (2009-08): Electromagnetic compatibility (EMC)—Part 5-8: Installation and mitigation guidelines—HEMP protection methods for the distributed infrastructure. *Basic EMC publication*.

IEC/TS 61000-5-9 Ed. 1.0 (2009-07): Electromagnetic compatibility (EMC)—Part 5-9: Installation and mitigation guidelines—System-level susceptibility assessments for HEMP and HPEM. *Basic EMC publication*.

IEC 61000-6-6 Ed 1.0 (2003-04): Electromagnetic compatibility (EMC)—Part 6-6: Generic standards—HEMP immunity for indoor equipment. *Basic EMC publication*.

Written evidence from the Royal College of Physicians

The Royal College of Physicians (RCP) plays a leading role in the delivery of high quality patient care by setting standards of medical practice and promoting clinical excellence. We provide physicians in the United Kingdom and overseas with education, training and support throughout their careers. As an independent body representing over 25,000 fellows and members worldwide, we advise and work with government, the public, patients and other professions to improve health and healthcare.

INTRODUCTION

1. The Royal College of Physicians (RCP) welcomes the House of Commons Defence Select Committee's inquiry into Developing Threats to Electronic Infrastructure. We value the opportunity to provide comment.

COMMENTS

2. We believe that it would be appropriate to consider the effect of electromagnetic pulse (EMP) on patients with implantable cardiac devices.

October 2011

Written evidence from Peter Taylor, Ethos Consultancy

I am a writer with a recently developed interest in spaceweather impacts. I am sure that you will receive many detailed submissions in answer to your inquiry which will contain much of the relevant science—I add here some comments which may be of assistance in your assessment of this material.

My own interest was sparked firstly by analysis of ice-core records. This kind of material is unlikely to come your way as it is a difficult area. I have not had the time to evaluate the material fully, nor provide you with a reliable guide to the data—but from what I have seen, it is possible to assess the frequency of “Carrington” type events—I will call them “megaflares”, as they leave a chemical imprint in the ice-core record. The general conclusion is that such events may have a frequency in the range of 1:200 to 1:500 years. Perhaps you would be able to instigate a more detailed analysis.

As you will know the last such event was in 1859.

Given the large potential impact of such an event on modern infrastructure, this is a very high risk, and doubtless why you are now devoting your time to the issue. Of course, this phenomenon is well-known within the science community, and you might usefully ask someone why the issue is only now being addressed.

I, myself, only came across a detailed investigation on publication of the US National Academy of Science report in late 2008, along with the Congressional hearing.

My main points are:

- that report showed that the long-distance electric grid could be disabled to such an extent that repairs might take three to four (optimistically);
- it was not clear to what extent the electronic infrastructure of satellites and terrestrial computer systems and data storage was robust to such an event;
- it was not clear what strength of solar EMP was required to disable vehicles with electronic ignition; and
- it was not clear whether this damage would be confined to the northern hemisphere or would be worldwide.

It would be of great value if your inquiry could establish:

- the likely frequency of such megaflares and their relation to the sunspot cycle.

From what I have read, megaflares are not restricted to high points in the solar cycle.

This is important because there has been much recent misunderstanding regarding the high-point of the next solar cycle. In 2006, NASA’s team was predicting a 2012 peak in a very high cycle. That prediction has had to be revised each year since as the solar cycle is behaving unpredictably. Firstly, this cycle (number 24) is obviously now much lower than the previous one. Secondly, it may peak later in 2013, or it may already be at its peak—this is not discernible from the data, and past patterns are not well known. The Carrington event was not associated with the peak nor a particular high cycle strength.

Thus—a megaflare could occur at any time. The cycle is already producing X-class flares and its behaviour is not predictable (“normal” within the instrumental record).

This makes your work of the utmost urgency.

I would like to see you focus on emergency preparations:

- the NAS report identified water and food distribution as critically impacted—this is due to the short (three day) supply food chains and centralised distribution; and with regard to water—the dependency upon the electrical grid for pumping supplies;
- cities would be without light and water and within three days supermarket shelves would be emptied; and
- there is a question whether any transport would be operating as well as a complete lack of communications via radio, TV, telephone and press.

In my view, the public need to be briefed on emergency measures:

- there need to be *regional* food and water supply centres;
- there needs to be a fleet of public service vehicles that are hardened to EMP (as are military fighting vehicles);
- each household should be advised to carry one month’s supply of non-perishable food (with guidance on what to purchase) and bottled water; and
- each household should purchase a gas-bottle emergency system for cooking.

These measures would go some way to mitigating panic and disorder following an emergency and long-term loss of power supplies.

Finally—there are lessons from Fukushima for all industrial plant where safety relies upon electrical systems. In the case of nuclear plant, failure of the electrical grid causes an immediate shut-down but the plant will then be reliant upon its diesel generators. Each nuclear plant should carry at least three month's supply of diesel. Failure to supply diesel will result in melt-down of the reactor core with extreme consequences for a crowded island such as Britain. Additionally, nuclear waste tanks at Sellafield have about 100x the potential release of a single nuclear reactor—and they also require 24/7 power supplies for cooling.

I find it quite extra-ordinary that the scientific and engineering community have constructed an infra-structure that is so vulnerable to a perfectly natural and rather regular event. As the NAS report makes clear, a Carrington event could incapacitate power supplies for several years ... something from which civilisation would not readily recover. Your work is thus of the utmost importance.

I do hope you will be able to give some thought as to what constitutes a robust power-grid, transport and communications system—whether, for example, smaller scale and decentralised supply systems would be less vulnerable.

October 2011

Written evidence from The United States Federal Energy Regulatory Commission

I. INTRODUCTION

1. The United States Federal Energy Regulatory Commission's (FERC's) Office of Electric Reliability makes this submission in response to an inquiry by the Defence Committee of the House of Commons of the United Kingdom issued on 13 September 2011. This submission responds to four of the eight issue items listed in the inquiry notice.

2. This submission provides responses based on a study sponsored and managed by FERC, the US Department of Energy (DOE), and the US Department of Homeland Security (DHS) and performed by the Oak Ridge National Laboratory that examined the effects of electromagnetic pulses (EMP) on the US power grid. For a comprehensive analysis of the effects of EMP on the US power grid, a full electronic version of the Oak Ridge study is available at http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml.

3. The responses below are limited to the US power grid and do not address effects on other infrastructure systems. While the threats posed by EMP and the vulnerabilities of electrical infrastructure to EMP are not unique to the US, differences between the US and UK power grids should be considered when reviewing the applicability of these responses to the UK. Moreover, these responses do not address UK specific assessments, such as any particular threats to the UK, the likelihood of the use of an EMP weapon against the UK, any contingencies in place in the UK, and the broader security posture of the UK infrastructure, which were identified as issue items in the inquiry notice.

II. INQUIRY RESPONSES

A. *The extent to which space weather is forecasted and the effectiveness of early warning systems that may be in place*

4. In the US, monitoring and space weather services are provided by the Space Weather Prediction Center (SWPC), which is part of the National Weather Service within the US Department of Commerce. The SWPC issues space weather alerts, watches and warnings based on real time monitoring and forecasting of solar and geophysical events that may impact satellites, power grids, communications and navigation. Solar events capable of impacting the power grid typically have a transit time of 1 to 4 days, which allows for long and short range forecasts. SWPC provides long and short range (up to one hour) alerts and warnings to power grid operators. This information has been used to alert grid operators in advance of geomagnetic storms. However, due to the indeterminate nature of geomagnetic disturbances (GMD), the magnitude and effects of any resulting geomagnetically induced currents (GICs) cannot be accurately predicted from this monitoring, and therefore it is not possible to forecast the localized effects of these disturbances on the power grid. Work continues in this area of forecasting.

5. SWPC monitors and makes available an extensive range of information associated with solar activity, which can be found at <http://www.swpc.noaa.gov/>.

B. *The potential impact of such events for both civilian and military infrastructure*

6. The EMP pulse is divided into three time specific event categories (E1, E2 and E3 waves).⁵⁰ Each category likely affects different elements of the system. With the E1 wave, the concern lies primarily with the impact on lower voltage electronic devices. The E3 wave effects, being very similar to those produced by a

⁵⁰ Oak Ridge Study, Report Meta-R-321, at page 1-1.

geomagnetic storm,⁵¹ have a greater impact on power equipment. The main concern from E3 waves is their effect on power transformers. The E2 portion of the electromagnetic pulse is similar to lightning and is therefore generally considered to be safeguarded by current surge protection devices. Accordingly, E2 waves are not normally considered to have a significant impact on systems with adequate surge protection.

7. The E1 wave is a high magnitude pulse generated in the first few microseconds after a nuclear event or is produced intentionally by intentional electromagnetic interference (IEMI) devices designed to interfere, disrupt or destroy sensitive electronic equipment. These pulses are associated with frequencies in the MHz and GHz range that are coupled directly to conductors and can penetrate unshielded locations. The concern with these devices is that a high voltage can be introduced on low voltage electronic systems causing disruptive or destructive effects. Impacts from the E1 wave are divided into five main areas of concern: substation controls and communications, power generation facilities, power control centers, distribution line insulators and distribution transformers.⁵² Except for the distribution line insulators and transformers, the major impact is expected to be on electronic power system control equipment such as relays, SCADA systems, PLCs, computer and communication equipment.

8. While E3 impacts are expected from EMP weapons, the detrimental effects experienced on the US power grid thus far have originated from naturally-occurring GICs that result from geomagnetic storms. These effects have caused damage and failure of large power transformers⁵³ and also have had disruptive secondary effects by causing transformers to absorb reactive power and produce harmonics⁵⁴ not normally encountered on the system. These factors have caused system instabilities, including system collapse and extended power outages/reductions.⁵⁵

C. Ways of mitigating electromagnetic pulse events, either targeted or naturally occurring

9. Protection methods are divided into two categories: low frequency (E3) and high frequency (E1) protection. It should be noted that a third category, intermediate frequency (E2) protection, is addressed already through normal surge protection on the U.S. power grid. However, systems that are not protected against lightning and other surge events are unprotected against the effects related to this E2 category.

10. The Oak Ridge study assessed methods for controlling the effects of E3 like events to prevent GICs from flowing on the system or otherwise ensure that the GIC flow is below the level that produces disruptive or damaging effects. The Oak Ridge study outlined infrastructure and operational hardening methods for blocking or reducing GICs. There has been no wide scale application of these methods because further work is needed. While operational methods are currently implemented in limited cases, the Oak Ridge study found that these methods alone are unlikely to resolve the GIC problem. For example, the Oak Ridge study found that in a severe GMD event mitigation methods that depend upon operational procedures alone are unlikely to provide the substantial levels of GIC reduction needed to limit the potential for permanent damage to transformers.⁵⁶ Likewise, the study also found that equipment such as neutral resistors only reduced GICs, rather than blocking it altogether.⁵⁷ This method is susceptible to events that exceed its design capability thereby rendering the mitigation less effective or even void.

11. The Oak Ridge study also addressed E1 waves, which are associated with high frequencies, and discussed mitigation methods designed to prevent the penetration of electromagnetic energy into areas that contain susceptible equipment. For example, susceptible devices can be placed in one or more conductive enclosures (eg, "Faraday cage") to increase the shielding protection.⁵⁸ Using terminal protection devices (eg, surge protectors and filters) at possible entry points; providing effective shielding of cables; using equipment more tolerant to surges; and using wiring practices that reduce energy propagation can also be effective.⁵⁹ E1 can also corrupt data and disrupt communications equipment. Error detection and correction methods may prove beneficial in compensating for these effects.⁶⁰

D. The resources available in respect of research and development in this field

12. Research covering all aspects (E1, E2 and E3) of the EMP effects on the US power grid has been conducted by the Oak Ridge National Laboratories for FERC, DOE, and DHS and is available at http://www.ornl.gov/sci/ees/etsd/pes/ferc_emp_gic.shtml. These reports also contain a comprehensive list of references. The Electric Power Research Institute has done work on the effects of GIC on power transformers and the Institute of Electrical and Electronics Engineers has published numerous papers on this subject.

⁵¹ *Id* at page 3–1.

⁵² Oak Ridge Study, Report Meta-R-320, at page 2–45.

⁵³ Oak Ridge Study, Report Meta-R-319, at pages 2–29 and 2–31.

⁵⁴ *Id* at page 1–25.

⁵⁵ *Id* at page 2–1

⁵⁶ Oak Ridge Study, Report Meta-R-322, at page ix

⁵⁷ *Id* at page 1–2

⁵⁸ Oak Ridge Study, Report Meta-R-324, at page 4–1

⁵⁹ *Id* at page 4–3.

⁶⁰ *Id* at page 4–4.

13. Monitoring and forecasting services for space weather events are available through the Space Weather Prediction Center at <http://www.swpc.noaa.gov/> and NASA (Goddard) at <http://ccmc.gsfc.nasa.gov/>. Both organizations are conducting on-going research on space weather and its effects on the earth.

November 2011

Written evidence from the Met Office

MET OFFICE AND SPACE WEATHER SCIENCE

1. Space weather is identified in the National Security Strategy and falls under Natural Hazards, which is one of the four Tier 1 risks facing the UK as identified by the National Security Council.

2. The potential impacts of space weather are growing rapidly in proportion to our dependence on technology. Of greatest concern are the impacts on satellite and radio communication, GPS signals, defence and security activities and potential damage/disruption of the power grid. The massive expansion of technologies that are vulnerable to space weather, and our increasing world-wide dependence on them, has grown during a minimum in solar activity but we are now entering a period of increased activity with the next solar maximum expected around 2012–13.

3. Working with academic partners within the UK, the Met Office engaged with the Cabinet Office's initiative to define a reasonable worst case scenario for space weather to enable impacted sectors to make impact and mitigation assessments for the National Risk Assessment (NRA) and will continue, through the Natural Hazard Partnership's (NHP)⁶¹ Scientific Review Group, to provide science advice and a review of the risks posed by space weather.

4. The Civil Contingencies Secretariat (CCS) has tasked the NHP Scientific Review Group (SRG) to provide assistance in:

- identifying any new NRA hazards⁶² and providing advice on the reasonable worst case scenario for these hazards;
- supplementing departmental advice on what the reasonable worst case scenario for existing hazards would look like and on the likelihood assessments;
- identifying those NRA hazards that are linked and could plausibly occur concurrently, and;
- developing pre-prepared science advice which could be used during emergencies.

5. In addition, and in line with CCS's recognition of the space weather risks, leading UK experts in the field, including the Met Office, formed the Space Environment Impacts Expert Group (SEIEG). This group, led by Professor Mike Hapgood, from the Science and Technology Facilities Council (STFC) will continue to provide policy support to CCS, will advise the Science Advisory Group in Emergencies (SAGE) in the event of a major event, and will identify future research needs.

THE EXTENT TO WHICH SPACE WEATHER IS FORECAST AND THE EFFECTIVENESS OF EARLY WARNING SYSTEMS

6. The National Oceanic and Atmospheric Administration (NOAA) Space Weather Prediction Center (SWPC) in the US is regarded as the world-leader in monitoring and forecasting Earth's space environment and provides accurate and reliable solar-terrestrial information on an operational 24/7 basis to the civilian sector. Similarly, the Air Force Weather Agency (AFWA) provides an operational space weather service to the US military. However, both AFWA and the SWPC have recognised they do not have the required resilience in systems and data assimilation to provide a fully resilient operational global service.

7. The Met Office has a long-standing capability in providing resilient 24/7 operational services to both civilian and defence sectors and, critically, has the visualisation and interpretation skills required to translate technical alerts into a service that is relevant and focussed to each sector. In this context, the Met Office has established a 24/7 Hazard Centre with underpinning infrastructure, systems and functionality for Met office staff and partners to better manage major natural hazard related incidents and their impacts, including those arising from space weather. Moreover, the Met Office is already undertaking preliminary research to extend its global weather forecast model into the ionosphere.

8. Against this background, a Memorandum of Agreement between the Met Office and NOAA was signed recently to bring together the existing strengths of both organisations in an equal partnership to ensure they can develop proactive risk mitigation and resilient global operational services. AFWA are also keen to develop a more collaborative relationship with the Met Office to ensure military operations are similarly supported by a resilient service and do not remain dependent on a single centre. To achieve this, the Met Office is developing a resilient space weather prediction capability over the next few years.

⁶¹ The NHP is an evolving partnership, chaired by the Met Office, of thirteen public sector organisations specialising in environmental science. Its remit is to work better together to coordinate the development and delivery of a range of hazard related services and advice to Government stakeholders and the emergency response community.

⁶² NRA hazards are defined as non-malicious events, including natural hazards, industrial accidents, human and animal health.

9. Currently, the NHP provides, through the Hazard Centre, a daily Hazard Summary to the partners and other key stakeholders (eg Olympic Committee) on the current status of natural hazard risks which includes a section on the geomagnetic risks. This specific section is provided through our close working partnership with the British Geological Survey, leading experts in this area of space weather science.

THE RESOURCE AVAILABLE IN RESPECT OF RESEARCH AND DEVELOPMENT IN THIS FIELD

10. Pure space weather prediction capability is limited. Although the SWPC is developing a predictive capability through numerical modelling, they are keen to interface with an atmospheric modelling capability that can represent the current state of the ionosphere and its internal, natural variability. The cooperative framework mentioned above between NOAA and the Met Office is expected to enable a more rapid advance of the science, accelerate the development of improved models and space weather prediction systems, and to make more effective use of space weather data.

11. Given the impacts of space weather are not constrained by geographical or political boundaries, international collaboration is a sensible, and the most cost effective and efficient, solution to providing a resilient operational global space weather prediction system. In this context, the Met Office's ongoing collaborations in space weather science with partners across the UK's research institutes remain equally as important to ensure the best transfer and sharing of the science internationally.

12. The UK's combined expertise in space weather is distributed across a number of organisations and research institutes. The NHP, the formation of SEIEG, and the planned space weather programme within NERC's Natural Hazards theme, therefore, are a significant step in ensuring the science develops collaboratively and at a rapid pace within the UK. The Met Office's inclusion in these efforts will also enable the best possible pull through of emerging science to applied services delivered through the Hazard Centre.

13. We are also investigating how we can extend this reach with respect to the International Space Innovation Centre (ISIC) at Harwell. This STFC-supported public-private partnership was formed to bring together Government, industry and the academic community with the express purpose of promoting greater and more efficient collaboration in the development of space related technologies and science. Our involvement in ISIC will provide a valuable hub in the delivery of operational services developed from these and space weather research collaborations.

14. Currently, expertise from distinct centres of science within the UK and the US is being applied operationally within the Met Office to provide the Hazard Summary and we are in the early stages of collaboration under the MOA with NOAA—the first goal being to mirror their warning capability. Clarity in the Government's requirement for a predictive capability and sustainable resource and funding levels are key to realising a resilient and fully operational service.

December 2011

Supplementary written evidence from the Ministry of Defence

HARDENING OF THE NUCLEAR FIRING CHAIN

The Committee requested reassurance that the entire Nuclear Firing Chain is sufficiently hardened to cope with the impact of E1–3 waves of a High altitude Electromagnetic Pulse (HEMP), or a Coronal Mass Ejection, including any elements that are not in direct control of the MoD or rely on the commercial and/or civil sector. I can confirm this is the case, noting that no elements of the nuclear firing chain are beyond the direct control of the MoD.

As part of the UK's strategic nuclear deterrent, the Nuclear Firing Chain is designed and maintained to assure the UK's ability for retaliatory action should we be subject to a nuclear attack, and this has been the case since the days of the Cold War.

The MoD audits the integrity of the Nuclear Firing Chain regularly and acts to ensure that it maintains the highest possible standards, but it would not be appropriate to comment on specific measures here.

CONSIDERATION OF THE THREAT FROM IRAN IN THE WIDER CONTEXT OF HEMP

The Committee also requested clarification of the oral evidence regarding Iran's capability. The department welcomes this opportunity and feels it is appropriate to also provide greater clarity on the elements which, when combined, would create a significant HEMP threat to the UK.

Elements required for a viable HEMP weapon

A number of elements are required to enable a state or non-state actor to successfully launch a nuclear EMP attack:

-
- A *delivery system* capable of adequate range and altitude, with the capacity to carry a significant payload. A ballistic missile is, therefore, the most likely delivery system and, given the weight of a HEMP device, it must be capable of carrying a payload significantly heavier than a high explosive warhead.
 - A *nuclear device* is also required to deliver a HEMP. Successful uranium enrichment and sophisticated weapons engineering are required to manufacture a viable nuclear device. To be delivered at high altitude to generate a HEMP, the nuclear device must also be ruggedised sufficiently to withstand: the harsh conditions of launch; the high velocity journey through the atmosphere and into space; and, perhaps, depending on where on the flight path the nuclear device is detonated, a period of re-entry.
 - As well as manufacturing a robust nuclear device, it must then be successfully *integrated* into the ballistic missile to create a weapon system.

The development of all these elements is technically very challenging and expensive, with progress likely to be made in small incremental steps over a period of many years, and we judge this to be within the grasp of only a limited number of state actors.

Threat to the UK and the Government's response

The National Security Strategy and National Security Risk Assessment assessed the risk from a nuclear attack and thus HEMP, as part of the risk of an attack on the UK by another state or proxy using CBRN (chemical, biological, radiological and nuclear) weapons. This risk was judged to be low likelihood but in view of the impact, to be considered in the second tier of priorities for UK National Security.

Currently no state has both the intent to threaten our vital interests and the *capability* to do so with nuclear weapons. MOD's view is that over the next decade, existing space launch vehicle technology could theoretically be adapted by states to deliver a nuclear device; however, the MoD does not currently see the UK or Western Europe as a target for such an EMP attack. MoD does not believe that any non-state actors can currently produce improvised nuclear devices and none are likely to be able to make a sufficiently robust warhead for missile delivery in the foreseeable future. It is more likely that terrorist groups would aspire to produce improvised nuclear devices as a future means of directly creating, widespread physical damage on the ground.

In view of the continued existence of large nuclear arsenals, the possibility of further proliferation of nuclear weapons in combination with the risk of increased international instability and tension, the MoD supports cross-Government efforts to meet our commitment to advancing progress towards the long-term goal of a world without nuclear weapons, to zero tolerance of proliferation, and to the integrity and strengthening of the Nuclear Non-Proliferation Treaty (NPT). The Government considers the NPT as the cornerstone of global efforts to prevent the spread of nuclear weapons, to promote the safe and secure use of civil nuclear energy and to pursue the long-term goal of a world without nuclear weapons. Our highest priorities are continuing to pursue the entry into force of the Comprehensive Test Ban Treaty and continuing to press for the immediate commencement of negotiations on a Fissile Material Cut-off Treaty in the Conference on Disarmament. We are also working to bring Israel, Pakistan, and India into the non-proliferation mainstream. Under NPT guidelines, these states could only ever accede to the NPT as non-nuclear weapons states, and we continue to call on them to do so as such and for them to agree a full scope Comprehensive Safeguards Agreements with the International Atomic Energy Agency.

As well as supporting the Government's counter-proliferation efforts, the MoD also contributes to preventing a nuclear attack by maintaining the nuclear deterrent—which both the Prime Minister and the Defence Secretary are committed to renewing. We cannot discount the risk that a nuclear threat to our vital interests will not re-emerge by 2050 and we need a credible nuclear capability to deter these threats. The Government is therefore committed to the maintenance of a credible minimum nuclear deterrent.

The nuclear deterrent will remain the ultimate guarantor of our national security for the foreseeable future, but it could, in future, be complemented by NATO's Ballistic Missile Defence capability. Ballistic Missile Defences are designed to be able to defend against limited missile attacks, so may usefully reinforce the nuclear deterrent by providing some additional protection against HEMP.

To respond to the specific point raised in the letter, the MoD does not dispute that Iran has the capability to launch a missile to several tens of kilometres, but stands by David Ferbrache's response to Question 69 that Iran does not have the capability to launch a [nuclear] device to an altitude of several tens of kilometres. The MOD would like to reinforce this by clarifying that when David Ferbrache responded to Question 67, he was doing so in the context of the preceding questions, and was referring to Iran's ability to launch a nuclear device and missile.

Supplementary written evidence from Charles Hendry MP, Minister of State, Department of Energy & Climate Change

During the evidence session on 9 November I referred several times to a letter to industry and (in Q97 in the transcript of the session) you asked for a copy of that letter. I am pleased to attach the master of that letter together with the address list to which it was sent. The same letter was sent to each addressee, each copy being signed jointly by Simon Virley, Director General, Energy Markets & Infrastructure, DECC and Nick Winsor, Executive Director UK, National Grid on 6 October 2011 and posted the same day.

I should add that a positive response to the joint letter has returned from industry and work is being progressed through the Energy Emergencies Executive Committee as intended.

In closing, I would like to assure the Committee of DECC's continuing engagement with industry, the Cabinet Office and other government departments on tackling emerging threats to the energy sector.

21 November 2011

6 October 2011

MODELLING THE IMPACT OF SEVERE SPACE WEATHER ON GB ELECTRICITY SYSTEM

DECC and National Grid have been working closely over the past year to gain a better understanding of the potential impacts of a severe space weather event on electricity assets and networks. Historical records suggest that the so-called "Carrington event" of 1859 is a reasonable worst case scenario. Evidence indicates this event was about ten times more intense than the most severe recent event which occurred in 1989 and led to a major power system disturbance in Quebec, Canada. Whilst the impact of the 1989 event on the GB electricity system was more limited, two supergrid transformers incurred damage. Accordingly, National Grid introduced revised operational procedures to cope with such a scenario. But as our understanding of the potential severity of space weather events has developed, informed by the work of space scientists and the British Geological Survey (BGS), we need to better understand the implications and potential mitigating actions that could be taken.

In July, National Grid presented to the Energy Emergencies Executive Committee (E3C) its initial impact assessment of an extreme Space Weather event on the GB network. This work adds to our shared knowledge of the potential damage that can occur to electricity network infrastructure from the effects of a severe space weather event. Whilst significant progress continues to be made, the existing work is limited in that the model used by National Grid examines transmission assets only. This is a concern because it means a complete picture of the impact of severe space weather on the GB electricity system is not yet available. Moreover, some assets, such as generator transformers, are not included in the existing modelling but may have heightened vulnerability to a geomagnetic disturbance due to their coastal location, design, and loading.

It is therefore vital we develop a more complete model. We are writing jointly to convey a sense of urgency in achieving this aim and we are requesting your support. Specifically, we see the need for a collaborative approach which will require the sharing of data especially transformer design, construction and configuration information. This will enable a better understanding of the potential impact of severe space weather covering the transmission, distribution and generation assets across the GB electricity system. We believe that this work is most appropriately taken forward by the E3C, with an early detailed information request. Realising a complete, model will be an involved and complex process hence your earliest attention will be needed. We would expect an initial report from the E3C by February 2012.

It is imperative that we move forward with this work immediately and we urge your support in this regard.

Written evidence from EMPact America

ELECTROMAGNETIC PULSE (EMP): THREATS AND PREPAREDNESS

This summarizes key findings of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack, established by the U.S. Congress 2001–08, and of other subsequent studies. The Executive Summary of the EMP Commission Report is appended.⁶³

An electromagnetic pulse is a super-energetic radio wave that can destroy electronics. An EMP can be generated by a nuclear weapon, naturally by a geomagnetic storm, and by non-nuclear radiofrequency weapons.

A nuclear weapon detonated at high altitude (HOB 40 kilometers or more) will generate an EMP that will propagate from the point of detonation to the line of sight on the horizon, covering a vast region with a potentially destructive EMP field. A single nuclear weapon detonated at an altitude of 400 kilometers above the geographic center of the U.S. would cover the entire contiguous United States with an EMP. U.S. critical infrastructures are presently unprotected from EMP. All critical infrastructures depend directly or indirectly upon electronics and electricity, especially upon the electric power grid, that is especially vulnerable to EMP.

⁶³ Not printed. See also the more in depth 2008 report by the EMP Commission, *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures* (Washington, D.C.: 2008).

Thus, a nuclear EMP attack could collapse all the critical infrastructures—electric power, communications, transportation, banking and finance, food and water—that sustain modern economies and the lives of millions.

Any nuclear weapon, even a crude first-generation nuclear weapon of low-yield, could inflict a catastrophic EMP attack, according to the EMP Commission. The EMP Commission also found that Russia and China have probably developed what the Russians term “Super-EMP” nuclear weapons—nuclear weapons designed specifically to generate extraordinarily powerful EMP fields. Credible Russian sources told the EMP Commission in 2004 that technology for Super-EMP nuclear weapons has leaked to North Korea, enabling that nation to develop such weapons “within a few years”.

Nor is it necessary to have a sophisticated long-range missile to make a nuclear EMP attack. A short-range missile, like a Scud, launched off a freighter would suffice to deliver a nuclear warhead to high-altitude for an EMP attack. Iran has conducted such a launch mode, has detonated missiles at high-altitude, and openly writes about destroying the United States and “the West” with an EMP attack.

Solar flares and coronal mass ejections from the Sun can generate geomagnetic storms on Earth with effects similar to the EMP from a nuclear weapon. In 1989, a geomagnetic storm temporarily blacked out Quebec and parts of the United States, causing costly damage to some extremely high voltage (EHV) transformers. EHV transformers require long lead times to replace and are indispensable to the operation of the electric grid. A 1921 geomagnetic storm, that occurred before most of the U.S. was electrified, if it happened today, according to a study by the National Academy of Sciences, would destroy some 350 EHV transformers and cause a protracted blackout of the United States, requiring four to 10 years for recovery.⁶⁴

The EMP Commission warned that every century or so there occurs a “great” geomagnetic storm, like the Carrington Event of 1859, that caused fires in telegraph stations, forest fires, and destroyed the newly laid transatlantic cable. The Carrington Event posed no threat to civilization because mankind was not yet dependent upon electricity for survival. But if the Carrington Event happened today, power grids and the critical infrastructures that sustain modern societies would probably collapse worldwide.

Many scientists believe that we are overdue for another great geomagnetic storm like the Carrington Event. Many are concerned that there is a heightened prospect for such a catastrophic natural EMP event during the solar maximum, when the Sun emits more solar flares and coronal mass ejections. The solar maximum recurs every 11 years, next in December 2012 through 2013.

Non-nuclear EMP weapons, like radiofrequency weapons, can damage and destroy electronics locally. Such weapons have short ranges, kilometers for some military systems to meters for devices improvised by terrorists or criminals. Industrial EMP simulators, intended to test commercial systems for hardness against interference from stray electronic and radio emissions, are on the open market and can be purchased by anyone. At least one such EMP simulator is designed to look like a suitcase, can be operated by an individual, and is powerful enough to damage or destroy the electronic controls that regulate the operation of transformers and other components of the power grid. Armed with such a device, and with some knowledge about the electric grid, a terrorist or lunatic could blackout a city.

The EMP Commission concluded that it is necessary and affordable to protect the electric grid and other critical infrastructures from nuclear, natural, and non-nuclear EMP threats. Technology and techniques for EMP protection are well understood, having been developed and employed by the U.S. Department of Defense for military forces for over 50 years. The EMP Commission made numerous cost-effective recommendations for protecting all the civilian critical infrastructures from EMP. The Commission recommendations are based on an “all hazards” strategy that would protect not only against EMP, but mitigate the full spectrum of possible threats—including cyber attack, sabotage, and natural disasters.

In September 2010, an excellent interagency study sponsored by the U.S. Federal Energy Regulatory Commission, that included participation by the Department of Defense, the Department of Homeland Security, and the White House, independently reassessed the EMP threat—and arrived at the same conclusions as the EMP Commission. The FERC estimates that protecting the national electric grid from EMP would entail raising electric rates for a period of three years, at a cost to the average rate payer of 20 cents annually.⁶⁵

Dr William R Graham and Dr Peter Vincent Pry

13 October 2011

⁶⁴ National Academy of Sciences, *Severe Space Weather Events—Understanding Societal and Economic Impacts* (Washington, D.C.: National Academies Press, 2008).

⁶⁵ Federal Electric Regulatory Commission (FERC) Interagency Report, *Electromagnetic Pulse: Effects on the U.S. Power Grid*, Executive Summary (2010); FERC Interagency Report by John Kappenman, *Geomagnetic Storms and their Impacts on the U.S. Power Grid* (Meta-R-319) Metatech Corporation (January 2010); FERC Interagency Report by Edward Savage, James Gilbert and William Radasky, *The Early-Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid* (Meta-R-321) Metatech Corporation (January 2010); FERC Interagency Report by John Kappenman, *Low-Frequency Protection Concepts for the Electric Power Grid: Geomagnetically Induced Current (GIC) and E3 HEMP* (Meta-R-321) Metatech Corporation (January 2010); FERC Interagency Report by William Radasky and Edward Savage, *High-Frequency Protection Concepts for the Electric Power Grid* (Meta-R-324) Metatech Corporation (January 2010).

**Email from the Parliamentary Clerk, Ministry of Defence,
to Clerk of the Defence Select Committee**

Dear [Clerk]

Professor Sir Mark Welland (MoD Chief Scientific Adviser) has been asked about providing evidence to the inquiry on 9 November. However, Sir Mark advises that he does not have responsibility for the particular areas the Committee is investigating. He has therefore suggested that the most appropriate CSA to attend may be...at the Department for Energy and Climate Change. Alternatively, the CSA from the Home Office...or a representative from the Cabinet Office may be able to provide evidence on the critical infrastructure vulnerabilities, but, I am advised, are unlikely to be able to provide much information at unclassified level.

From MoD's perspective, Min(AF), Nick Harvey, would give evidence with our Director of Cyber, who is David Ferbrache.

Parliamentary Clerk

6 October 2011

ISBN 978-0-215-04189-0



9 780215 041890

