The Royal Academy of Engineering

Scientific Advice and Evidence in Emergencies

A response to the House of Commons Science and Technology Committee

September 2010

Introduction

The Academy welcomes the inquiry into *Scientific advice and evidence in emergencies* and has previously responded to the Government Chief Scientific Officer's consultation on *Guidelines on scientific advice in policy making* in February 2010[1].

In the *Guidelines on scientific advice in policy making* response, the Academy made the point that while it is important that the scientific and engineering advice used by government should be independent, at the height of a crisis, the level of independence could be less of a priority as expert knowledge becomes more important. To take the example of BSE, at the inception of the crisis, it would have been unhelpful not to use the expertise of stakeholders such as farmers and vets directly involved, despite their having a direct interest in the issues.. Later, as the issues become clearer, a broader group of experts with fewer direct interests would be appropriate to advise on mitigation and recovery.

In this response, we have tackled two of the four case studies the Committee has chosen to cover: solar events and cyber security. These differ in important aspects: space weather is a natural phenomenon, whereas an attack on cyber infrastructure is likely to be a deliberate act. The emphasis in terms of space weather events is therefore resilience and recovery where as the emphasis for cyber attacks is prevention ahead of resilience and recovery.

[1] http://www.raeng.org.uk/societygov/policy/responses/pdf/Scientific_Analysis_in_Policy_Making.pdf

Solar Storms

1. **What are the potential hazards and risks and how would they be identified? How prepared is the Government for the emergency?**

Extreme solar storms can knock out space craft and affect passengers' health on transpolar air flights through the effects of high energy particles and radiation. They can also cause long lasting problems if physical damage or data corruption occurs in space to ground radio communication, radio navigation or radio surveillance systems. Furthermore, such storms can damage electrical transformers and thus cause outages on the electricity network. These extreme events, sometimes known as Carrington Events (after British astronomer Richard Carrington), probably occur once every century or two.

Many critical infrastructure systems rely on timing signals derived from the GPS system to manage date transfers over networks and synchronisation. In the event of the loss of that timing signal, for what ever reason, most systems can "free wheel" with marginally reduced efficiency for a number of hours or days on less accurate internal clocks. Alternatively, highly accurate timing signals could be derived from ground based navigation systems such as eLORAN which would be significantly more robust to space weather events than the GPS satellite constellation. In the event of the loss of external timing signals, new innovations such as chip scale atomic clocks (CSACs) will reduce this vulnerability further. It is expected that such systems would be able to "free wheel" for the duration of any space weather event, re-synchronising their clocks when timing signals from the GPS system become available again.

Very much less extreme solar storms occur much more frequently and mitigation is largely provided through good engineering practice; for example by designing well protected spacecraft and using suitably rated transformers on the electricity network. Through strong engineering in place already, the UK infrastructure is generally well protected with long lasting problems being most unusual. Somewhat more problematical is dealing with the variability of signals caused by day-to-day space weather. For such radio systems, the national need is generally focused on defence systems which require higher signal integrity rather than civilian applications.

2. **How does the Government use scientific advice and evidence to identify, prepare for and react to an emergency?**

There are three types of space weather effects that need to be considered, each with differing warning periods from observation and duration. Because of the topology of the earth's magnetic field, the effects of radiation and geomagnetic storms are felt more acutely near the poles.

- Electromagnetic radiation
    - Arrival: 8 minutes
    - Duration: 1-2 hours
    - Effects: Dayside high frequency (HF) radio blackout, radio noise bursts causing interference on some satcom, navigation and radar systems
- High-energy charged particles – direct effects
    - Arrival: 15 minutes to days
    - Duration: hours to days

    - Effects: Satellite anomalies, passenger radiation exposure, avionic glitches
- High-energy charged particles – indirect effects
    - Arrival: 1-4 days
    - Duration: hours to days
    - Effects: Severe HF radio blackout in polar regions (including polar HF communications to aircraft), suppression of HF capability at all latitudes, GPS/Galileo accuracy degradation, potential for power grid problems.

The quantification of the risk associated with major storm events is not a simple matter and can only be achieved through the combined study of both engineers and space scientists. Many studies of this type have been conducted by various agencies, but the majority fail to consider both the engineering and scientific solutions. In principle, it is best, where possible, to engineer out the risk at the design stage if this can be achieved at acceptable cost.

There have been no extreme solar storm events in the UK since the start of the space era, but lesser storms have caused problems on European Space Agency (ESA) satellites and on HF communication systems amongst others. Lesser storms have also caused minor perturbations to the electricity network in the UK.

Scientific and engineering advice on space weather effects has been used and applied by operators to safeguard the services they provide and ensure a certain level of system resilience. Space weather events are transient and most effects are transient as well. Where there are longer term effects and where risks have not been successfully engineered out of systems, the recovery and resilience of affected systems are, to a large extent, independent of the cause of the failure. Where it is applicable, Government should use scientific and engineering advice to ensure the resilience or quick recovery of critical systems in the event of a serious space weather event.

3. What are the obstacles to obtaining reliable, timely scientific advice and evidence to inform policy decisions in emergencies?

The UK has no central coordinating agency for these events. One clear candidate is the Centre for the Protection of National Infrastructure (CPNI). Another is Defence Intelligence (DI) Intelligence Collection Strategy and Plans (ICSP) in the MOD. This Department has responsibility for the Defence Meteorological Programme and the MOD embryonic Space Weather programme. Wherever in Government this capability is located, it should have the ability to deal with classified material.

4. How effective is the strategic coordination between Government departments, public bodies, sources of scientific advice and the research base in preparing for and reacting to emergencies.

There have been no major storm events since the start of the space era but in the context of lesser storm events there is little indication of any coordination across government. However, the MOD recognised some years ago that the response to impact of space weather on radio systems must be unified. Consequently, it contracted QinetiQ to develop a space-weather mitigation model with real-time

capability which can be used operationally to support radio systems, where engineering mitigation is not possible.

How important is international coordination and how could it be strengthened?

International coordination is critical. Space weather sensors and predictions are an international endeavour; moreover the impact of extreme solar storms will be global. Realistically, the US will be a focus for space weather monitoring and notification as US society and defence are highly reliant on space assets. The US electricity network is also located at a higher geomagnetic latitude than the UK system making it more susceptible to such events. The European Space Agency (ESA) has the remit to provide the civilian focus for solar storm monitoring and space weather in Europe and will develop high level links into the US programme. In the UK and in the defence domain, linkages have been developed between MOD and DoD, resulting in a series of US-UK MOU Project Arrangements in this topic area.

Cyber Attacks

1. **What are the potential hazards and risks surrounding cyber attacks and how are they identified? How prepared is the Government for an emergency in this area? What kind of systems are the most likely targets and what would the impact be?**

The risk of serious cyber attack is perhaps somewhat hyped in the media, and in reality it is small; there is no known looming threat of an 'internet 9/11'. However, the risk is not zero and is likely to be increasing. Nation states have developed and will develop a cyber warfare capability – the attacks on Estonia in 2007 are evidence of this.

There is no single scenario to prepare for – different individuals, organisations or countries will attack different targets for their particular reasons. Cyber attacks can be used by criminals to make money or gain information; be undertaken purely as an exercise in hubris or with malign intent by hackers; or by nations to cripple another's critical national infrastructure.

It will not always be clear who the attacker is and what their motives are. For example, a cyber attack apparently by a hacker working alone might, in fact, be a politically motivated attack. It is also possible to disguise which country an attack originates from, as perpetrators working in one country can bounce information they send from a server in another country. This makes it very difficult to mobilise the appropriate response swiftly. In the time it takes to ascertain whether an attack should be met with a military, diplomatic or criminal agency response, the attack could have occurred and perpetrators will have moved on.

Large-scale organised cyber crime is a significant threat, with growing markets for selling and acquiring cyber attack capabilities. There is a flourishing and fast evolving market in the trading of botnet code that can insert itself into computers that then launch denial of service attacks under central or distributed direction.

Cyber attacks can have real physical effects, especially if they are targeted at critical infrastructure. An attack aimed at the control systems in a power plant could interrupt generation and potentially damage the plant. If smart meters are introduced, cyber attacks could turn large numbers of them off remotely. However, in reality more damage is likely to be done to the electricity infrastructure through physical attacks on substations. Conversely, nation states could also attack cyber-infrastructure using other means, such as an Electromagnetic Pulse (EMP), though to effect large scale damage to the cyber-infrastructure would require a pulse of the magnitude caused by a nuclear explosion.

2. **How does the Government use scientific advice and evidence to identify, prepare for and react to a cyber attack?**

The Office of Cyber Security (OCS) and other agencies have established ad-hoc networks seeking academic and industry support, but this is still formative. The role of the OCS needs clarification, particularly in terms of its ability to coordinate existing expertise.

The network of CSAs is, as always, important in providing Government with a capability to use scientific advice and evidence, and can work with the learned societies and professional bodies to do so. The GCSA John Beddington's recent

review of cyber security, run by an ad hoc committee of experts in the area, should feed into national security strategy.

The Serious Organised Crime Agency (SOCA) appears to have had a good understanding of how the criminal world is developing cyber attack capabilities. It cooperated and coordinated with other law enforcement agencies but there is undoubtedly much more to be done here and more support will be required by any agency planned to replace SOCA. In general, there is little expertise within the public sector, and the Government relies on experts in the private sector working together on common issues.

Ensuring availability of evidence and advice is a challenge. There is science and engineering research devoted to encryption and the hardening of the software running our systems. But there is too little research on the systemic way in which the Web is changing and evolving and new applications can arise faster than our ability to appreciate their significance. The newly emerging discipline of Web Science is an attempt to anticipate how the evolving cyber capabilities present new vulnerabilities and new opportunities and it could be exploited further by Government.

3. What are the obstacles to obtaining reliable, timely scientific advice and evidence to inform policy decisions in emergencies? Has the Government sufficient powers and resources to overcome the obstacles?

There is a lack of coherent leadership within Government, with no central conduit for advice on this area. The process of obtaining advice needs to be better resourced & made coherent with alerting through CPNI and SOCA or its replacement.

Academics working in this area rarely have the level of security clearance required to engage with Government and help to plan for cyber attacks, putting potentially useful advice is out of reach. Government also needs to work with experts in the commercial sector, but some of these may work in businesses which lack the structure to engage with Government.

The fact that almost all critical infrastructure assets are in private hands is a potential obstacle, as is the fact that the UK is a small player in a globalised world.

4. How effective is the strategic coordination between Government departments, public bodies, private bodies, sources of scientific advice and the research base in preparing for and reacting to a cyber attack?

Coordination is likely to be limited because:

- some of these areas are highly sensitive and the agencies involved find it difficult to share insights
- key aspects of the cyber estate are in the control of private companies
- many of the public bodies that need to play a role lack the required competences
- research on the Web as a critical ecosystem is fragmented.

At present, there is no one place in Government where responsibility lies, and different departments ask the same of advice of the same people. The role and resourcing of OCS needs to be resolved, clarifying whether OCS is merely raising

awareness of this issue, or whether it will be setting out and enacting a cyber security strategy.

5. How important is international coordination and how could it be strengthened?

Organised cyber crime is not an issue that can be resolved at a national level and urgently needs international diplomatic effort to agree behavioural norms, including a UN cyber crime treaty. Mutual Legal Assistance Treaty processes are not fit for purpose in this domain as they take too long: attacks are over and perpetrators have moved on before any kind of agreement can be reached. There must be better international police cooperation in order to deal with the high levels of acquisitive cyber crime.

Submitted by:
Mr P Greenish CBE
Chief Executive
The Royal Academy of Engineering
3 Carlton House Terrace
London SW1Y 5DG

Prepared by:
Katherine MacGregor
Policy Advisor

14 September 2010