HOUSE OF LORDS

European Union Committee

5th Report of Session 2009–10

Protecting Europe against large-scale cyber-attacks

Report with Evidence

Ordered to be printed 9 March 2010 and published 18 March 2010

Published by the Authority of the House of Lords

London : The Stationery Office Limited
£price

HL Paper 68

The European Union Committee

The European Union Committee of the House of Lords considers EU documents and other matters relating to the EU in advance of decisions being taken on them in Brussels. It does this in order to influence the Government's position in negotiations, and to hold them to account for their actions at EU level.

The Government are required to deposit EU documents in Parliament, and to produce within two weeks an Explanatory Memorandum setting out the implications for the UK. The Committee examines these documents, and 'holds under scrutiny' any about which it has concerns, entering into correspondence with the relevant Minister until satisfied. Letters must be answered within two weeks. Under the 'scrutiny reserve resolution', the Government may not agree in the EU Council of Ministers to any proposal still held under scrutiny; reasons must be given for any breach.

The Committee also conducts inquiries and makes reports. The Government are required to respond in writing to a report's recommendations within two months of publication. If the report is for debate, then there is a debate in the House of Lords, which a Minister attends and responds to.

The Committee has seven Sub-Committees which are:
Economic and Financial Affairs and International Trade (Sub-Committee A)
Internal Market (Sub-Committee B)
Foreign Affairs, Defence and Development Policy (Sub-Committee C)
Environment and Agriculture (Sub-Committee D)
Law and Institutions (Sub-Committee E)
Home Affairs (Sub-Committee F)
Social Policy and Consumer Affairs (Sub-Committee G)

Our Membership

The Members of the European Union Committee are:

Lord Bowness
Lord Carter of Coles
Baroness Cohen of Pimlico
Lord Dear
Lord Dykes
Lord Freeman
Lord Hannay of Chiswick
Baroness Howarth of Breckland
Lord Jopling
Lord Kerr of Kinlochard
Lord Paul
Lord Plumb
Lord Powell of Bayswater
Lord Richard
Lord Roper (Chairman)
Lord Sewel
Baroness Sharp of Guildford
Lord Teverson

The Members of the Sub-Committee which conducted this inquiry are listed in Appendix 1.

Information about the Committee

The reports and evidence of the Committee are published by and available from The Stationery Office. For information freely available on the web, our homepage is
http://www.parliament.uk/hleu
There you will find many of our publications, along with press notices, details of membership and forthcoming meetings, and other information about the ongoing work of the Committee and its Sub-Committees, each of which has its own homepage.

General Information

General information about the House of Lords and its Committees, including guidance to witnesses, details of current inquiries and forthcoming meetings is on the internet at
http://www.parliament.uk/about_lords/about_lords.cfm

Contacts for the European Union Committee

Contact details for individual Sub-Committees are given on the website.
General correspondence should be addressed to the Clerk of the European Union Committee, Committee Office, House of Lords, London, SW1A 0PW
The telephone number for general enquiries is 020 7219 5791. The Committee's email address is euclords@parliament.uk

CONTENTS

Oral Evidence

Written Evidence

NOTE: References in the text of the report are as follows:
(Q) refers to a question in the oral evidence
(p) refers to a page of written evidence

SUMMARY

We all rely on the Internet, at every level: individuals, small firms, large companies, international corporations, and at national level. Yet at every level our Internet communications are vulnerable. The Internet is run by private companies, but it is an increasingly important part of the critical national infrastructure (CNI); and we have always expected States to take significant responsibility for CNI.

The issue of large-scale cyber-attacks on the Internet has moved up the international agenda in recent months. In this inquiry we have been looking at how States and their major organisations can defend themselves and their critical information infrastructures (CIIs) against such attacks, whether these attacks are criminally or politically motivated; along with the similar issues which arise when considering how to reduce the risk of disruptions to the CII caused by natural or man-made disasters.

Individual States bear primary responsibility for their CNI, but the infrastructures of the Member States of the European Union are heavily interdependent. This has led to EU legislation beginning to regulate the extent and manner of cooperation between the Member States. However, the Internet is a global network of networks where individual States and groups of States cannot be viewed in isolation, so we started by considering whether intervention at an EU level was appropriate. We concluded that it was.

There are wide differences between the Member States. Some, like Estonia, are very heavily reliant on the Internet but have—or had until very recently—defences wholly inadequate to protect their CII against even minor attacks. Some, and the United Kingdom is among them, also rely heavily on the Internet, but have sophisticated and well-developed defences to guard against attacks or disruptions. Yet other Member States rely less on the Internet, but their defences are insufficient. We concluded that all Member States have an interest in bringing the defences of the lowest up to those of the highest, and that this is a matter of legitimate concern to the EU as a whole.

In 2009 the Commission published a Communication with proposals for enhancing the preparedness, security and resilience of the Member States in protecting their CIIs from large-scale cyber-attacks and disruptions. This document is central to our inquiry. The Communication does not put forward legislation, but makes a large number of proposals for common action by the Member States. Some, like the development of national and governmental Computer Emergency Response Teams (CERTs), will be of great benefit to many less advanced Member States. In the case of other suggestions, like enhanced EU action at global level, it is hard to see exactly what is being proposed. But we believe that there is much in the Communication that should be supported.

Lastly we looked at ENISA, the European Network and Information Security Agency. This small body has been useful as a platform for the exchange of views and of best practice, but is not helped by being in Crete, on the periphery of the EU. We believe that with a widening of its mandate to include some former third pillar matters it can play a more significant part in the developments envisaged by the Communication.

Protecting Europe against large-scale cyber-attacks

CHAPTER 1: OUR INQUIRY

Introduction

1. There is now scarcely any activity of our daily lives which does not rely on the Internet.[1] Banking,[2] travel and tax, trading, saving and dating—everything is increasingly performed online and so depends on the Internet. And while any country can survive without online shopping, to be deprived for any length of time of online communication for government, energy or defence, to give only some examples, can rapidly bring a country to its knees. We explain in the following chapter how this briefly happened to Estonia.

2. Internet failures can be the result of malicious attacks or natural disasters, but all States take precautions to guard against them, both by themselves and through the private sector. The European Union takes a major interest in the organisation of such precautions in the Member States, attempting to improve them both individually and collectively. In April 2009 the Commission sent a Communication to the Council giving its views as to how the Member States might through the EU strengthen the security and resilience of their critical information infrastructures (CIIs) and develop their defences against cyber-attacks.[3]

3. In this inquiry we have looked at the part which the EU can play in helping the United Kingdom and other Member States to prevent and detect cyber-attacks, to respond to them, mitigate their effects and recover from them; and in particular at the strategy set out in the Communication, and the programme of work it envisages. But the Internet is a global network of networks, and cyber-attacks can be launched from anywhere, making use of insecure computer systems sited anywhere on the planet. The EU cannot be looked at in isolation either from the Member States individually or from the rest of the world, and we have looked at these questions in a global context.

Conduct of the inquiry

4. This inquiry has been conducted by Sub-Committee F (Home Affairs), a list of whose members is printed in Appendix 1. They issued a call for written evidence in October 2009; this is reproduced in Appendix 3. In reply they received evidence from 25 persons and bodies. Between November 2009 and January 2010 they took oral evidence from 11 witnesses, and received

---

1 By the first quarter of 2009 nearly 65% of United Kingdom households had a fixed-line broadband connection, and more than 8 million people had at some point used their mobile phone to access the Internet: Ofcom: The Communications Market Research Report, 6 August 2009

2 Over 22 million people now bank online in the United Kingdom: Payments Council, p 154.

3 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149 final, Council document 8375/09). http://register.consilium.europa.eu/pdf/en/09/st08/st08375.en09.pdf

supplementary written evidence from a number of them. A full list of the witnesses is at Appendix 2. To all of them we are most grateful.

5. We have been fortunate to have as our specialist adviser Dr Richard Clayton of the University of Cambridge Computer Laboratory. We are most grateful to him for his expertise in the subject and for his guidance throughout the inquiry.

6. **We recommend this report to the House for debate.**

CHAPTER 2: BACKGROUND TO THE INQUIRY

Cyber-attacks: some definitions

7. Attacks on and through the Internet can range from the trivial to the potentially catastrophic. The Internet is increasingly used as a medium for the commission of crime. The scale of just one type of criminality—online banking fraud—is enormous. One study estimated US losses in 2008 to have been $1.7 billion,[4] although recent research claims to have identified flaws in the methodology and suggests that the true figure is significantly lower.[5] In the United Kingdom, where the Payments Council collates accurate data from all of the banks, losses from online banking fraud reached £39 million for the first half of 2009, a rise of 55% over the first half of 2008.[6] Individual losses can be very large, but cyber-crime of this type by its nature depends on a fully functioning Internet; as Dr Steve Marsh, the Deputy Director of the Office of Cyber Security in the Cabinet Office, told us, it is not in the interest of criminals to bring down the infrastructure which is earning them money (Q 19). This is therefore not the sort of cyber-attack we are concerned with in this inquiry.[7] Nor have we considered the generally small-scale attacks launched by disaffected persons for their own gratification or for the admiration of their peers.

8. At the other end of the scale is so-called cyber-warfare. This can be thought of as the politically motivated use of the Internet deliberately to damage the organs of a State or alliance of States; but "cyber-warfare is really just one end of a wide spectrum of threats" (Marsh, Q 33). In between these extremes lie many variants, including incidents where cyber-attacks against a State originate in the private sector but coincide with the interests of a potentially hostile State—"proxy" attacks.

9. The routine weapon for many types of Internet attack is the botnet—a collection of compromised computers (bots) running malicious programs that allow them to be controlled remotely. "It is almost depressingly easy for a criminally-minded individual of even limited technical knowledge to create, maintain and exploit botnets, as many are now sold on underground markets in kit form complete with support arrangements."[8] Botnets are inexpensive and relatively easy to create and manage. In 2008 Symantec saw botnets being sold online for as little as $0.04 per member bot.[9]

10. Internet attacks are very difficult to trace, and the ultimate source of such attacks can seldom be attributed with any confidence to a particular country, let alone a particular individual. Usually the most that can be said for certain is that a large number of bots have been commanded to send the victim a

---

4 Gartner: http://www.gartner.com/it/page.jsp?id=936913

5 Cormac Herley & Dinei Florêncio: A Profitless Endeavor: Phishing as Tragedy of the Commons. New Security Paradigms Workshop, 2008: http://research.microsoft.com/en-us/um/people/cormac/papers/phishingastragedy.pdf

6 http://www.ukpayments.org.uk/media_centre/press_releases/-/page/732/

7 Cyber-crime was the subject of a report by the House of Lords Science and Technology Committee: *Personal Internet Security*, 5th Report, Session 2006–07, HL Paper 165-I (report) and 165-II (evidence), and a follow-up report: *Personal Internet Security: Follow-up*, 4th Report, Session 2007–08, HL Paper 131.

8 Payments Council, p 155.

9 Symantec, p 52.

flood of traffic designed to overwhelm their servers or consume their bandwidth. This method of attack is called a distributed denial of service (DDoS), and the aim is to make the victim's computer, or even their entire network, unusable for either internal or external users.

Estonia, April–May 2007

11. An example often given of cyber-warfare against a State, in this case a Member State, and the example used by the Commission in its Communication, is the series of coordinated DDoS attacks against Estonia in April–May 2007.

BOX 1

Attacks against Estonia, April–May 2007

Estonia has the highest broadband connectivity in Europe. In 2007, 98 percent of all bank transactions in Estonia used electronic channels and 82 percent of all Estonian tax declarations were submitted through the Internet. Nearly every school in Estonia uses an e-learning environment, and the use of ID cards and digital signatures has become routine in both public and private sector administrations in Estonia.[10]

Estonia has a significant ethnic Russian population, and the movement of a statue of a Soviet soldier commemorating the end of World War II led to civil unrest within Estonia and complaints by the Russian Government. Online DDoS attacks began to target Estonian government and private sector sites, including banking institutions and news sites. The attacks built up over the course of a few weeks and peaked at 11 pm Moscow time on Victory Day, 9 May.

The attacks hit many parts of the infrastructure, including the websites of the prime minister, parliament, most ministries, political parties, and three of the biggest news organisations. Members of the Estonian Parliament went for four days without email. Government communications networks were reduced to radio for a limited period. Financial operations were severely compromised, ATMs were crippled, and Hansabank, the largest bank, was forced to close its Internet operations. Most people found themselves effectively barred from financial transactions while the attacks were at their height. Estonia responded by closing large parts of its network to people from outside the country, and a consequence was that Estonians abroad were unable to access their bank accounts.

12. The attacks were not particularly large: Dr José Nazario of Arbor Networks told us they were "modest by global standards" (Q 153); but they were particularly effective because Estonia is one of the most wired countries in the world but lacked an IT security apparatus of similar scale. This has since improved. XS4ALL, a Dutch Internet Service Provider (ISP), believes in any case that the attacks against Estonia were "atypical for the damage they caused" (p 164).

Attribution

13. The initial reaction in Estonia was to assume that these were attacks by the Russian State, but Dr Marsh told us that it was "very hard to say whether

[10] Staff, "Cyber Security Strategy," Estonia Ministry of Defence.

these were state-sponsored or state-condoned or really people who thought that they would act patriotically for whatever cause they were supporting at the time" (Q 38). One individual, a 20-year old ethnic Russian living in Estonia, was eventually prosecuted and fined for his part in the attacks, but it is clear that he was not solely responsible for events.[11]

14. Among those who have claimed responsibility is the Russian youth group Nashi. Dr Nazario's view is that, even in the case of Georgia where the peak size of the attacks was substantially larger than the attacks on Estonia the year before, we simply do not have the evidence to attribute any of these attacks to a specific group or a Government agency. On the contrary, analysis of the data suggests non-State actors.[12]

China

15. The attacks against Georgia to which Dr Nazario refers (and indeed corresponding attacks by Georgia against the Russian Internet) were an example—perhaps the first example—of attempts to wage war using the Internet as a weapon. But Professor Ross Anderson, Professor of Security Engineering at Cambridge University, brought to our attention an attack on a different scale but in its own way just as harmful: the infiltration, also known as GhostNet, of the email system of the Office of the Dalai Lama carried out by hacker groups and civilian auxiliaries as part of China's overall strategy.[13]

BOX 2

The Dalai Lama

In the run up to the Beijing Olympics, Professor Anderson got a call for help from the Dalai Lama's private office: they believed that their machines had been compromised. He told one of his research assistants to go to Dharamsala and see whether he could help them. It turned out that some 30 of their 50 machines had been compromised. They had had a rootkit[14] installed on them and confidential information was being abstracted to China. It was clear that this was an action, in effect, of the Chinese State, because the intelligence product was used by Chinese diplomats on more than one occasion when the Dalai Lama's staff were arranging for him to meet foreign dignitaries. The dignitaries were contacted by Chinese diplomats and warned off. Had it not been for that, then perhaps there might have been some difficulty in attribution.[15]

16. The recent and on-going dispute between China and Google, which is the world's largest Internet search company, cannot be classed as a direct attack

---

11 http://news.bbc.co.uk/1/hi/technology/7208511.stm

12 Nazario, *Politically Motivated Denial of Service Attacks*, a paper presented at the Conference on Cyberwarfare organised by the Cooperative Cyber Defence Centre of Excellence in Tallinn, Estonia, in June 2009. During the Georgian attack there was a peak bandwidth utilisation of over 800 Mbps, as compared with 95 Mbps in the Estonian attack.

13 There is a discussion of China's cyber programmes in our report *Stars and Dragons: The EU and China* (7th Report, Session 2009-10, HL Paper 76, 22 March 2010).

14 A rootkit is a software system that consists of one or more programs designed to obscure the fact that the system has been compromised: see http://en.wikipedia.org/wiki/rootkit

15 Q 246. Extracted from *The snooping dragon: social-malware surveillance of the Tibetan movement,* by Shishir Nagaraja and Ross Anderson, University of Cambridge Computer Laboratory Technical Report No 746, March 2009, http://www.cl.cam.ac.uk/techreports/UCAM-CL-TR-746.pdf.

by China against Google, but rather as attempts, described by Google as "highly sophisticated", to spy upon the activities of human rights activists around the world. Discovery of a sophisticated intrusion into a corporate Google system, reminiscent in many ways of the attack on the Dalai Lama, led Google to identify about 30 other US companies that were also being spied upon, along with the compromise of dozens of individual Gmail (Google-hosted web-based email) accounts.

17. The discovery of this espionage has led Google to announce that it will refuse to continue the censorship of its Internet search engine in China. On 2 February 2010 US Director of National Intelligence, Dennis C. Blair, called the Google attacks a "wake-up call." Cyberspace cannot be protected, he said, without a "collaborative effort that incorporates both the US private sector and our international partners." The US National Security Agency (NSA) is now joining with Google to help Google defend itself better against future attacks. The alliance is being designed to allow the two organisations to share critical information without violating Google's policies or laws that protect the privacy of online communications. Achieving collaboration is not easy, because private companies do not trust the government to keep their secrets and because of concerns that collaboration can lead to continuous government monitoring of private communications.[16]

18. These examples illustrate that attacks can be of major importance without necessarily being large-scale. Estonia was both; thousands of machines were involved in the DDoS attack, and the results were dramatic, albeit only for a short time. The attack on the Dalai Lama involved only a few machines, was of importance only to those involved, and scarcely featured in the news. The dispute with Google, though of great political importance and constantly in the headlines, has directly involved only their corporate machine and a few dozen end users. This type of cyber-espionage, involving very small numbers of attacking machines and botnets, is not on the scale envisaged by the Commission, nor is it within their competence under the Treaties, for the reasons we give in paragraph 37. The Communication is concerned only with three types of attack:

- an attack that is aimed at the network itself, or at some specific piece of critical information infrastructure (such as the power grid), and which hence impacts on almost all users;
- an attack that uses large-scale resources to attack a small number of sites, e.g. DDoS attacks; or
- an attack (using any scale of resource) on a large number of sites, e.g. the indiscriminate bulk sending of emails (spamming).

Natural disasters and accidental damage

19. The Internet can also be affected by major natural disasters such as Hurricane Katrina in 2005, when President Bush admitted that the administration had lost situational awareness in New Orleans as a direct result of degraded communications infrastructure (Stevens, p 161), and by major accidental damage. The Communication refers to these collectively as "disruptions".

---

16 Washington Post, 4 February 2010.

20. The December 2005 explosion at the Buncefield oil refinery, reportedly the largest peacetime explosion ever seen in Europe, is an example of how parts of the Internet can be accidentally damaged. The offices of the IT company Northgate Information Solutions, adjacent to the refinery, were destroyed, with short-term effects including the disruption of automated admission and discharge systems for Addenbrooke's and Papworth Hospitals in Cambridge, and as far as the James Paget Hospital in Great Yarmouth. The company also runs payroll systems for the employers of one in three Britons, paying out billions of pounds each month. Significantly however, good business continuity planning at the company in this case ensured that the disruption to these services was minimised.

21. On 30 January 2008, while sheltering from savage storms in the Mediterranean, ships off the coast of Alexandria dragged their anchors and severed two inter-continental fibre-optic cables. The cable breaks resulted in the loss of 75% of Internet capacity between Europe and the Middle East, Pakistan and India. This severely disrupted connections from United Kingdom banks to call centres in Bangalore which make extensive use of Voice Over Internet Protocol (VOIP).

Resilience of the Internet

22. We asked all our witnesses for their views on whether the Internet was resilient to attack, since this is a prominent concern of the Commission Communication. They were unanimous that it was highly resilient. Mr Ilias Chantzos, the Director of Government Relations at Symantec UK Ltd, part of an American multi-national company which is one of the world leaders in information security, went so far as to say: "…the Internet is probably one of the most resilient networks that has ever been built. I would argue that the Internet has been designed to withstand a nuclear war" (Q 144).

23. Professor Jon Crowcroft, Marconi Professor of Communications Systems at Cambridge University, explained the reason for its resilience: "The Internet is a network of networks, and its management is to a very high degree decentralised. This is one of its greatest strengths in resisting attacks. It is hard to find specific weak points, and rare that any particular failure will lead to widespread problems … Terrorists and other enemy organisations are themselves organised in decentralised ways. Asymmetric warfare works for them because their targets are centralised and obvious. The net is one infrastructure which resists this, and should be understood to be more robust as a result of this" (p 124). The Government took the same view in their written evidence: "The Internet is inherently resilient due to diverse network routes, robust network designs, a variety of network providers and the use of different makes of network equipment." With regard to the position of the United Kingdom, their view was that "It is highly unlikely that the UK could be 'cut off' from the Internet by remote electronic attack or technical failure" (p 1).

24. We do not think the Government are being complacent: our witnesses generally thought the United Kingdom had sophisticated defences compared to most other States. ENISA, the European Network and Information Security Agency, commenting on mechanisms for dealing with Internet incidents, wrote that "the UK, along with a limited number of other Member States, is considered a leader in this area with developed practices that set benchmarks for others to adopt." It was for this very reason that, in their

view, the United Kingdom could only benefit from the development of greater capabilities in other Member States (p 73).

25. The 9/11 attacks on the World Trade Centre took down many network connections in New York, but did not bring the Internet down, though they slowed it. JANET, the United Kingdom academic network, told us that their main link went to one side of the World Trade Centre and the back-up link to the other side, but there was a link to New Jersey as well.[17] Chris Gibson, the Chief Finance Officer of FIRST,[18] added: "In my bank we build the network to cater for that, we will have satellite connections that are wholly separate from the ground connections until they get to the building so if someone takes a JCB and drives through it, fine, we have a satellite connection and it will work" (Q 87).

26. This is not to say that attacks cannot take down individual parts of the Internet and have a dramatic short-term effect. We have already referred to the effect of the Buncefield explosion on hospitals a long way away, but this was put right in a matter of days. The United Kingdom Information Systems Security Association (ISSA-UK) and the BCS (the Chartered Institute for IT), which submitted evidence jointly, explained that individual enterprises and critical infrastructures can be vulnerable to attack (p 143), and Mr Cormack was "confident" that a botnet could take any university off the JANET UK network (Q 87). A failure of the Thames Barrier would flood the London Docklands and have a major impact on the Internet. But the point repeatedly made to us was that the Internet itself would be able to withstand attacks robustly, and better than any traditional alternative means of communication.[19]

27. Whether enough has been done to protect the infrastructure itself is another matter. Section 2 of the Digital Economy Act 2010[20] will insert in the Communications Act 2003 a new section 134B1(h) which will require Ofcom to prepare reports on "the preparations made by providers of UK networks for responding to an emergency, including preparations for restoring normal operation of UK networks disrupted by the emergency". The impact on the Internet of a failure of the Thames Barrier is a prime example of the sort of matter Ofcom should be considering.

28. **We are conscious that cyber-attacks, or natural or man-made disasters, can cause acute disruption to the Internet in the short term. However we believe that the United Kingdom is reasonably well placed to cope with such disruptions. We note that it is thought to be a leader among Member States, with developed practices that set benchmarks for others to adopt.**

---

17 Andrew Cormack, Chief Regulatory Adviser of JANET (Joint Academic Network) (UK), Q 87.

18 Forum for Incident Response and Security Teams

19 See, in addition to the witnesses already cited, ENISA (p 70) and Tim Stevens (p 161).

20 The reference is to clause 2 of the Digital Economy Bill at the conclusion of the Report Stage in the House of Lords on 8 March 2010.

CHAPTER 3: IS THERE A ROLE FOR THE EU?

29. The protection of Europe against cyber-attacks is undoubtedly a matter to be dealt with at every level: by individual firms, by network providers, by Governments, and by global initiatives. In this chapter we consider to what extent there is a role for the EU.

A legitimate role

30. There was consensus among our witnesses that this was a legitimate area for the EU to be concerned about, and that it had some role to play, but there was no unanimity as to what that role should be, and just how extensively the EU as such should be involved. Witnesses generally agreed with the proposition that Internet security issues were either extremely local, or were global in nature. Nonetheless they saw value in regional action, provided that it was proposed within a wider framework and led on to global initiatives. However the Communication, and most of the witnesses, were vague about what form such global initiatives should take.

31. On 8 December 2008 the Council adopted a Directive on Critical Infrastructure Protection,[21] the purpose of which was to identify and designate European Critical Infrastructures (ECI) which would benefit from a common approach to the improvement of their protection. The first draft of the Directive[22] included "Information, Communication Technologies, ICT" in the long list of critical infrastructure sectors in Annex 1. This Committee had considered that draft in the course of its normal scrutiny of EU legislation and took the view, which the Government shared, that the designation of many categories of sensitive infrastructure as ECI would, because of the wide sharing of information this would entail, not so much protect the infrastructure as potentially put it at risk. During the course of negotiations the scope of the Directive was greatly reduced, and the Directive as adopted, which will in any case not come into force until 2011, includes only energy and transport as ECI sectors. However Mr Andrea Servida from the Commission Directorate General Information, Society and Media, who was one of the authors of the Communication, explained (QQ 111, 116) that the next ECI sector in line was to be the IT sector.[23]

32. Perhaps surprisingly, those of our witnesses who were most positive about the role the EU could play were two US companies. In written evidence Mr Chantzos, for Symantec, explained: "A European wide approach to critical infrastructure protection would enable the development of a common, shared level of understanding and recognition of the specific critical infrastructures within Member States that need to be protected from online attacks. Also more importantly a pan-European approach is necessary to identify the interdependencies that currently exist in the critical infrastructures shared across Member States [and] ensure risks are identified,

---

21 Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection (OJ L345, 23 December 2008, p 75).

22 Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (COM (2006) 787 final, Council Document 16933/06 of 18 December 2006), together with Commission Communication on a European Programme for Critical Infrastructure Protection (COM (2006) 786 final, Council Document 16932/06).

23 Directive, Article 3(3): "Priority shall be given to the ICT sector".

assessed and addressed in a way that protects these critical systems against possible attack" (p 54). And Dr Nazario told us: "The EU has a major role to play; it is a common economic system, with common political goals … Engaging with the US is going to be key, I think, for connectivity purposes … So being able to communicate as a single economic voice or a unified voice to software vendors around the world will have a significant impact at raising, for example, software quality standards and software features" (Q 152).

33. Professor Anderson was also very positive: "I do believe that the European Union has a significant role to play in Internet policy, broadly defined, and that it is going to have an even larger role in the future ... Of course the European Union is going to have a role to play in this. Of course it should have a centre of technical expertise" (Q 263).

Member States with less resilient systems

34. A number of witnesses saw the main role of the EU as bringing the Member States with less developed systems for handling cyber-attacks up to the level of the most advanced—among which the United Kingdom was always seen as prominent. Improvements would include the addition of redundant capacity as a back-up for existing capacity,[24] and the development of Computer Emergency Response Teams (CERTs).[25] Thus Symantec believed that effectively securing Europe's critical infrastructure network meant having in place a common European-wide approach and strategy. "This is seen as particularly important given that many Member States are at different stages of Internet development and levels of understanding regarding the interconnected nature of networks and level of risk to possible cyber-attack" (p 53).

35. The same point was made by Europol: "There is clear asymmetrical development; some MS [Member States] are forging ahead with great advances in certain areas, whilst other MS lag behind in terms of technology" (p 124). Mr Geoffrey Smith from the Department for Business, Innovation and Skills (BIS), who with Dr Steve Marsh gave evidence on behalf of the Government, felt that there was a lot the EU could do to improve national protection, in particular encouraging the Member States which were the laggards up to the speed of the front runners (Q 3).

National security

36. One recurring theme was that, whatever the role of the EU, national security was the exclusive preserve of the Member States. In the first Cyber Security Strategy of the United Kingdom,[26] issued at the same time as the 2009 update of the National Security Strategy of the United Kingdom,[27] the Government undertook to establish the Office of Cyber Security (OCS).[28] This would, among other things, "be responsible for bringing greater

---

24 See paragraphs 22 to 28 on Resilience.

25 See paragraphs 57 et seq.

26 Cm 7642, June 2009.

27 Cm 7590, June 2009.

28 The two Houses of Parliament have established a Joint Committee on the National Security Strategy (JCNSS) to keep the National Security Strategy under review. The Committee met for the first time on 9 February 2010. The Committee has yet to decide whether its work should extend to consideration of the Cyber Security Strategy.

coherence to the UK's work with overseas partners and international organisations";[29] but the Cyber Security Strategy contains not a single reference to the EU by name.

37. Mr Smith, while agreeing that it was only right that the EU should use its influence to enhance the ability of Member States to protect their critical infrastructures, added: "We have to be very clear on what the role of the European Union is, and this is an area where we get into a well trod problem area of national security and what is the responsibility of Member States versus the role of the Community" (Q 3). This was a view shared by Mr Chantzos. He emphasised that "when we are talking about information security we are talking about the issues which impinge upon national sovereignty" (QQ 149, 151).

The wider global context

38. A second theme, one stressed by the great majority of our witnesses, was that, as the Government said in their written evidence, "the Internet operates as a global phenomenon and does not recognise borders; this is something which should be reflected in any work which takes place to ensure availability of Internet services" (p 9). SOCA, the Serious Organised Crime Agency, though operationally independent of the Government, took the same line: "The imposition of boundaries within Internet Governance is a difficult if not futile issue. Certainly policy and process can be developed nationally or within a European framework but any regulatory control will be limited by the extent to which the offending infrastructure actually sits within such regulation. SOCA's projects are globally focused and engagement with the Council of Europe and the European Commission are important … The best solution is a global one …" (p 160).

39. Mr Servida, an author of the Communication, gave his reasons for believing that there was a European dimension, but continued: "The real dimension is a global dimension but we think that there is no possibility for Europe as a region to cope, to work in the globalised environment of electronic communication networks and services unless there is first a kind of unified way of approaching the problem" (Q 112).

40. At present the global initiatives that tackle security threats are mainly organised on an entirely ad hoc basis, with loose groupings of people from relevant parts of industry coming together to address particular incidents. The CERTs (and in particular CERT/CC at Carnegie Mellon University, Pennsylvania—the very first CERT to be created) often play a key role in recruiting experts to join these working groups. A recent example of this type of global initiative is the Conficker Working Group[30] who have spent the last year ensuring that the criminals who built a botnet of 7-million compromised computers (bots) have not had the chance to exploit its power. Mr Chantzos described this as "a very good example where the industry stuck together" (Q 149).

A second best?

41. There was also a third recurrent theme. A number of witnesses, while somewhat reluctantly conceding that there was a role for the EU, saw it very much as a second best. These are only some of the views expressed:

---

29 Paragraph 3.18.

30 http://www.confickerworkinggroup.org/wiki/

- "Until a worldwide strategy can be defined and agreed upon a European-centric approach should be pursued." (Phillip Ineson on behalf of Boxing Orange Ltd, p 123);
- "In the absence of a concerted and committed global response to the issue, a European-centric policy may be the simplest and most compelling option to protect European interests." (Dr Stefan Fafinski , p 136);
- "International companies and any enterprise with an international customer base will generally seek a global rather than a European solution. In the absence of an international response, however, a European response is a step in the right direction." (Joint ISSA-UK and BCS evidence, paragraph 3.3, p 145).

42. **We agree that the protection of the Member States and their critical infrastructures from large-scale cyber-attacks is a matter of legitimate concern to the EU.**

43. **We regard the primary role of the EU as being to coordinate the activities of the Member States, spread best practices, and bring the slowest Member States up to the speed of the fastest.**

44. **The national security of Member States, and the protection of critical information infrastructure as part of it, is not a matter for the EU as such.**

45. **Any assessment of the role of the EU must be made in a global context, recognising that the Internet has no borders, and that many multinational companies operate both within and outside the EU.**

46. **We believe that the Government and the EU should be giving greater attention to how cyber-security could be developed on a global basis. In particular, consideration needs to be given to the gradual development of international rules which will effectively discourage the launching of proxy attacks from within the jurisdiction of some of the main users of the Internet.**

CHAPTER 4: THE COMMISSION COMMUNICATION

47. The sub-title of the Commission Communication is "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience."[31] The Communication is set out in full in Appendix 4. It is accompanied by over four hundred pages of impact assessment which we do not print.[32]

48. The Communication "focuses on prevention, preparedness and awareness, and defines a plan of immediate actions to strengthen the security and resilience of CIIs [Critical Information Infrastructures]." Five "pillars" are proposed to tackle these challenges:

- Preparedness and prevention: to ensure preparedness at all levels;
- Detection and response: to provide adequate early warning mechanisms;
- Mitigation and recovery: to reinforce EU defence mechanisms for CII;
- International cooperation: to promote EU priorities internationally; and
- Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures (see paragraph 31).

49. The Commission does not intend, at least for the present, to propose a binding legislative framework to carry its proposals into effect. Initially the Communication and Action Plan would provide the framework for coordination and cooperation "to engage Member States, the private sector and civil society." The Commission envisages that the Communication could be endorsed by the Council, and that the European Parliament may also decide to contribute to the discussion. It is only once the consequences of this work had been assessed that the Commission might consider putting forward proposals for legislation.[33]

Reaction to the Communication

50. ENISA, which we consider in more detail in the following chapter, has an important role in the EU plans. It was perhaps predictable that they warmly welcomed the Communication as "providing the clearest framework yet for enabling Europe to act in case of major disruptions" (p 70).[34] But the Government also "very much welcomed the communication … we thought that was a positive step forward, and I think you may recall that our explanatory memorandum[35] said that we welcomed the initiative. We had

---

31 COM(2009)149 final, Council document 8375/09. http://register.consilium.europa.eu/pdf/en/09/st08/st08375.en09.pdf

32 The impact assessment is in three parts and can be found at: http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad01.en09.pdf, http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad02.en09.pdf and http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad03.en09.pdf. A summary of the impact assessment can be found at: http://register.consilium.europa.eu/pdf/en/09/st08/st08375-ad03.en09.pdf .

33 Summary of impact assessment, sections 4 and 5.

34 It is clear from the remainder of ENISA's evidence that it does not think it is for the EU as such "to act in case of major disruptions".

35 http://10.160.3.10:81/PIMS/Static%20Files/Extended%20File%20Scan%20Files/EUROPEAN_SCRUTINY/European%20Explanatory%20Memorandum/ES%2030528.pdf

some concerns around the action plan and the realistic deliverability of some components of that, but in terms of should the European Union be providing some degree of leadership in this area we have no problem with that in principle—we think it is a good thing" (Smith, Q 3).

51. A more common reaction was to say that the Communication was fine as far as it went, but that it did not go very far. This is not necessarily a criticism. As Mr Chantzos said, the Communication is a policy statement; it is not a programme itself, but a statement of intentions—what the Commission would like the EU to do in this particular area. He thought the first requirement for the Communication to have an impact was that it should actually be followed through. It was for the Commission to do the different things that it talked about: the work on early warning, on common exercises, on information exchange, and on the review of the ENISA mandate (Q 141).

52. Others too, like Mr Cormack, thought it was hard to assess the Communication without knowing what would follow from it: "If I am feeling optimistic I can read the communication as very positive in supporting and extending the existing networks. I do not think there is anything in there that automatically gives me nightmares but as with many communications from governments it can be read in many ways, so it may be trite to say the devil is in the detail" (Q 105). And Mr Smith thought that the section of the Communication dealing with what needed to be done globally to improve Internet resilience was "one of the least clear parts of the Communication … even today I am not sure that I could give you a clear account of where this work might take us" (Q 3).

53. **We agree with those of our witnesses who believe that a full assessment of the value of the Communication as a whole will only be possible when we can see how it is followed up, and whether it has in fact contributed to "protecting Europe from large-scale cyber-attacks and disruptions by enhancing preparedness, security and resilience", as its title envisages. Meanwhile we share the broadly positive view of most of our witnesses.**

54. **The Communication says little about the role of the EU in a global context. In any proposals for specific action, the Commission will need to pay particular attention to the way they will fit into a global framework. We believe that the more advanced Member States, the United Kingdom among them, have an influential role to play in broadening the dialogue with other principal international players, in particular the US, Russia and China.**

Specific actions

55. The Communication, though addressed to the Council, does not make specific proposals for the Council to adopt. However it envisages specific actions, some of which are already beginning to take place:

- Making National/Government CERTs a key component of national capabilities;
- Creating an EU-level Public/Private Partnership for resilience;
- Launching an EU-level forum for Member States to share good practice and information relating to CIIs;
- Creating an EU-level information sharing and alert system;

- Running a national contingency planning exercise in every Member State, then a pan-European exercise, and planning for a global one; and
- Working at EU and global levels on principles and guidelines for Internet resilience and stability.

56. We consider some of these actions in the remainder of this chapter.

Computer Emergency Response Teams (CERTs)

57. A Computer Emergency Response Team, or CERT, is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, to publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.[36] A closely related organisation is the "abuse team" run by most Internet Service Providers to handle reports of incidents involving their customers.

58. In the United Kingdom there are a number of CERTs; many large private sector companies have their own, and so do organisations with a common interest. An example is JANET. Their Chief Regulatory Adviser, Mr Andrew Cormack, explained that JANET is the United Kingdom's education network connecting all universities, colleges, regional schools networks and research organisations together and to the Internet. JANET is a large computer network used by up to 16 million people in the United Kingdom either as school pupils, as university students, as teachers or as researchers, "though most of them were probably unaware that we exist" (Q 49).

59. The Government explained that CERTS are a critical part of dealing with Internet incidents, as they have the relevant expertise and experience to deal rapidly with any problems. Their view was that the CERT model found in the United Kingdom had so far proved very effective. But it was important that CERTS did not work in isolation, but maintained a close working relationship with other organisations with an interest in cyber incidents, such as the private sector and law enforcement (p 8). This was a view shared by ISSA-UK and the BCS: "CERTs are a useful, effective and essential response measure but they demand high standards of skills, training and rehearsal, and they are unlikely to have sufficient capacity to deal with widespread, multiple incidents, as might be encountered in a large-scale major cyber incident" (p 145).

60. There are a number of Government CERTs set up to deal with Internet incidents. GovCertUK is the Government CERT for the public sector system, housed within GCHQ. It provides warnings, alerts and assistance in resolving serious IT incidents for the public sector. It works closely with the CPNI (Centre for the Protection of National Infrastructure, the Government authority that provides protective security advice to businesses and organisations across the national infrastructure) and with relevant law enforcement agencies, international CERT networks and, increasingly, the recently established CSOC (Cyber Security Operations Centre, the Government body responsible for defence against cyber-attacks, located in GCHQ). In addition to emergency response, GCHQ and CPNI provide warnings, alerts and assessment of information security products and services (pp 1–2).

---

[36] Definition taken from "Inventory of CERT activities in Europe", ENISA, September 2007.

61. The United Kingdom does not currently have a national CERT in addition to sector and company specific CERTs. However the Commission propose that all Member States should set up national CERTs. Section 5.1 of the Communication invites Member States to "define … a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation", and to "make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response." The target for this is "end of 2011 for establishing well functioning National/Governmental CERTs in all Member States."

62. On the face of it, this appears to be suggesting that all Member States, even those which like the United Kingdom already have a large and sophisticated CERT network, should establish a national CERT. If this is what is intended, there was a marked lack of support for the proposal from our witnesses.

63. One of those most opposed to the Commission trying to impose national CERTs on Member States was Professor Anderson: "The problem is that national CERTs only have a fraction of the necessary expertise, and if you limit effective action to government bodies then you are in effect cutting out the communication service providers, the electric power companies, and the various other private utilities which, like it or not, control most of Europe's critical national infrastructure. You are also cutting out various NGOs and academics and others who have good expertise, and are also, for example in the case of the UK, probably marginalising other government bodies that have or are building relevant expertise, such as the National Physical Laboratory" (Q 239).

64. Despite the apparently unequivocal language of the Communication, it is possible that the Commission intend this proposal to apply only to those Member States with less developed capacity to resist cyber-attacks. The Government thought it likely that the Commission were seeking to address the problem of Member States with little or no CERT capacity, and that it was unlikely that they would seek to impose a "one size fits all" model on Member States such as the United Kingdom which were "far advanced in this area" (p 9). Lord West of Spithead, the Parliamentary Under-Secretary of State at the Home Office and Minister for Security, said: "… we need to keep that under review, whether we should have a 'national' CERT or not, and it is something we are looking at. When one looks at some of the countries in the EU, they have no CERTs at all and they need to get a kick-start" (Q 288).

65. Support for this interpretation of the Commission's true intention came from Mr Servida: "How you organise it [CERTs], whether it is just a national one or, the model which is the UK, different ones, is really up to the Member States" (Q 134). As one of the authors of the Communication, Mr Servida can be assumed to know what was intended. If that is the true intention, the words "all Member States" were poorly chosen.

66. It is certainly the case that a number of Member States, mainly Eastern European, have very few CERTs. Until 2007 Estonia was a glaring example. ENISA told us that they focused their efforts on supporting the development of CERTs in Member States that were less well-developed than countries such as the United Kingdom through brokering relations between potential partners. They had worked with Hungary to provide expertise in the

establishment of a national CERT in Bulgaria (p 74). The Government thought ENISA might be able to support less established CERTs in meeting the standards of trust and competence required to join the EGC (EU Government CERTs), a forum which does not currently cover every Member State (p 10).

67. Dr Udo Hembrecht, the Executive Director of ENISA, agreed that in smaller Member States with a less mature Internet industry a national CERT initially made sense, but thought this should not preclude them from subsequently having sector-specific CERTs as they became more sophisticated. It had been shown in the past that sector-specific CERTs worked very well because they understood the business. "In the end if we have CERTs in every sector or every Member State in a trusted communication then we shall have really improved something" (QQ 206–207).

68. We believe that the Commission proposal as described in evidence to us and as defined in the preceding paragraphs could prove valuable and should be supported. Mr Cormack pointed out that still only about 25 per cent of European IP addresses had a CERT or an abuse team sitting somewhere above them. "There is therefore definitely a role for Government, European bodies, anyone, please, to try and help fill in those blanks on the map, the 75 per cent of IP addresses which, when I get an incident from them, I can do nothing about because I have no trusted contact" (Q 69).

69. **The Commission propose establishing national CERTs in all Member States. We agree that those Member States where there are too few or inadequate CERTs should be encouraged to set up national CERTs to replace or supplement them. The Government should support this proposal.**

70. **None of our witnesses have suggested that the United Kingdom's current system of sector and company specific CERTs should be replaced by a national United Kingdom CERT, and we agree with them that there would be no advantage in this. The Government should explain that any suggestion that the United Kingdom and any other countries with a sophisticated CERT network should have to establish national CERTs would make no sense and would bring no added protection.**

71. **We urge the Commission, when responding to our report, to clarify their intentions in this respect.**

Public private partnerships

72. Despite the fact that so much of the Internet infrastructure is privately owned and operated, an important lesson from the attack on Estonia was that when the extent of the problem became apparent, it was to the Government that people looked to sort the problem out. Not only do governments themselves believe that Critical National Infrastructure is a matter for them, but in times of crisis, citizens agree with that analysis. The importance of a genuine public private partnership is clear.[37]

---

[37] The expression "public private partnership" is often used to describe the forum for the Private Finance Initiative (PFI). Like the Commission and the majority of our witnesses, we use it simply to indicate a close working relationship between governments and the private sector.

73. This seems in principle to be well understood. In their written evidence the Government told us that the United Kingdom had adopted a public private partnership model, where Government maintained a close working relationship with industry on a voluntary basis to ensure communications resilience—including that of the Internet. Their view was that to date this model had proved successful in enhancing the resilience of the communications sector. This, they thought, was something which the European Commission had realised, and they saw value in the Commission exploring what might be done on a multilateral basis within the European Union and how that might link with global initiatives in this area (p 8).

74. We put to a number of witnesses the extent to which the Internet industry relies on the skills of private entrepreneurs, and asked them whether the often-repeated intention of involving them in this work was matched on the ground. For the Commission, Mr Servida went so far as to say: "The very pillar for intervention is the European public private partnership for resilience for which we have launched the idea." But when pressed to say what exactly was being done, the most he could say was: "We have started a process to engage at the European level with private sector and public bodies in Member States in order to see how to establish it. By the end of this year [2009] we will come forward with the road map and the plan is to launch it by mid 2010." He added that the Commission, while agreeing on the need to engage the private sector, saw this as a reason "why the private sector should come forward" (QQ 128, 129). We suggest that, on the contrary, this is a reason for the Commission to take the initiative, rather than wait for the private sector to do so.

75. We would be better placed to assess the extent of the problem if we had received evidence from United Kingdom ISPs, but the only ISP which replied to our call for evidence was XS4ALL, a Dutch company. With the single exception of JANET(UK), the United Kingdom's networking companies, Internet trade bodies and Internet exchange points showed a similar lack of interest.

76. **We regret that United Kingdom Internet Service Providers and the rest of the commercial United Kingdom Internet industry should not have shown more interest in submitting evidence to this inquiry. This may be a reflection of their view that the Commission Communication will have little effect on them.**

77. Mr Smith told us that the Government had recast the European Communications Resilience and Response Group (ECRRG) "to try and bring the industry more into the centre of it, rather than Government leading this process" (Q 17).[38] Lord West explained that historically the Government had been involved with the industry, and that he had spoken to various groups in the telecommunications industry; the Communications and Electronic Security Group had been closely involved with them and there were very close Government links with BT and other providers. He added: "We need to develop mechanisms where we are talking to a much broader range of the innovative entrepreneurial businesses in the UK, but it is difficult to see quite how we can do that and still maintain this trusted environment, and that is the challenge we have" (QQ 278, 280).

---

[38] The Group brings together representatives of the telecommunications industry and the relevant Government departments, Ofcom and other bodies. It is chaired by a representative of the industry.

78. We agree that there is a challenge, and it seems plain to us that it has yet to be met. We share the view of ISSA-UK and the BCS: "In the security field, public-private partnerships tend to be talking shops rather than joint ventures. They are useful for sharing best practices but by themselves are unlikely to drive through the required levels of change" (p 145). Talking to the industry, and emphasising the importance of doing so, is a far cry from fully involving experienced Internet entrepreneurs in the formulation of Government policy. We regard this as essential if the policy is to be firmly grounded in reality, for the benefit of users and of the industry.

79. **It is clear to us that, despite good intentions, the involvement of Internet entrepreneurs in the formulation of Government policy is as yet at best superficial. Both the Government and the Commission seem to think that it is for the private sector to come forward. We think that, on the contrary, it is for the public sector to take the initiative and to offer to experienced Internet entrepreneurs a real say in how public private partnerships are best developed.**

The EU and NATO

80. The EU and NATO have a considerable overlap in their respective memberships. In an earlier report dealing with civil protection we have drawn attention to inadequate cooperation and coordination between the two bodies, so that the work of each tends too often to duplicate the work of the other, rather than complementing it.[39] Where cyber-attacks are launched against NATO Member States it is perhaps natural that NATO should see itself as having a significant part to play. We asked our witnesses whether NATO should in fact have a role, and if so, what this should be.

81. Since the attacks on Estonia in 2007, NATO itself has been in no doubt that defending its Member States against cyber-attacks is one of its responsibilities. In October 2008 the Cooperative Cyber Defence Centre of Excellence, which had been set up in Tallinn in May 2008, was accredited to NATO by a decision of the North Atlantic Council. In April 2008 NATO had launched its Policy on Cyber Defence which allows for extended cyber defence if requested from NATO Member States. The new policy envisages a common coordinated approach to cyber defence and any response to cyber-attacks. It does not allow for pre-emptive operations, but reflects an understanding that militarised cyber-war is inherently escalatory. Through its Cyber Defence Management Authority (CDMA) established by the Policy, NATO has the authority to respond immediately to cyber-attacks on its Member States and to deploy support teams. It holds annual "red team" exercises aimed at engendering cooperation and awareness across the NATO community. NATO evidently hopes that its operations can provide a model of best practice that can filter down to national levels.[40]

82. Dr Marsh told us: "There is no one way to protect the Internet; many organisations have a role to play in this and clearly NATO has a role itself in protecting certain networks, the EU has a role and national bodies have a role as well" (Q 34). However, Lord West was more doubtful that NATO had any part to play. Asked whether we should be looking more to NATO to

---

39 *Civil Protection and Crisis Management in the European Union* (6th Report, Session 2008–09, HL Paper 43).

40 Written evidence of Tim Stevens, p 162. See also the report of the NATO Parliamentary Assembly "NATO and Cyber Defence", http://www.nato-pa.int/Default.asp?SHORTCUT=1782.

protect the Internet, he replied that he did not regard them as the appropriate body unless an individual member's security was threatened: "If the security of one nation was involved we could draw on some of their abilities" (Q 275).

83. Professor Anderson explained his reservations about NATO having a role. "First, on the technical side, NATO tried for many, many years and failed, for example, to get agreement between NATO Member States on technical standards for identifying friend and foe in the military ... The second reservation that I have about that is that, if you make NATO lead agency rather than the European Union or ENISA, you intrinsically make cooperation with the Russians much harder" (Q 250).

84. It is unclear what the Commission's own views are about the involvement of NATO. The Communication itself has a single reference to NATO: "This initiative takes into account NATO activities on common policy on cyber defence, i.e. the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence." Just what account is taken of these matters, and whether, and if so how, they affect the Commission's proposals, is not vouchsafed. Nor, when we put to Mr Servida the question of cooperation between the two institutions, did we get a very satisfactory answer: "The relationship of the institution with NATO is mostly with Solana, the Office of External Relations and I must say that, in preparation of the policy proposal that is on the table today, Commissioner Reding actually met the Secretary-General of NATO at that time to address a very specific aspect, that is the aspect of how to work with the private sector" (Q 117). Mr Servida then explained some of the initiatives of NATO with the private sector, but we are still in the dark as to how the EU and NATO will, in planning protection against and combating major cyber-attacks, complement each other's work rather than duplicating it.

85. **The Communication mentions NATO only once. The EU and NATO should urgently develop their thinking on working together, and the Government should encourage this to happen, to achieve cooperation rather than duplication.**

86. **Just as with other aspects of civil protection, there is considerable overlap between the roles of the EU and NATO in relation to cyber-attacks, and cooperation between them should be put on a more formal basis.**

87. **The institutional changes introduced by the Treaty of Lisbon, and in particular the merging of the external relations responsibilities of the Commission and the Council Secretariat, should enable a more coherent approach to be taken.**

Resilience exercises

88. When he gave evidence to us early in November 2009 Mr Smith explained that on 11 and 12 November the Government would be running Exercise White Noise, the first major test in the United Kingdom of a (simulated) catastrophic communications failure (Q 39). The exercise would test the Government's strategic response to a widespread failure of the United Kingdom telecommunications system, lasting for a number of days. It was part of an ongoing programme of civil contingencies exercises that rehearsed and thereby improved the efficiency of the United Kingdom response to a

range of emergency scenarios. A month after the exercise Mr Smith gave further details.

BOX 3

Exercise White Noise

The scenario focused on the consequences of a widespread failure of the United Kingdom Public Switched Telephone Network. The hypothetical failure was introduced through an unspecified technical error by a foreign operator with a connection to the United Kingdom. The effect of the failure was that all fixed line and mobile operators in the United Kingdom lost the ability to connect calls both within their own networks and between each other's systems; no voice telephony, either fixed line or mobile, was possible within the UK unless it was over either a private wire/network or Voice Over Internet Protocol (VOIP) telephony system. The simulated fault meant that the Internet and other forms of Internet Protocol communication (e.g. email and VOIP) were possible; however fax, dial-up Internet, mobile phones (including mobile data), international connections and access to the 999 service all failed under this scenario.

The focus of the exercise for Government was to mitigate the effects of the failure on citizens, while ensuring that the telecoms networks were restored to normal operation as quickly as possible. Telecoms operators needed to isolate their systems from each other in order to correct the fault and re-establish their ability to carry traffic over their networks. The United Kingdom telecoms network is in fact a complex set of interlinking networks, all owned by private companies. The interconnections and the flow of traffic between networks are determined by commercial contracts between individual telecoms companies. This makes establishing priorities for reconnection and co-ordination between the telecoms operators and Government following a major incident complex.[41]

89. Mr Smith told us that the exercise was a success, as judged by the participants (over 95% of whom stated in the post-exercise survey that they had learned from the exercise), by Exercise Control and by the Department for Business, Innovation and Skills (BIS) as lead Department. The exercise identified some key areas where the response could be improved. These were being reviewed, and action would be taken over the coming year to address the issues (p 24). On 12 February 2010 Stephen Timms MP, a Parliamentary Under-Secretary of State at BIS, wrote to say he thought the exercise was realistic in terms of the pressure such an event would place on ministers and officials. It was in particular clear that the Government needed to work with the industry "to avoid the obvious problem of not being able to manage a communications failure through lack of communications" (p 111).

90. In their Communication the Commission invite Member States "to develop national contingency plans and organise regular exercises for large-scale network security incident response and disaster recovery, as a step towards closer pan-European coordination". The target is for each Member State to run at least one national exercise by the end of 2010. This would lead to pan-European exercises on large-scale network security incidents; again, the target was to design and run the first such exercise by the end of 2010.

[41] Extracted from the supplementary evidence from the Department for Business, Innovation and Skills (BIS), pp 23–24.

Dr Udo Helmbrecht, the Executive Director of ENISA, told us that it was now part of ENISA's work programme that there should be an exercise in 2010. He added: "I know that the military community has a lot of expertise in how to do exercises, so we do not have to invent the wheel again" (Q 201).

91. With the exception of Sweden, other Member States have not yet run such exercises, so it may be that a pan-European exercise would be premature and of limited use until at least the majority of Member States with a developed cyber system have run their own national exercises. As the Government said, this is an area where preparedness needs to be built up in individual Member States before becoming effective at EU level.[42] We understand from NATO's exercise director, Major Carlos S. Torralba, that NATO has run two cyber-exercises in the last two years, and that although the United Kingdom has participated in these only as an observer, it will play a full part in the exercise planned for 2010. Further annual exercises are planned, evidence of the importance which NATO continues to attach to the need for robust defences against cyber-attacks.

92. **We hope that the United Kingdom and other Member States with a capacity for protection against cyber-attacks will shape Commission thinking as to when a pan-European exercise might be of value. An exercise involving the US might be beneficial. This points again to the need for close cooperation between the EU and NATO.**

Timescales

93. In the case of much that is proposed in the Communication, our witnesses thought the suggested timetables were unrealistic, but particularly in the case of resilience exercises. In their Explanatory Memorandum, submitted in April 2009 less than a month after the publication of the Communication, and so still 20 months from the end of 2010, the Government described the timetable for emergency response exercises as "highly aspirational".[43] Mr Smith, who on the day he gave evidence to us was just concluding the organisation of Exercise White Noise, and was therefore particularly well-placed to speak, told us frankly: "What we worry about is how realistic this would be to expect every country to do this by the end of 2010—frankly, that is not going to happen—how realistic it is to have really large-scale exercises in Europe ... Again, that would be a major challenge, to put it politely, to do that in the next 18 months" (Q 39). Lord West felt able to be more forthright: "…the thought of a pan-European exercise on the scale they are talking about [by the end of 2010] is really not a starter. If they tried to do it, and it would be then probably without proper preparation, you would not learn anything from it, it would just be a bit of a mess." He suggested that the Commission should set their sights lower and do a rather smaller-scale exercise first of all, learn the lessons from that, see what problems and issues arose, and only then move to something bigger (Q 286).

94. **We agree with the Government that the Commission's timetable for a pan-European exercise in the course of this year is unrealistic. Instead, as a first step, they should encourage the majority of Member**

---

42 Explanatory Memorandum, 28 April 2009, paragraph 14.

43 Ibid.

States to have carried out national resilience exercises by the end of the year.

95. It is not only in the case of exercises that our witnesses thought many of the Commission's target dates over-ambitious. The Government referred to the view expressed in their Explanatory Memorandum, and added: "We have now clear evidence that the Commission is seeking to make progress on all of the key activities in the timescale envisaged. We still believe that some of the ideas for what Member States should do—particularly in terms of carrying out exercises—will prove to be unrealistic" (p 11).

96. ISSA-UK and the BCS thought there were potential short-term matters, such as the establishment of a shared, global infrastructure and response capability to detect botnets, which could be achieved by the end of 2010, but added: "It is hard to imagine that any major change could be driven thorough in such a short timescale. Cyber security demands immediate attention but most change needs to evolve through distinct stages of process maturity over a number of years" (p 146). The Payments Council, the organisation responsible for developing tactical and strategic responses to threats to payment services, concluded: "This is an enduring problem that will require a well thought-through strategic response and it will therefore not be feasible to implement this by the end of 2010. Existing structures have taken many years to evolve and become effective following a process of trial and effort and numerous false starts. We recommend that the Commission takes this opportunity to adopt a more flexible approach that takes a longer term view, and that builds on existing successes rather than attempt to create too much that is new" (p 157).

97. Mr Cormack, looking at the effect the proposed timetable would have on ENISA, described it as "quite an aggressive timescale," and thought that with their current resources ENISA would struggle with it (Q 102).

98. **It is not only in the case of resilience exercises that our witnesses thought many of the Commission's target dates over-ambitious. We hope the Commission will accept that changes that are meticulously prepared will be more valuable than any designed only to meet artificial deadlines.**

CHAPTER 5: ENISA

Functions of the agency

99. ENISA, the European Network and Information Security Agency, was set up by Regulation in March 2004.[44] This was prior to the merger of the first and third pillars by the Treaty of Lisbon, and the Regulation emphasises that ENISA deals only with first pillar matters, and in any case is without prejudice to "activities concerning public security, defence, State security (including the economic well-being of the State when the issues relate to State security matters) and the activities of the State in areas of criminal law."[45] This gave ENISA a relatively limited mandate. We consider below whether, when its mandate is next renewed, it should be extended to some former third pillar matters.

100. EU agencies are often established with grandiose and high-sounding purposes. In the case of ENISA this was "for the purpose of ensuring a high and effective level of network and information security within the Community and in order to develop a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, thus contributing to the smooth functioning of the internal market."[46]

101. More realistically, Dr Udo Helmbrecht, the Executive Director, told us: "The benefits: what we try to do is to have added value for the Member States and for the Commission, so that there are two directions. One is that we provide guidance to the European Commission in the process, for example, of their legislation via European projects or research areas. On the other hand, we work together with the Member States, for example in building up CERTs and having reports which they can use in their own Member States. So I want to try to do those things on a European level with cross-border activities or cross-border needs in this area" (Q 177). Another matter the work programme concentrated on was the resilience framework within the Critical Information Infrastructure Protection (CIIP). Over the next year they would be starting a new activity on identity and trust (Q 190).

102. Dr Chantzos summarised ENISA's current mandate: "ENISA has been designed to be a centre of excellence and has been designed to be a platform for exchange of information, exchange of best practice, of brokerage, of co-operation and exchange of views. It has not been designed to be an operational agency" (Q 170).

Management and staff

103. The Executive Director of ENISA is appointed for a term of up to 5 years.[47] Dr Helmbrecht is the second Director, and took up his appointment on 16 October 2009, two months before giving evidence to us. The relationship

---

44 Regulation (EC) No 460/2004 of the European Parliament and of the Council of 10 March 2004 establishing the European Network and Information Security Agency (OJ L77, 13 March 2004, p.1).

45 Ibid, Article 1(3).

46 Ibid, Article 1(1). The reference at the end to "the smooth functioning of the internal market" is needed to give the Regulation a sound legal basis in Article 95 TEC.

47 Ibid, Article 7(3).

between the Director and the Chairman of the Management Board is important for the smooth functioning of the agency. Over the last two years we have conducted inquiries into two other EU agencies, Frontex and Europol, and in both cases have looked at the relationship between the Director and the Management Board.[48] In the case of Frontex the Chairman of the Management Board is elected for a period of two years, renewable once. The Executive Director and the Chairman therefore had an opportunity to establish a good working relationship, and had done so. By contrast, we were highly critical of the fact that the Chairman of the Management Board of Europol was the representative of the Presidency, and therefore changed every six months. Even under the Europol Decision, which came into force on 1 January 2010, the Chairman of the Management Board is to be selected "by and from within" the Member States holding the current Presidency and the two succeeding Presidencies. We are glad therefore that the Chairman of ENISA's Management Board is appointed for two and a half years renewable.[49] Dr Helmbrecht said that ENISA had been lucky in its current Chairman, Dr Reinhard Posch, who was the Austrian Chief Information Officer. It was useful that he overlapped the change of Director (Q 193).

104. ENISA currently has a staff of around 65 (Q 178). Mr Smith described ENISA as "small" (Q 3), Lord West as "very small". He added: "I am not saying that big is best because quite often big is worse, but I think that needs looking at quite closely to make sure it is able to do the things the EU wants it to do" (Q 289). Intellect, the United Kingdom trade association for the IT industry, thought that the scale of national endeavours greatly exceeded the present capacity of ENISA. "If ENISA is to have a role as a serious centre of excellence and creator of policy, then it needs to be more substantial than is currently the case" (p 138).

105. We agree that a staff of 65 is a very small number to be responsible for its current programmes; when the Commission asked for an analysis by an independent consultant, they said it was almost not worth having an agency of less than 100 people (Q 46). We believe the problems with the location of ENISA, to which we refer below, may affect recruitment. We consider below whether ENISA's mandate should be extended. **Even if there is no extension of ENISA's mandate, we believe that consideration should be given to increasing the number of staff to enable it to perform all its tasks satisfactorily.**

Assessments of ENISA's work

106. Mr Smith thought that the creation of ENISA was "not the biggest success story of all time", but that it had had some impact in drawing people together in the European Union (Q 3). Other assessments of ENISA have been rather more positive. The Payments Council were "highly supportive" of ENISA, believing that it has the potential to be a powerful force for good in promoting the development of CERTs in Europe. It could however be "awkward in its execution" (p 157). Mr Cormack was even more supportive:

---

[48] *FRONTEX: the EU external borders agency* (9th Report, Session 2007–08, HL Paper 60), paragraphs 82–91; *EUROPOL: coordinating the fight against serious and organised crime* (29th Report, Session 2007–08, HL Paper 183), Chapter 5.

[49] Regulation, Article 6(3).

"One of the things that has been seen by the community as very positive is the establishment and involvement of ENISA … there was a very strong welcome given to the members of ENISA staff who, like me, are now personal members of FIRST, so they are very much involved there" (Q 96). And Symantec told us: "Since its creation in 2004, ENISA has played a valuable role in bringing together government, industry and academia to share experience, knowledge and good practice" (p 56).

The impact of the Communication on ENISA's mandate

107. ENISA was initially established only for five years up to 13 March 2009,[50] but its mandate was subsequently extended for three further years to 13 March 2012.[51] The amending Regulation makes no changes to ENISA's constitution, functions or powers, and it is clear from the recitals that this is a temporary expedient, pending decisions on the changes needed. Mr Servida explained the view of the Commission: "In terms of effectiveness or impact of ENISA we think that there is a need to reform this body which was established under different conditions" (Q 135).

108. The Communication was published less than a month after the extension of ENISA's mandate. Section 4 on The Way Forward states: "It is necessary to strengthen the existing instruments for cooperation, including ENISA ..." This will indeed be necessary if the Communication is implemented, given that major new roles are envisaged for ENISA under the first three of the five sections of the Action Plan.[52]

109. Dr Helmbrecht saw no formal role for ENISA in formulating the agency's new mandate, which he saw as solely a political process and a political decision. He explained that the procedure for changing the mandate started with a Communication from the Commission and then co-decision between the Council and Parliament. But he agreed that there would be informal discussion before the process started officially in the first half of this year (Q 187).

110. **We hope that ENISA, though not formally involved in the EU legislative process, will through its Executive Director, its Management Board and its Permanent Stakeholders Group have an important voice in the drafting of the new mandate.**

111. The entry into force of the Treaty of Lisbon, not of course mentioned in the Communication, means that the mandate would no longer necessarily be limited to matters related to the functioning of the internal market, as currently required by having Article 95 TEC as its legal base, but could be extended to some of what previously were third pillar matters. We agree with the Payments Council (p 157) that ENISA's current place within the pillar structure appears to be hampering its scope for action. **We hope that agreement can be reached, well before the expiry of the current mandate, on extending the work of ENISA to matters such as police and judicial cooperation over criminal use of the Internet, with a commensurate increase in resources.**

---

50 Ibid, Article 27.

51 Regulation (EC) No 1007/2008 of the European Parliament and of the Council of 24 September 2008 amending Regulation (EC) No 460/2004 establishing the European Network and Information Security Agency (OJ L293, 31 October 2008, p.1).

52 See paragraph 48 above.

Location

112. Prior to the adoption of the Regulation setting up ENISA, the European Council decided at the meeting on 12–13 December 2003 to locate the Agency in Greece. Subsequently, and perhaps surprisingly, the Greek government decided to locate it, not in Athens as might have been expected, but at Heraklion in Crete. The process was described by Mr Smith: "The agency came at the end of a big log-jam of agencies that did not have homes ... ENISA came towards the back of that queue … As we approached enlargement, it suddenly became crucial that we solve this problem … It was a surprise to everyone when ENISA was given to Greece and the terms under which it was given were that Greece would decide the location of the agency. It chose to locate in Crete and that was the decision of the Greek government, and I have no reason to challenge that decision" (Q 46).

113. The Greek government believed it had sound reasons for its decision, since Heraklion is the location of the Greek Foundation of Research and Technology (FORTH). ENISA (p 74) and Dr Helmbrecht (Q 212) pointed to the advantages of being close to a university campus and a research institute working on computer science and intelligence. Nevertheless, this decision has caused many problems and been the subject of widespread adverse comment. The panel of experts appointed by the Commission to carry out the mid-term evaluation of ENISA, as required by Article 25(1) of the Regulation, examined the location and made some scathing criticisms.

BOX 4

ENISA Evaluation Report: Location

Taking Brussels as a reference point, ENISA is the most distant agency, about 2,400 km away. This is 600 km further than CEDEFOP,[53] which is based in Greece too but in Thessalonica (and has a liaison office in Brussels). ENISA is approximately 1,000 km further than OHIM[54] in Alicante or EMCDDA[55] in Lisbon.

The problem is not distance by itself, but its impact on the mission of the agency, which requires continuous interaction with the main IT and security policy research centres.

Heraklion is not a capital city and flight schedules, especially in winter, are limited, requiring a stopover in another city (usually Athens). Travel time is between 7 to 10 hours each way, which results in an average time of up to 3 days for each event or meeting attended by an agency employee, as well as for members of the Management Board and experts cooperating with ENISA such as members of the Permanent Stakeholders Group (who are not even paid for their time).

The agency is very far from the main knowledge centres of security, mainly located in northern Europe. This reduces the opportunities for spontaneous interactions, short meetings, and keeping in touch with evolving policy priorities and new ideas.[56]

53 European Centre for the Development of Vocational Training

54 Office for Harmonisation in the Internal Market (Trade Marks and Designs)

55 European Monitoring Centre for Drugs and Drug Addiction

56 Extracted from section 3.2 of Evaluation of the European Network and Information Security Agency: Final Report by the Experts Panel, IDC EMEA, 8 January 2007.

114. These criticisms were made over three years ago, but those of our witnesses who referred to the location made it clear that these difficulties persist. Mr Smith told us: "I have seen a lot of Athens Airport over the last few years" (Q 47). ENISA told us that in 2009 their staff spent 85 nights in stopovers in Athens while on mission—and this excluded meetings in Athens itself. And the Payments Council noted: "Even in the Internet world personal contacts are important, particularly in the security field. [ENISA's] location is also likely to affect its access to the resources and skills that it requires in order to be effective" (p 157).
115. The location of ENISA also gives rise to problems of recruiting and retaining staff. All staff live in Crete because that is a condition of their contract. Dr Helmbrecht told us that the agency has no difficulty recruiting staff of the right calibre, but "it is currently a difficult situation for families with children because you do not have a well-established European School in Heraklion, so if you have parents with children from the ages of, say, 12 to 18 it is nearly impossible currently" (QQ 211, 213).
116. Professor Anderson was, as we have said, in no doubt that the EU had a significant role to play in Internet policy, and that it should have an organisation like ENISA; but he was highly critical of its current location. Ideally he thought it should be in Brussels where its expertise would be available on tap, but he also mentioned Cambridge or Munich where there was a well-established existing technical culture. If policy dictated that it had to be in Greece, then it should be within a 20-minute taxi ride of Athens airport. "There is not just an issue of convenience ... there is also an issue of recruitment and retention of high grade technical staff. Good software people like to be in places where there are other good software people ... if you cannot attract and retain top class technical people, you cannot run an agency like that" (Q 263).
117. The Management Board meets twice a year. Although some meetings have been held in Crete there have been meetings in Brussels, Vienna, Madrid, Paris and London, the clearest testimony of their views on the location. But there has been one recent improvement. In autumn 2009 ENISA opened a branch office in Athens paid for by the Greek government, so that meetings can be held there. In 2010 the Management Board will be meeting there twice, and maybe also the Permanent Stakeholders Group (QQ 212, 221). If the headquarters cannot be in Athens, an office there is the next best thing. ENISA will continue to be a centre of excellence only if the best brains in the business can be attracted to meetings; whenever possible a meeting in Athens should be preferred to one held in Crete.
118. **From the evidence we have received (though not that of the Executive Director) we are convinced that the decision to site ENISA at Heraklion was not taken on the basis of a careful cost/benefit analysis, and that it has led and continues to lead to problems over the recruitment and retention of staff, and over the scheduling of meetings.**
119. **We welcome the fact that, to meet some of these problems, the government of Greece has recently made facilities available in Athens for ENISA meetings. We hope that any conference facilities which ENISA may need there will be provided so that it can function as efficiently as possible.**
120. **We urge the Government to ensure that, when the question of location of EU agencies arises in the future, the Member State in which the agency is to be located should take into account the views of other Member States on the choice of site within that country, and that all such decisions should be taken only on the basis of a rigorous cost/benefit analysis.**

CHAPTER 6: SUMMARY OF CONCLUSIONS AND RECOMMENDATIONS

Resilience of the Internet

121. We are conscious that cyber-attacks, or natural or man-made disasters, can cause acute disruption to the Internet in the short term. However we believe that the United Kingdom is reasonably well placed to cope with such disruptions. We note that it is thought to be a leader among Member States, with developed practices that set benchmarks for others to adopt. (paragraph 28)

Is there a role for the EU?

122. We agree that the protection of the Member States and their critical infrastructures from large-scale cyber-attacks is a matter of legitimate concern to the EU. (paragraph 42)

123. We regard the primary role of the EU as being to coordinate the activities of the Member States, spread best practices, and bring the slowest Member States up to the speed of the fastest. (paragraph 43)

124. The national security of Member States, and the protection of critical information infrastructure as part of it, is not a matter for the EU as such. (paragraph 44)

125. Any assessment of the role of the EU must be made in a global context, recognising that the Internet has no borders, and that many multinational companies operate both within and outside the EU. (paragraph 45)

126. We believe that the Government and the EU should be giving greater attention to how cyber-security could be developed on a global basis. In particular, consideration needs to be given to the gradual development of international rules which will effectively discourage the launching of proxy attacks from within the jurisdiction of some of the main users of the Internet. (paragraph 46)

The Commission Communication

Reaction to the Communication

127. We agree with those of our witnesses who believe that a full assessment of the value of the Communication as a whole will only be possible when we can see how it is followed up, and whether it has in fact contributed to "protecting Europe from large-scale cyber-attacks and disruptions by enhancing preparedness, security and resilience", as its title envisages. Meanwhile we share the broadly positive view of most of our witnesses. (paragraph 53)

128. The Communication says little about the role of the EU in a global context. In any proposals for specific action, the Commission will need to pay particular attention to the way they will fit into a global framework. We believe that the more advanced Member States, the United Kingdom among them, have an influential role to play in broadening the dialogue with other principal international players, in particular the US, Russia and China. (paragraph 54)

Computer Emergency Response Teams (CERTs)

129. The Commission propose establishing national CERTs in all Member States. We agree that those Member States where there are too few or inadequate CERTs should be encouraged to set up national CERTs to replace or supplement them. The Government should support this proposal. (paragraph 69)

130. None of our witnesses have suggested that the United Kingdom's current system of sector and company specific CERTs should be replaced by a national United Kingdom CERT, and we agree with them that there would be no advantage in this. The Government should explain that any suggestion that the United Kingdom and any other countries with a sophisticated CERT network should have to establish national CERTs would make no sense and would bring no added protection. (paragraph 70)

131. We urge the Commission, when responding to our report, to clarify their intentions in this respect. (paragraph 71)

Public Private Partnerships

132. We regret that United Kingdom Internet Service Providers and the rest of the commercial United Kingdom Internet industry should not have shown more interest in submitting evidence to this inquiry. This may be a reflection of their view that the Commission Communication will have little effect on them. (paragraph 76)

133. It is clear to us that, despite good intentions, the involvement of Internet entrepreneurs in the formulation of Government policy is as yet at best superficial. Both the Government and the Commission seem to think that it is for the private sector to come forward. We think that, on the contrary, it is for the public sector to take the initiative and to offer to experienced Internet entrepreneurs a real say in how public private partnerships are best developed. (paragraph 79)

The EU and NATO

134. The Communication mentions NATO only once. The EU and NATO should urgently develop their thinking on working together, and the Government should encourage this to happen, to achieve cooperation rather than duplication. (paragraph 85)

135. Just as with other aspects of civil protection, there is considerable overlap between the roles of the EU and NATO in relation to cyber-attacks, and cooperation between them should be put on a more formal basis. (paragraph 86)

136. The institutional changes introduced by the Treaty of Lisbon, and in particular the merging of the external relations responsibilities of the Commission and the Council Secretariat, should enable a more coherent approach to be taken. (paragraph 87)

Resilience exercises

137. We hope that the United Kingdom and other Member States with a capacity for protection against cyber-attacks will shape Commission thinking as to when a pan-European exercise might be of value. An exercise involving the

US might be beneficial. This points again to the need for close cooperation between the EU and NATO. (paragraph 92)

Timescales

138. We agree with the Government that the Commission's timetable for a pan-European exercise in the course of this year is unrealistic. Instead, as a first step they should encourage the majority of Member States to have carried out national resilience exercises by the end of the year. (paragraph 94)

139. It is not only in the case of resilience exercises that our witnesses thought many of the Commission's target dates over-ambitious. We hope the Commission will accept that changes that are meticulously prepared will be more valuable than any designed only to meet artificial deadlines. (paragraph 98)

ENISA (European Network and Information Security Agency)

Management and staff

140. Even if there is no extension of ENISA's mandate, we believe that consideration should be given to increasing the number of staff to enable it to perform all its tasks satisfactorily. (paragraph 105)

The impact of the Communication on ENISA's mandate

141. We hope that ENISA, though not formally involved in the EU legislative process, will through its Executive Director, its Management Board and its Permanent Stakeholders Group have an important voice in the drafting of the new mandate. (paragraph 110)

142. We hope that agreement can be reached, well before the expiry of the current mandate, on extending the work of ENISA to matters such as police and judicial cooperation over criminal use of the Internet, with a commensurate increase in resources. (paragraph 111)

Location

143. From the evidence we have received (though not that of the Executive Director) we are convinced that the decision to site ENISA at Heraklion was not taken on the basis of a careful cost/benefit analysis, and that it has led and continues to lead to problems over the recruitment and retention of staff, and over the scheduling of meetings. (paragraph 118)

144. We welcome the fact that, to meet some of these problems, the government of Greece has recently made facilities available in Athens for ENISA meetings. We hope that any conference facilities which ENISA may need there will be provided so that it can function as efficiently as possible. (paragraph 119)

145. We urge the Government to ensure that, when the question of location of EU agencies arises in the future, the Member State in which the agency is to be located should take into account the views of other Member States on the choice of site within that country, and that all such decisions should be taken only on the basis of a rigorous cost/benefit analysis. (paragraph 120)

Conclusion

146. We recommend this report to the House for debate. (paragraph 6)

APPENDIX 1: SUB-COMMITTEE F (HOME AFFAIRS)

The members of the Sub-Committee which conducted this inquiry were:

Lord Avebury
Baroness Billingham (from 24 November 2009)
Lord Dear
Baroness Garden of Frognal
Lord Hannay of Chiswick
Lord Harrison
Lord Hodgson of Astley Abbotts
Lord Jopling (Chairman)
Lord Mackenzie of Framwellgate (from 24 November 2009)
Lord Mawson
Lord Naseby (from 24 November 2009)
Lord Richard

Baroness Henig and Lord Marlesford were members of the Sub-Committee until 24 November 2009.

Dr Richard Clayton of the University of Cambridge Computer Laboratory was appointed Specialist Adviser for the inquiry.

Declarations of Interests:

A full list of Members' interests can be found in the Register of Lords Interests:

http://www.publications.parliament.uk/pa/ld/ldreg.htm

Interests declared by Members relevant to the inquiry:

Lord Dear

Chairman, Blue Star Capital plc (investment company specialising in homeland security solutions)
Chairman, OmniPerception Ltd (high tech recognition systems)

On his appointment as Specialist Adviser Dr Clayton declared that he was joint author of a report for ENISA, the European Network and Information Security Agency, on "Security Economics and the Internal Market" in 2007-08, and joint owner of a consultancy company which had been commissioned by ENISA to write a further report.

APPENDIX 2: LIST OF WITNESSES

The following witnesses gave evidence. Those marked * gave oral evidence.

* Professor Ross Anderson, Professor of Security Engineering, Cambridge University

* Arbor Networks

Association of Chief Police Officers (ACPO)

BCS, the Chartered Institute for IT (British Computer Society)

Boxing Orange

Professor Jon Crowcroft, Marconi Professor of Communications Systems, Cambridge University

* Department for Business, Innovation and Skills (BIS)

* ENISA, the European Network and Information Security Agency

* European Commission

Europol

Dr Steven Fafinski, Lecturer in Law at Brunel University and a Director of Invenio Research Limited

* Forum for Incident Response and Security Teams (FIRST)

Intellect

Information Sharing and Analysis Centre (ISACA), London Chapter

Information Systems Security Association (ISSA-UK)

* Joint Academic Network (JANET) (UK)

Professor Juliet Lodge, Jean Monnet Centre of Excellence, University of Leeds

Ofcom

* Office of Cyber Security, Cabinet Office

Payments Council

Serious Organised Crime Agency (SOCA)

Mr Tim Stevens

* Symantec (UK) Ltd.

XS4All Internet

APPENDIX 3: CALL FOR EVIDENCE

Sub-Committee F (Home Affairs) of the House of Lords Select Committee on the European Union is conducting an inquiry into **EU policy on protecting Europe from large scale cyber-attacks**.

Following on from the EU Directive 2008/114/EC "on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection", in March 2009 the EU Commission published a Communication on Critical National Infrastructure Protection entitled "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149 final, Council document 8375/09). This document was accompanied by 400+ pages of "Impact Assessment" (COM(2009)399 and 400, Council document 8375/09 ADD 1-4) setting out the background to the Commission's approach to this issue.

The Commission is concerned that an increasing number of vital services depend on digital systems, and in particular on a working Internet. Major economic or social damage could be caused if these digital systems are disrupted, either by "hacking" or "spamming" attacks, or as a result of technical failures, or as a side-effects of a natural disaster.

The Commission is especially concerned that intentional "cyber-attacks" are growing in sophistication and frequency, and that the risks that services now run are poorly understood and insufficiently analysed.

The proposal has four specific goals:

- bridge gaps in national policies for security and resilience of critical systems;
- enhance European governance of this area;
- improve Europe's incidence response capability;
- improve the resilience and stability of the Internet.

This inquiry will focus on what are the proper roles for the EU and its Member States in this important area, where many of the critical systems involved are operated by private industry and not—as was once the case for communications providers—by public bodies. The Sub-Committee welcomes evidence on all aspects of the inquiry, but in particular on the following issues:

Threat analysis

- How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?
- Are commercial companies doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable?
- The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?
- How concerned should be we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?

International responses

- The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?
- The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?
- Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?
- The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?
- Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?
- Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?
- Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

European Network and Information Security Agency (ENISA)

- The Commission see a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?
- Is ENISA being effective in its role, or does it need reform?

Timescales

- Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?

APPENDIX 4: THE COMMISSION COMMUNICATION

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection: "Protecting Europe from large-scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"

1. Introduction

Information and Communication Technologies (ICTs) are increasingly intertwined in our daily activities. Some of these ICT systems, services, networks and infrastructures (in short, ICT infrastructures) form a vital part of European economy and society, either providing essential goods and services or constituting the underpinning platform of other critical infrastructures. They are typically regarded as critical information infrastructures (CIIs) as their disruption or destruction would have a serious impact on vital societal functions. Recent examples include the large-scale cyber-attacks targeting Estonia in 2007 and the breaks of transcontinental cables in 2008.

The World Economic Forum estimated in 2008 that there is a 10 to 20% probability of a major CII breakdown in the next 10 years, with a potential global economic cost of approximately 250 billion US$.

This Communication focuses on prevention, preparedness and awareness and defines a plan of immediate actions to strengthen the security and resilience of CIIs. This focus is consistent with the debate launched at the request of the Council and the European Parliament to addresses the challenges and priorities for network and information security (NIS) policy and the most appropriate instruments needed at EU level to tackle them. The proposed actions are also complementary to those to prevent, fight and prosecute criminal and terrorist activities targeting CIIs and synergetic with current and prospective EU research efforts in the field of network and information security, as well as with international initiatives in this area.

2. The Policy Context

This Communication develops the European policy to strengthen the security of and the trust in the information society. Already in 2005, the Commission highlighted the urgent need to coordinate efforts to build trust and confidence of stakeholders in electronic communications and services. To this end a strategy for a secure information society was adopted in 2006. Its main elements, including the security and resilience of ICT infrastructures, were endorsed in Council Resolution 2007/068/01. However, ownership and implementation by stakeholders appear insufficient. This strategy also strengthens the role, on tactical and operational levels, of the European Network and Information Security Agency (ENISA), established in 2004 to contribute to the goals of ensuring a high and effective level of NIS within the Community and developing a culture of NIS for the benefit of EU citizens, consumers, enterprises and administrations.

In 2008 ENISA's mandate was extended *'à l'identique'* until March 2012. At the same time, the Council and the European Parliament called for *"further discussion on the future of ENISA and on the general direction of the European efforts towards an increased network and information security."* To support this debate, the Commission

launched last November an on-line public consultation, the analysis of which will be made available shortly.

The activities planned in this Communication are conducted under and in parallel to the European Programme for Critical Infrastructure Protection (EPCIP). A key element of EPCIP is the Directive on the identification and designation of European Critical Infrastructures, which identifies the ICT sector as a future priority sector. Another important element of EPCIP is the Critical Infrastructure Warning Information Network (CIWIN).

On the regulatory side, the Commission proposal to reform the Regulatory Framework for electronic communications networks and services contains new provisions on security and integrity, in particular to strengthen operators' obligations to ensure that appropriate measures are taken to meet identified risks, guarantee the continuity of supply of services and notify security breaches. This approach is conducive to the general objective of enhancing the security and resilience of CIIs. The European Parliament and the Council broadly support these provisions.

The actions proposed in this Communication complement existing and prospective measures in the area of police and judicial cooperation to prevent, fight and prosecute criminal and terrorist activities targeting ICT infrastructures, as envisaged inter alia by the Council Framework Decision on attacks against information systems and its planned update.

This initiative takes into account NATO activities on common policy on cyber defence, i.e. the Cyber Defence Management Authority and the Cooperative Cyber Defence Centre of Excellence.

Lastly, due account is given to international policy developments, in particular to the G8 principles on CIIP; the UN General Assembly Resolution 58/199 Creation of a global culture of cybersecurity and the protection of critical information infrastructures and the recent OECD Recommendation on the Protection of Critical Information Infrastructures.

3. What is at Stake

3.1. Critical information infrastructures are vital for the economy and societal growth of the EU

The economic and societal role of the ICT sector and ICT infrastructures is highlighted in recent reports on innovation and economic growth. This includes the Communication on i2010 mid-term review, the Aho Group report and the European Union yearly economic reports. The OECD underlines the importance of ICTs and the Internet *"to boost economic performance and social well-being, and to strengthen societies' capacity to improve the quality of life for citizens worldwide"*. It further recommends policies that strengthen confidence in the Internet infrastructure.

The ICT sector is vital for all segments of society. Businesses rely on the ICT sector both in terms of direct sales and for the efficiency of internal processes. ICTs are a critical component of innovation and are responsible for nearly 40% of productivity growth. ICTs are also pervasive for the work of governments and public administrations: the uptake of eGovernment services at all levels, as well as new applications such as innovative solutions related to health, energy and political participation, make the public sector heavily dependent on ICTs. Last, not least, citizens increasingly rely on and use ICTs in their daily activities: strengthening

CII security would increase citizens' trust in ICTs, not least thanks to a better protection of personal data and privacy.

3.2. The risks to critical information infrastructures

The risks due to man-made attacks, natural disasters or technical failures are often not fully understood and/or sufficiently analysed. Consequently, the level of awareness across stakeholders is insufficient to devise effective safeguards and countermeasures. Cyber-attacks have risen to an unprecedented level of sophistication. Simple experiments are now turning into sophisticated activities performed for profit or political reasons. The recent large scale cyber-attacks on Estonia, Lithuania and Georgia are the most widely covered examples of a general trend. The huge number of viruses, worms and other forms of malware, the expansion of botnets and the continuous rise of spam confirm the severity of the problem.

The high dependence on CIIs, their cross-border interconnectedness and interdependencies with other infrastructures, as well as the vulnerabilities and threats they face raise the need to address their security and resilience in a systemic perspective as the frontline of defence against failures and attacks.

3.3. Security and resilience of critical information infrastructures to boost confidence in the information society

In order to ensure that ICT infrastructures are used to their maximum extent, thus fully realising the economic and social opportunities of the information society, all stakeholders must have a high level of confidence and trust in them. This depends on various elements, the most important of which is ensuring their high level of security and resilience. Diversity, openness, interoperability, usability, transparency, accountability, auditability of the different components and competition are key drivers for security development and stimulate the deployment of security-enhancing products, processes and services. As the Commission already highlighted, this is a shared responsibility: no single stakeholder has the means to ensure the security and resilience of all ICT infrastructures and to carry all the related responsibilities.

Taking up such responsibilities calls for a risk management approach and culture, able to respond to known threats and anticipate unknown future ones, without over-reacting and stifling the emergence of innovative services and applications.

3.4. The challenges for Europe

In addition and complementarily to all the activities related to the implementation of the Directive on the identification and designation of the European Critical Infrastructures, in particular the identification of ICT sector-specific criteria, a number of broader challenges need to be addressed in order to strengthen the security and resilience of CIIs.

3.4.1. Uneven and uncoordinated national approaches

Although there are commonalities among the challenges and the issues faced, measures and regimes to ensure the security and resilience of CIIs, as well as the level of expertise and preparedness, differ across Member States.

A purely national approach runs the risk of producing a fragmentation and inefficiency across Europe. Differences in national approaches and the lack of

systematic cross-border cooperation substantially reduce the effectiveness of domestic countermeasures, inter alia because, due to the interconnectedness of CIIs, a low level of security and resilience of CIIs in a country has the potential to increase vulnerabilities and risks in other ones.

To overcome this situation a European effort is needed to bring added value to national policies and programmes by fostering the development of awareness and common understanding of the challenges; stimulating the adoption of shared policy objectives and priorities; reinforcing cooperation between Member States and integrating national policies in a more European and global dimension.

3.4.2. Need for a new European governance model for CIIs

Enhancing the security and the resilience of CIIs poses peculiar governance challenges. While Member States remain ultimately responsible for defining CII-related policies, their implementation depends on the involvement of the private sector, which owns or controls a large number of CIIs. On the other hand, markets do not always provide sufficient incentives for the private sector to invest in the protection of CIIs at the level that governments would normally demand.

To address this governance problem public-private partnerships (PPPs) have emerged at the national level as the reference model. However, despite the consensus that PPPs would also be desirable on a European level, European PPPs have not materialised so far. A Europe-wide multi-stakeholder governance framework, which may include an enhanced role of ENISA, could foster the involvement of the private sector in the definition of strategic public policy objectives as well as operational priorities and measures. This framework would bridge the gap between national policy-making and operational reality on the ground.

3.4.3. Limited European early warning and incident response capability

Governance mechanisms will be truly effective only if all participants have reliable information to act upon. This is particularly relevant for governments that have the ultimate responsibility to ensure the security and well-being of citizens.

However, processes and practices for monitoring and reporting network security incidents differ significantly across Member States. Some do not have a reference organisation as a monitoring point. More importantly, cooperation and information sharing between Member States of reliable and actionable data on security incidents appears underdeveloped, being either informal or limited to bilateral or limitedly multilateral exchanges. In addition, simulating incidents and running exercises to test response capabilities are strategic in enhancing the security and resilience of CIIs, in particular by focusing on flexible strategies and processes for dealing with the unpredictability of potential crises. In the EU, cybersecurity exercises are still in an embryonic state. Exercises running across national boundaries are very limited. As recent events showed, mutual aid is an essential element of a proper response to large-scale threats and attacks to CIIs.

A strong European early warning and incident response capability has to rely on well-functioning National/Governmental Computer Emergency Response Teams (CERTs), i.e. having a common baseline in terms of capabilities. These bodies need to act as national catalysers of stakeholders' interests and capacity for public policy activities (including those related to information and alert sharing systems reaching out to citizens and SMEs) and to engage in effective cross-border

cooperation and information exchange, possibly leveraging existing organisations such as the European Governmental CERTs Group (EGC).

3.4.4. International cooperation

The rise of the Internet as a key CII requires particular attention to its resilience and stability. The Internet, thanks to its distributed, redundant design has proven to be a very robust infrastructure. However, its phenomenal growth produced a rising physical and logical complexity and the emergence of new services and uses: it is fair to question the capability of the Internet to withstand the rising number of disruptions and cyber-attacks.

The divergence of views on the criticality of the elements making up the Internet partly explains the diversity of governmental positions expressed in international fora and the often contradicting perceptions of the importance of this matter. This could hinder a proper prevention of, preparedness for and ability to recover from threats affecting the Internet. For example, the consequences of the transition from IPv4 to IPv6 should also be assessed in terms of CII security.

The Internet is a global and highly distributed network of networks, with control centres not necessarily following national boundaries. This calls for a specific, targeted approach in order to ensure its resilience and stability, based on two converging measures. First, achieving a common consensus on the European priorities for the resilience and stability of the Internet, in terms of public policy and of operational deployment. Secondly, engaging the global community to develop a set of principles, reflecting European core values, for Internet resilience and stability, in the framework of our strategic dialogue and cooperation with third countries and international organisations. These activities would build upon the recognition by the World Summit on Information Society of the key importance of the stability of the Internet.

4. The Way Forward: towards more EU Coordination and Cooperation

Because of the Community and international dimension of the problem an integrated EU approach to enhance the security and resilience of CIIs would complement and add value to national programmes as well as to the existing bilateral and multilateral cooperation schemes between Member States.

Public policy discussions in the aftermath of the events in Estonia suggest that the effects of similar attacks can be limited by preventive measures and by coordinated action during the actual crisis. A more structured exchange of information and good practices across the EU could considerably facilitate fighting cross-border threats.

It is necessary to strengthen the existing instruments for cooperation, including ENISA, and, if necessary, create new tools. A multi-stakeholder, multi-level approach is essential, taking place at the European level while fully respecting and complementing national responsibilities.

A thorough understanding of the environment and constraints is necessary. For example, the distributed nature of the Internet, where edge nodes can be used as vectors of attack, e.g. botnets, is a concern. However, this distributed nature is a key component of stability and resilience and can help a faster recovery than would normally be the case with overformalised, top-down procedures. This calls for a cautious, case-by-case analysis of public policies and operational procedures to put in place.

The time horizon is also important. There is a clear need to act now and put rapidly in place the necessary elements to build a framework that will enable us to

respond to current challenges and that will feed into the future strategy for network and information security.

Five pillars are proposed to tackle these challenges:

(1) Preparedness and prevention: to ensure preparedness at all levels;

(2) Detection and response: to provide adequate early warning mechanisms;

(3) Mitigation and recovery: to reinforce EU defence mechanisms for CII;

(4) International cooperation: to promote EU priorities internationally;

(5) Criteria for the ICT sector: to support the implementation of the Directive on the Identification and Designation of European Critical Infrastructures.

5. The Action Plan

5.1. Preparedness and prevention

Baseline of capabilities and services for pan-European cooperation. The Commission invites

Member States and concerned stakeholders to

- define, with the support of ENISA, a minimum level of capabilities and services for National/Governmental CERTs and incident response operations in support to pan-European cooperation.
- make sure National/Governmental CERTs act as the key component of national capability for preparedness, information sharing, coordination and response.

Target: end of 2010 for agreeing on minimum standards; end of 2011 for establishing well functioning National/Governmental CERTs in all Member States.

European Public Private Partnership for Resilience (EP3R). The Commission will

- foster the cooperation between the public and the private sector on security and resilience objectives, baseline requirements, good policy practices and measures. The primary focus of the EP3R would be on the European dimension from strategic (e.g. good policy practices) and tactical/operational (e.g. industrial deployment) perspectives. EP3R should build upon and complement existing national initiatives and the operational activities of ENISA.

Target: end of 2009 for a roadmap and plan for EP3R; mid of 2010 for establishing EP3R; end of 2010 for EP3R to produce its first results.

European Forum for information sharing between Member States. The Commission will

- establish a European Forum for Member States to share information and good policy practices on security and resilience of CIIs. This would benefit from the results of the activities of other organisations, in particular ENISA.

Target: end of 2009 for launching the Forum; end of 2010 for delivering the first results.

5.2. Detection and response

European Information Sharing and Alert System (EISAS). The Commission supports the development and deployment of EISAS, reaching out to citizens and SMEs and being based on national and private sector information and alert sharing systems. The Commission financially supports two complementary prototyping projects. ENISA is called upon to take stock of the results of these projects and other national initiatives and produce a roadmap to further the development and deployment of EISAS.

Target: end of 2010 for completing the prototyping projects; end of 2010 for the roadmap towards a European-system.

5.3. Mitigation and recovery

National contingency planning and exercises. The Commission invites Member States to

- develop national contingency plans and organise regular exercises for large scale networks security incident response and disaster recovery, as a step towards closer pan-European coordination. National/Governmental CERTs/CSIRTs may be tasked to lead national contingency planning exercises and testing, involving private and public sector stakeholders. The involvement of ENISA is called upon to support the exchange of good practices between Member States.

Target: end of 2010 for running at least one national exercise in every Member State.

Pan-European exercises on large-scale network security incidents. The Commission will

- financially support the development of pan-European exercises on Internet security incidents, which may also constitute the operational platform for pan-European participation in international network security incidents exercises, like the US Cyber Storm.

Target: end of 2010 for the design and run of the first pan-European exercise; end of 2010 for pan-European participation in international exercises.

Reinforced cooperation between National/Governmental CERTs. The Commission invites Member States to

- strengthen the cooperation between National/Governmental CERTs, also by leveraging and expanding existing cooperation mechanisms like the EGC. The active role of ENISA is called upon to stimulate and support pan-European cooperation between National/Governmental CERTs that should lead to enhanced preparedness; reinforced European capacity to react and respond to incidents; pan-European (and/or regional) exercises.

Target: end of 2010 for doubling the number of national bodies participating in ECG; end of 2010 for ENISA to develop reference materials to support pan-European cooperation.

5.4. International cooperation

Internet resilience and stability. Three complementary activities are envisaged

- European priorities on long term Internet resilience and stability. The Commission will drive a Europe-wide debate, involving all relevant public and private stakeholders, to define EU priorities for the long term resilience and stability of the Internet.

Target: end of 2010 for EU priorities on critical Internet components and issues.

- Principles and guidelines for Internet resilience and stability (European level). The Commission will work with Member States to define guidelines for the resilience and stability of the Internet, focusing inter alia on regional remedial actions, mutual assistance agreements, coordinated recovery and continuity strategies, geographical distribution of critical Internet resources, technological safeguards in the architecture and protocols of the Internet, replication and diversity of services and data. The Commission is already funding a task force for DNS resiliency that, together with other relevant projects, will help build the consensus.

Target: end of 2009 for a European roadmap towards principles and guidelines for Internet resilience and stability; end of 2010 for agreeing on the first draft of such principles and guidelines.

- Principles and guidelines for Internet resilience and stability (global level). The Commission will work with Member States on a roadmap to promote principles and guidelines at the global level. Strategic cooperation with third countries will be developed, notably in Information Society dialogues, as a vehicle to build global consensus.

Target: beginning of 2010 for a roadmap for international cooperation on principles and guidelines for security and resilience; end of 2010 for the first draft of internationally recognised principles and guidelines to be discussed with third countries and in relevant fora, including the Internet Governance Forum.

Global exercises on recovery and mitigation of large scale Internet incidents. The Commission invites European stakeholders to

- reflect on a practical way to extend at the global level the exercises being conducted under the mitigation and recovery pillar, building upon regional contingency plans and capabilities.

Target: end of 2010 for the Commission to propose a framework and a roadmap to support the European involvement and participation in global exercises on recovery and mitigation of large-scale Internet incidents.

5.5. Criteria for European Critical Infrastructures in the ICT sector

ICT sector specific criteria. By building on the initial activity carried out in 2008, the Commission will

- continue to develop, in cooperation with Member States and all relevant stakeholders, the criteria for identifying European critical infrastructures for the ICT sector. To this end, relevant information will be drawn from a specific study being launched.

Target: first half of 2010 for the Commission to define the criteria for the European critical infrastructures for the ICT sector.

6. Conclusions

Security and resilience of CIIs are the frontline of defence against failures and attacks. Their enhancement across the EU is essential to reap the full benefits of the information society. To achieve this ambitious objective an action plan is proposed to reinforce the tactical and operational cooperation at the European level. The success of these actions depends on their effectiveness to build upon and benefit public and private sector's activities, on the commitment and full participation of Member States, European Institutions and stakeholders.

To this end, a Ministerial Conference will take place on 27–28 April 2009 to discuss the proposed initiatives with Member States and to mark their commitment to the debate on a modernised and reinforced NIS policy in Europe.

Lastly, enhancing the security and resilience of CIIs is a long term objective, whose strategy and measures need regular assessments. Therefore, since this goal is consistent with the general debate on the future of network and information security policy in the EU after 2012, the Commission will initiate a stock-taking exercise toward the end of 2010, in order to evaluate the first phase of actions and to identify and propose further measures, as appropriate.

APPENDIX 5: GLOSSARY, ACRONYMS AND ABBREVIATIONS

ACPO	Association of Chief Police Officers
AWF	(Europol) Analysis Work File
BCS	BCS, the Chartered Institute for IT (British Computer Society)
BERR	Department for Business, Enterprise and Regulatory Reform (now BIS)
BGP	Border Gateway Protocol
BIS	Department for Business, Innovation and Skills (formerly BERR)
Botnet	Collection of compromised computers, individually called bots or zombies, running malicious programs that allow them to be controlled remotely; commonly used to launch DDoS attacks.
CCDCOE	(NATO) Cooperative Cyber Defence Centre of Excellence, Tallinn
CCS	(UK) Civil Contingencies Secretariat
CDMA	(NATO) Cyber Defence Management Authority
CEDEFOP	European Centre for the Development of Vocational Training
CEENet	Central and Eastern European Networking Association
CEPOL	European Police College
CERT	Computer Emergency Response Team
CESG	Communications and Electronic Security Group
CII	Critical Information Infrastructure
CIIP	Critical Information Infrastructure Protection
CIWIN	Critical Infrastructure Warning Information Network
CNI	Critical National Infrastructure
COBRA	Cabinet Office Briefing Room A
CPNI	(UK) Centre for the Protection of National Infrastructure
CPS	Crown Prosecution Service
CSIRT	Computer Security Incident Response Team (now synonymous with CERT)
CSIRTUK	Combined Security Incident Response Team (UK)
CSOC(UK)	Cyber Security Operations Centre in GCHQ
CSS	(UK) Cyber Security Strategy
CST	Council for Science and Technology
DCLG	Department for Communities and Local Government
DDoS	Distributed denial of service. A DDoS attack is launched by means of compromised systems (typically controlled via botnets) designed to overwhelm particular servers or networks by flooding them with packets of information.
DECC	Department of Energy and Climate Change
DEFRA	Department for Environment, Food and Rural Affairs

DfT	Department for Transport
DH	Department of Health
DHS	(US) Department of Homeland Security
DNS	Domain Name System
DTIO	Directorate of Targeting and Information Operations
EC	European Community
ECCP	European CyberCrime Platform
ECI	European Critical Infrastructure
ECRRG	Electronic Communications Resilience and Response Group
EEA	European Economic Area
EGC	European Government CERT Group
EISAS	European Information Sharing and Alert System
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ENISA	European Network and Information Security Agency
EPCIC	European Programme for Critical Infrastructure Protection
EP3R	European Public Private Partnership for Resilience
EU	European Union
Europol	European Police Office
FCO	Foreign and Commonwealth Office
FEMA	(US) Federal Emergency Management Agency
FIPR	Foundation for Information Policy Research
FIRST	Forum for Incident Response and Security Teams
FORTH	Foundation of Research and Technology, Heraklion (Crete)
FSIE	Financial Services Information Exchange
FSISAC	Financial Services Information Sharing and Analysis Centre
GCHQ	Government Communications Headquarters
GovCertUK	Government CERT UK: the Government CERT for the public sector system
GSI	Government Secure Internet
HMG	Her Majesty's Government
HO	Home Office
HTCC	(Europol) High Tech Crime Centre
ICANN	Internet Corporation for Assigned Names and Numbers
I-CROS	Internet Crime Reporting Online System
I-FOREX	Internet and Forensic Expertise
ICS	Institute of Computer Science, part of FORTH
ICT	Information and Communication Technology

IGF	(UN) Internet Governance Forum
IPPR	(UK) Institute for Public Policy Research
ISSA-UK	Information Systems Security Association
ISAC	Information Sharing and Analysis Centre
ISP	Internet Service Provider
IWWN	International Watch and Warning Network
JANET	Joint Academic Network
JCNSS	Joint Committee on the National Security Strategy
Lisbon	See Treaty of Lisbon
Malware	Malicious software
MoD	Ministry of Defence
MoJ	Ministry of Justice
MS	Member State(s) (of the European Union)
NATO	North Atlantic Treaty Organisation
NCFTA	National Cyber Forensics Training Alliance
NCIRC	NATO Computer Incident Response Capability
NHCTU	National Hi-tech Crime Unit (now transferred to SOCA)
NIS	Network and Information Security
NSA	(US) National Security Agency
NSS	(UK) National Security Strategy
OCS	(UK) Office of Cyber Security
OCTA	Organised Crime Threat Assessment
OECD	Organisation for Economic Cooperation and Development
OFCOM	(UK) Office of Communications
OFT	(UK) Office of Fair Trading
OHIM	Office for Harmonisation in the Internal Market (Trade Marks and Designs)
PCCIP	(US) President's Commission on Critical Infrastructure Protection
PCI	Payment Card Industry
PPP	Public private partnership
PSTN	(UK) Public Switched Telephone Network
Rootkit	A software system that consists of one or more programs designed to obscure the fact that the system has been compromised
SCADA	Supervisory Control and Data Acquisition
SEPA	Single European Payment Area
SIRT	Security Incident Response Team
SMEs	Small and Medium Enterprises
SOCA	Serious Organised Crime Agency

SOPs	standard operating procedures
TEC	Treaty establishing the European Community
TERENA	Trans-European Research and Education Networking Association
TEU	Treaty on European Union
TFEU	Treaty on the Functioning of the European Union
TISCA	Telecommunications Industry Security Advisory Council
Treaty of Lisbon	The Treaty between the Member States, signed in Lisbon on 13 December 2007, amending the TEU, and amending the TEC and re-naming it the TFEU
UKTI	UK Trade & Investment
VOIP	Voice Over Internet Protocol
WARP	Warning, Advice and Reporting Point
Zombies	Another word for bots; see Botnet

Minutes of Evidence

TAKEN BEFORE THE SELECT COMMITTEE ON THE EUROPEAN UNION (SUB-COMMITTEE F)

WEDNESDAY 4 NOVEMBER 2009

Present:	Dear, L	Jopling, L (Chairman)
	Garden of Frognal, B	Marlesford, L
	Harrison, L	Mawson, L
	Henig, B	Richard, L
	Hodgson of Astley Abbotts, L	

Memorandum by Department of Business, Innovation and Skills, Office of Cyber Security, Cabinet Office

The Government welcomes this inquiry. Recent attacks in Estonia and elsewhere underline the importance of increasing our capacity to protect our information infrastructure. The developments outlined in Digital Britain, the revised National Security Strategy and the new Cyber Security Strategy show a co-ordinated and holistic approach to ensuring that the UK benefits from information and communication technologies and takes a leading role in their use. The Government also welcomes the initiative of the European Commission in raising the profile of the security of information infrastructures throughout the EU and for proposing some first steps to improve the performance of Member States and the ability to benefit from working together.

This evidence has been submitted by the Department of Business, Innovation and Skills and the Office of Cyber Security in the Cabinet Office. The preparation of this evidence has involved officials from the Home Office, the Ministry of Defence, the Communications and Electronic Security Group and the Centre for the Protection of National Infrastructure.

1. Threat Analysis

1a. *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disaster?*

The internet is inherently resilient due to diverse network routes, robust network designs, a variety of network providers and the use of different makes of network equipment. It is highly unlikely that the UK could be "cut off" from the internet by remote electronic attack or technical failure. Natural disasters could affect a region, but it is likely that any impacts would be localised, and that redundancy of provision would minimise the risks of regional outage.

The UK Government takes very seriously the need to protect the integrity, confidentiality and availability of UK services and data. It works hard to protect critical systems from the impacts of attacks and other incidents. It is worth noting that the work taking place to enhance the resilience of communications covers the whole of the communications sector, including infrastructure and services, mobile and fixed line, as the infrastructure is so highly interconnected. This means that measures taken to enhance the resilience of the sector apply to the internet as much as they do to other parts of the communications sector.

There are wide ranging measures in place to protect the UK telecoms infrastructure; these are coordinated right across Government, including central Government departments as well as the agencies. BIS is involved in many different aspects of increasing the resilience of the communications sector—including the internet. One critical part of this is working with industry to ensure that communications networks—specifically those designated as Critical National Infrastructure (CNI) have robust technical and procedural measures in place to resist an incident or accident and recover quickly from it.

The Centre for the Protection of National Infrastructure (CPNI) provides security advice to the businesses and organisations that comprise the UK's critical national infrastructure (including public utilities companies and banks) that aims to reduce their vulnerability to terrorism and other threats, including electronic attack (cyber-terrorism and cybercrime). The advice provided covers physical, electronic and personnel security. CPNI has had regular contact with the providers of the key elements of the internet infrastructure in the UK. The Communications and Electronic Security Group (CESG)—part of GCHQ—provides Government

Departments with similar advice and guidance on how to protect against, detect and mitigate various types of cyber attack.

CPNI also makes available advice, tools and technical information that is designed to help reduce vulnerability to threats and mitigate the impact should an attack take place; it works closely with academia and research institutions, as well as the private sector to advance research in key and specialist areas in order to help protect the Critical National Infrastructure (which is broadly defined as essential services upon which the UK relies, the loss or compromise of which would lead to severe economic or social consequences or to loss of life.

The Government has also recently produced a UK Cyber Security Strategy, appointed a Minister for Cyber Security, consolidated Departments across Whitehall and established an Office of Cyber Security to provide strategic leadership and coherence in this area. It has also created a Cyber Security Operations Centre to monitor the health of cyber space, co-ordinate incident response, enable better understanding of attacks, and better advice and information about the risks.

— The overall picture of telecoms resilience in the UK is therefore a positive one. Every day telecoms companies manage a number of "business as usual" incidents (from theft of cables through to digital issues to impacts of bad weather). These events are managed and dealt with rapidly and effectively at a company level, and due to good continuity management processes in place, these events very rarely have a significant impact on local areas. For more disruptive events, we have arrangements in place to respond. These arrangements are discussed in more detail below.

1b. *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

The UK has adopted a public-private partnership model, where Government maintains a close working relationship with industry on a voluntary basis to ensure communications resilience—including that of the internet. To date this model has proven successful in enhancing the resilience of the communications sector—something which the European Commission has realised and is also trying to develop at a European level through the European Public-Private partnership for resilience outlined in their Communication on Critical information Infrastructure Protection.

In relation to incident response and resilience the EC-RRG (electronic communications resilience and response group) is an industry group made up of the fixed line, mobile and other communications operators including infrastructure providers. The group has Government and regulator representation and it covers the entire telecoms sector, and is not limited to the internet. The group is responsible for coordinating and managing emergency responses in the telecoms sector, with the aim of restoring service as soon as possible. It also works to enhance overall resilience across the sector. This year—for example—the group has completed work on setting up a resilient communications bridge which it can use in the event of disruptions to traditional communications services. It has also focussed on sharing information and good practice on issues around denial of access to key buildings, which could have a potentially severe impact on ensuring the availability of telecoms services, including the internet.

EC-RRG also runs annual small-scale exercises to test various resilience issues. In the past these have covered issues such as power failure, fuel shortages, as well as technical failure and related issues. It also ties in closely with the work driven forward by Civil Contingencies Secretariat (CCS) on enhancing resilience. The two main parts of this are on flooding—in the wake of the Pitt review—and on enhancing the Civil Contingencies Act 2004.

The Civil Contingencies Act provides the backdrop for work on enhancing resilience. Currently certain communications providers are required to share information on resilience (as part of their role as Category 2 responders), which they do through EC-RRG—though this group actually goes wider and includes volunteers from the wider communications service provider community who are not legally required to share information. The Act is currently under review, and some issues which will be addressed are whether more communications service providers should be classified as responders, and whether the categorisations are fitting and work effectively for all sectors.

The Digital Britain White paper also addressed key issues that needed to be progressed to make the UK a world leader in the supply and use of digital networks and technologies and acknowledged importance of existing work on resilience and security. The report identified the need to ensure that communications networks have sufficient procedures in place to resist attack and recover quickly. These measures are to be taken forward in the Digital Economy Bill (due in the fifth session). The proposals that will be set out in the Bill will allow Ofcom to assess the delivery of communications services in the face of problems that are realistically likely to be faced.

The Bill intends to amend the Communications Act 2003 to make promotion of investment in communications infrastructure one of Ofcom's principal duties, alongside the promotion of competition, and where appropriate to meet its overarching duties of securing the interests of citizens and consumers in the provision of communications services. In addition, Government will ensure Ofcom has an obligation to write as necessary to alert the Government to any matters of high concern regarding developments affecting the communications infrastructure and in any event to write every two years giving a full assessment of the UK's communications infrastructure.

The telecommunications industry is also moving towards the adoption of a minimum security standard for interconnections as a voluntary code of practice supported by the Office of Communications which should support increased levels of resilience of the UK internet. Industry is also undertaking work to enhance internet resilience—including for example: London Internet Exchange which has performed a significant amount of work on the resilience of its peering environment—as there is a significant commercial incentive for private peerings between internet service providers to be resilient. Also, Nominet—as registrar of the UK domain—has comprehensive resilience in its service provision.

Given the high level of voluntary good practice, further obligations on the internet industry may be counterproductive, in cost terms at least, but regulating resilience might prove beneficial if the market does not generate a solution (eg the need to put in resilience measures to avoid single points of failure on a core network or in Internet Exchanges). Likewise, the adoption of technical interconnection standards would assist in preventing the spread of network outages from one network to another. We believe that the Digital Economy Bill will provide a platform to address these issues and requiring Ofcom to report on resilience issues around UK networks is a significant step in both exposing this aspect of communications provision to increased market forces and in identifying rapidly if further regulation may be required.

Moreover, the requirements that are on the verge of being adopted in Europe on the overarching framework for the regulation of the communications sector will introduce higher standards. The Commission will propose standards to be applied to the security of networks and there will be greater transparency around the nature of the disruptive incidents on the networks. It is, however, important to remember that industry already has an extremely strong incentive to ensure that the services it provides are not damaged or interrupted, as this could potentially impact on contracts, income and reputation.

Cost implications for further regulation are hard to judge as there are no plans to increase the requirements placed on the companies—but building in resilience will often mean replicating infrastructure and using more expensive technologies. If special security and resilience measures are adopted to monitor communications protocols there will be further significant additional costs. However, in light of the success of the existing public-private partnership model, the costs of mandating resilience may outweigh the benefits.

1c. *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

The UK assesses the entire spectrum of risks and threats to the continuity of internet service. We share the Commission's concern but believe that Cyber-attacks are just one part of this extremely wide spectrum—as are issues such as fire, flooding, company failure, straightforward accidents or human error, conventional terrorist attacks on physical infrastructure, or even the impact of pandemic flu. It is important to have a balanced approach to the risks and threats and this is show in Figure 1. The National Risk Register—developed by Civil Contingencies Secretariat (in Cabinet Office)—may be specific to the UK, but it does highlight the wider number of issues which could potentially cause disruption, and could also impact upon internet services, either directly or indirectly. Neglecting other threats or risks in order to look only at cyber-attacks could well be counter-productive, as other threats to the communications network may be equally as damaging.

Figure 1

AN ILLUSTRATION OF THE HIGH CONSEQUENCE RISKS FACING THE UNITED KINGDOM

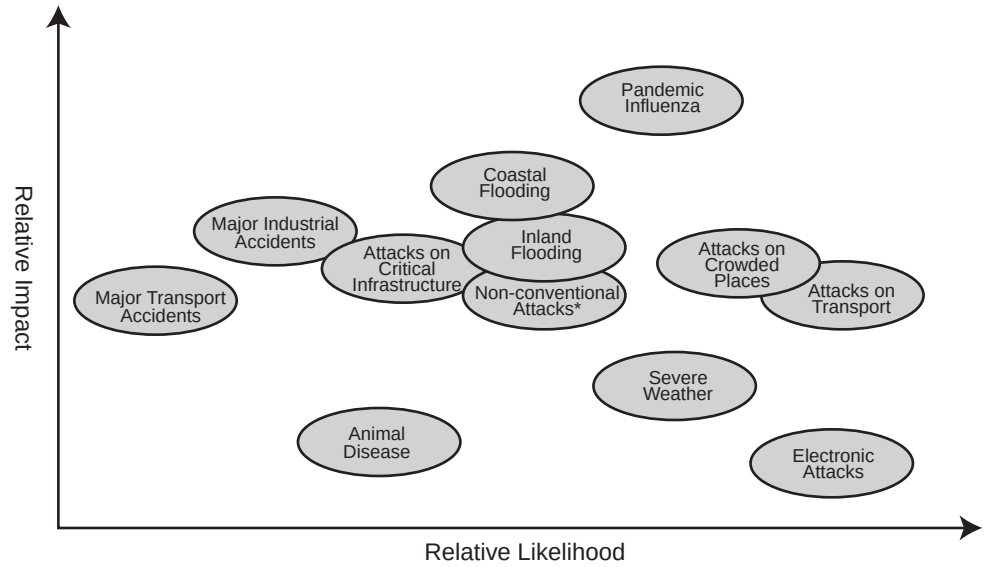


Figure 1—from Cabinet Office National Risk register: http://www.cabinetoffice.gov.uk/reports/national_risk_register.aspx

Attacks on computer systems are an increasing worldwide phenomenon. These can take place for many different reasons, such as for the purpose of extracting sensitive company information or intellectual property, or for political reasons either to disrupt or infiltrate computer systems, or to cause economic damage through disrupting internet services, as experienced through the denial of service attacks in Estonia.

However, the main threat to the resilience of the Internet is the loss of a part or parts of the network or their inaccessibility. This may come about as a consequence of the loss of a strategic resource (or "node") or a connection to the node or as a consequence of congestion between nodes. Nodes may become unavailable as a consequence of malfunction or physical loss.

The most extensive test to-date of physical loss was the complete loss of New York's main connection to the Internet following the collapse of the World Trade Centre in 2001. However, even with the loss of a significant node local Internet connectivity was not lost entirely although services were extremely degraded. Viruses do not only infect corporate and home computers; the Slammer virus (January 2003) infected Internet routers and other computers running Microsoft SQL server.[1] Routers are an essential component of the Internet responsible for directing information from sender to recipient and their unavailability would result in degradation of service. Although Slammer was particularly virulent causing a number of headline corporate IT failures[2] the effect on the Internet was not significant.

Resources might become inaccessible as a consequence of the loss of a physical connection between nodes. In December 2008 while sheltering from bad storms in the Mediterranean, ships off the coast of Alexandria dragged their anchors severing three international cables. The cable breaks resulted in significant loss of connectivity between Europe and the Middle East, Pakistan and India. Such "single points of failure" are rare. The UK has many diverse connections with the Internet by both cable and satellite.

The ability of the Internet to carry traffic is being continually tested through both legitimate and malicious use. Public interest in the Clinton—Lewinsky affair (1998) and its disclosure on an Internet blog resulted in the highest levels of traffic that the fledgling Internet had seen. During the subsequent years of the dot-com bubble[3] there was the largest investment in resources and connectivity in the Internet. Nevertheless, there are still occasions when legitimate use of the internet—such as the traffic directed to the BBC news site in the aftermath of the 7 July bombings—can lead to disruption as an accidental denial of service attack.

[1] Structured Query Language, part of database software.
[2] Including the Seattle 911 (equivalent to the UK 999/112) service; Continental Airlines flights out of Houston and Newark were grounded as the airline was unable to reconcile passengers on their reservation and flight check-in systems and Bank of America and Royal Bank of Canada were unable to dispense cash from 13,000 ATMs.
[3] Which "burst" in the spring of 2000.

Currently, it is unclear[4] as to exactly how much installed capacity is actually in use. If market prices reflect the situation, connectivity between principle population centres are still very much commoditised. The most recent test at a country level was as a consequence of the cyber attacks on Estonia (May 2007). Although one of Europe's smallest countries Estonia has the highest broadband connectivity in Europe but relatively few connections with networks outside the country. This is the principal reason why the attacks were initially so successful.

A similar disruptive event is not feasible in quite the same way in the UK, partly due to the greater diversity in internet access and the greater range of connections with other countries. Nevertheless, the situation can change and we cannot be complacent. We need to learn from the experiences of other countries and improve our own capacity to prevent and recover from attacks. The Commission initiative and the UK Cybersecurity strategy are complementary in that sense.

1d. *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

There is no "one way" to protect the internet, and most organisations and individuals have a part to play. The internet itself, while based on technologies developed to support military networks, has evolved as a communications and information-sharing tool for civil society, and it is only in more recent years as it has grown exponentially that the use of it has become more closely associated with militarisation. As already mentioned, the UK carries out a risk-assessment programme with the aim of ensuring that telecoms services, including the internet service, are maintained; and as part of this the UK looks at the potential threat of cyber-warfare, and issues where military involvement may be considered, (this possibility should be seen both in conjunction with "conventional warfare" but also as a threat in its own right). In this sense the MOD has a major interest in this area, but Government more widely is also concerned because of the economic damage that such threats could lead to.

Prior to the events of spring 2007, NATO primarily addressed the protection of its own communications and information systems rather than efforts to assist Alliance members to protect their systems. The new NATO policy on cyber defence envisages a common coordinated approach to cyber defence and any response to cyber attacks. NATO also recently established the NATO Computer Incident Response Capability (NCIRC) and the Cooperative Cyber Defence (CCD) Centre of Excellence (CoE) in Tallinn.

NATO's Cyber Defence focus remains the bespoke military communications and information systems but it recognises that the alliance and member state military forces rely heavily on use of the internet, particularly for logistic and administrative purposes.

In common with our allies, the MOD have a role in assuring their ability to deliver Defence outputs, and where these depend on the use of the internet, then there is a role for the MOD. Furthermore, the military have a role in providing assistance to the civil authorities when required to support National Security; this includes assistance in protection of the internet for broader aspects of national security. However, the MOD has a responsibility to operate in harmony and cooperation with Other Government Departments for optimum National effect/benefit and Allies as appropriate. It is particularly because of the need for coordination and cooperation across Government that the Office of Cyber Security (OCS) and Cyber Security Operations Centre (CSOC) have been established and why the MOD are directly supporting both organisations.

In comparing our approach with that of the USA, it should be noted that US Cyber Command have stopped short of adding defence of the public internet into their mission; that responsibility rests with Department of Homeland Security.

1e. *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

Without doubt, one of the major challenges in terms of internet security is the rise of sophisticated malicious software (usually referred to as "malware") and methods of remotely controlling how that software is used. The Government has long recognised the importance of this development and through the surveys published by BIS and its predecessors, the advice to users on GetSafeOnline and the advice to business users on the Cybersecurity Knowledge Transfer Network we have sought to make users aware of the key ways to avoid computers being compromised by this software.

[4] See for example, http://kn.theiet.org/magazine/issues/0906/into-the-light-0906.cfm

It is clear that they major driver for the development of this software is to exploit the opportunities on line to defraud individuals and companies. The software is designed primarily to obtain information in order to access and steal money from bank accounts (or for other criminal purposes) and this is done through remote exfiltration of relevant information—through key-loggers and Trojan software—and to trick users to giving away such information through deception often utilising mass mailings.

CPNI's website gives the following information about Botnets:

"Modern software consists of millions of lines of code, and programming errors—whether deliberate or not—can easily pass undetected. Programming errors create vulnerabilities that attackers with local or remote access can use to take over and control computers very easily. Considered alongside the growth of home computers using high speed broadband connections, there is a clear opportunity for the creation of vast networks of compromised or 'zombie' machines that can be used for malicious purposes.

Botnets, as these networks are called, can be used to gather credit card numbers by 'sniffing' or logging the strokes of a victim's keyboard or stealing information. They are also designed for the delivery of:

— distributed denial of service (DDoS) attacks;

— malware such as viruses, worms and Trojans; and

— spam email."

It is clear that botnets can be used for criminal activities or constructed or procured to carry out denial of service attacks on particular targets. The motivation for such attacks can be varied and can include extortion, political protest or acts of aggression against States or the internet infrastructure itself. It is likely, however, that botnets in the control of criminals are unlikely to be used to cause major damage to the internet as this would undermine their core criminal activity. Nevertheless, the potential for widespread damage exists—as evidenced by attacks in Estonia, South Korea and elsewhere.

The existence of botnets and the potential for such networks to carry out attacks against UK targets accordingly features in the UK's security planning. The development and implementation of the Cyber Security strategy will improve the UK's ability to be aware of the development of botnet threats and to be able to take appropriate action.

It is difficult for the Government to give evidence on the scale of the problem in terms of the number of machines compromised. This would require an inspection of the hard disk of every computer connected to the internet and this is neither practical nor appropriate in a democratic society. Possibly the best publicly available information comes from information security product vendors who can identify malicious activity by access to information gathered through the use of their products. The companies make such information available and we would commend the Committee to look at such reports for an indication on how the problem is changing. For example, the April 2009 Internet Threat Report from Symantec reported that the speed and efficiency with which malware was being "brought to market" was increasing and that the command and control function was changing rapidly to avoid detection and reliance on delivery through rogue ISPs. Symantec make estimates of the number of compromised machines—some nine million—and where the machines and the command and control servers are located.

The UK was assessed by Symantec in 2008 to rank 9th and 10th in the world for "spam zombies" and botnets. Figures can only be rough estimates, though: botnets are dynamic; a compromised machine may become part of a botnet at some future time; and a single compromised machine may be part of several botnets.

We believe that the number of zombie machines on central Government networks is low, and of course, they should be cleaned up when discovered. Connection policies to the Government Secure Intranet should prevent both the compromise of machines to form zombies, and the exploitation of these zombies in a botnet. However, we cannot guarantee that public sector organisations connect all their machines through GSI.

There are a number of initiatives under way that should help to reduce these problems: for example, Government has established the Public Sector Network programme, for procurement of network services. These services will be accredited against security standards set by CESG. The accreditation scheme will, however, be independent of Government, and hence network service providers will be able to market these accredited services to others.

2. International Responses

2a. *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

The European Directive on the Identification and Designation of European Critical Infrastructure (ECI) is designed to allow identification of infrastructure which is critical to two or more European Member States. It forms part of the overall European Programme on Critical infrastructure Protection (EPCIP).

At present the Directive covers energy and transport sectors and is currently being implemented by Member States. The Directive enables Member States to identify assets which although critical to them, do not lie within their territorial borders. Clearly this can only be achieved at a European level—and ultimately will enhance the robustness of the networks that it addresses. However, Member States identifying critical assets outside their territorial borders will have no rights in deciding how this infrastructure is protected, as the protection of critical infrastructure is primarily and ultimately the responsibility of the Member State in which the infrastructure is located. The measures put in place to protect critical infrastructure, including those designated as European Critical Infrastructure (ECI), must be decided on and implemented in line with the critical infrastructure protection policy of the country in which the infrastructure is located.

This approach is extremely helpful in identifying European Critical Infrastructure in the energy and transport sectors across the EU.[5] However, that does not mean that European Member States do not already have processes in place to identify and protect critical national infrastructure. Equally, companies designated as CNI, whether multinational or national, are likely to have their own internal policies on what parts of their company are critical—and this may not map directly on to what is considered CNI or ECI. In other words, encouraging identification of CNI is extremely useful in Member States (or operating companies) where this has not already been done. However—where this is already taking place, there may be an overlap in terms of work for ECI, as each Member State will have its own ways of identifying CNI.

The differing models for approaching and identifying CNI do not however mean that the designation of critical assets is fragmented and inefficient—this would only be true if the identification of ECI was attempted by a Member State on its own. Effective identification of CNI lies more around ensuring that rigorous processes are in place to identify relevant assets at a national level. However, the identification process is relatively meaningless if measures are not taken to protect the assets in question. What the Commission has achieved with this process is robust dialogue on CNI at a European level, a positive achievement in ensuring the availability of networks.

2b. *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

As already mentioned, the UK has promoted public-private partnerships as an effective means of engaging with industry on ensuring resilience and availability of networks; the prevailing model for promoting infrastructure resilience in the Communications sector centres on non-statutory relationships. HMG believes that much of the Commission Communication on Information Infrastructure Protection reflects ideas that have already been adopted with some success in the UK. The private sector—as owners and operators of communications infrastructure—should be closely involved in the thinking which is being developed around actions which need to be taken to protect critical infrastructure. Industry also has a vested interest to their own business to ensure continuity of service. It is for this reason, that the EC-RRG (referred to above) exists and has the characteristics of a public private partnership.

The work that CPNI does with the industry to explore in more detail issues around the protective security of key assets and services depends on a relationship of trust rather than compulsion—again—this is essentially a partnership approach.

Excluding business would be entirely counter-productive. However, it would be equally problematic to use industry ineffectively. We believe that the Commission should ensure it delivers a very focussed industry group with clear and specific deliverables. Without this focus it is likely any public private partnership—be it at an EU level or not—will achieve very little.

[5] The EPCIP scheme is currently limited to those two sectors, as a trial until 2011. The telecoms sector is likely to be one of the next sectors to come under the scheme.

We therefore see value in the Commission exploring what can be done on a multilateral basis within the European Union and how that might link with global initiatives in this area. We do not underestimate the problems of getting companies to commit resource to such partnerships at an EU level nor to establishing relationships of trust on such a large scale.

2c. *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

While we would hesitate in describing the current arrangements as "market failure" we would accept the Commission's premise that more should be done to prepare for high impact, low probability events. We know that certain Member States are far advanced in such planning, promote infrastructure resilience and have response plans in place. This evidence and the forthcoming major exercise on major telecoms failure indicates that the UK is in that group. It is clear that many Member States are not in that position and the activities proposed by the Commission will go some way to address that imbalance. It must be of benefit to the UK to both learn from the experience of other Member States and to see an increase in the general level of resilience in the EU and the ability to respond to incidents that impact across borders.

2d. *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

Much of the early warning system to which the Commission refers is already in place and functioning successfully. Any early warning and incident response capability will—if operating effectively—be of benefit to Member States. The sooner that a warning can be issued, the sooner that CERTS can activate their response to an incident, whether they are directly or indirectly involved. However, this would need to be an enhance to the early warning systems already in place such as that operated successfully by organisations such as European Government CERTs (ECG). See 3a below.

Both CSIRTUK and GovCERTUK (please see question 2e for further explanation on CERTS) have many international liaison partners and belongs to many international fora. Most partner organisations have both a warning and response capability to ensure that any measures which are required to be taken can be implemented quickly. CPNI is a member of EGC (European Government CERT), IWWN (International Watch and Warning Network) and part of a global network of friendly nations. CPNI also has mature relationships with many non-European CERT teams (eg in Australia, US, NZ, Canada and Japan). All of these networks are set up not only to share information on incidents which occur, but also to ensure that early warning of an incident is received wherever possible.

2e. *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

CERTS are a critical part of dealing with internet incidents, as they have the relevant expertise and experience to deal rapidly with any problems. It is also important that CERTS do not work in isolation, but maintain a close working relationship with other organisations who have an interest in cyber incidents such as the private sector and law enforcement. In the UK the CERT model so far proven to be very effective, and many organisations and private sector companies have their own CERT teams to manage a response.

There are a number of Government Computer Emergency Response Teams (CERTs) that are set up to deal with internet incidents in the UK. GovCertUK is the Government CERT for the public sector system, housed within GCHQ. It provides warnings, alerts and assistance in resolving serious IT incidents for the public sector. It works closely with CPNI, relevant law enforcement agencies, international CERT networks, and, increasingly, the recently established CSOC (Cyber Security Operations Centre) in GCHQ. In addition to emergency response GCHQ and CPNI provide warnings, alerts and assessment of information security products and services.

GovCertUK defines an incident as any real or suspected event in relation to the security of data or computer systems. Over the last 12 months, GovCertUK has handled more than 300 such incidents. However, the effort required to resolve any particular incident depends largely on its severity and complexity, which is determined by looking at both the potential impact on normal business and the potential compromise of any sensitive or confidential information.

The Centre for the Protection of National Infrastructure runs another Government CERT, CSIRTUK (the Combined Security Incident Response Team (UK)), which advises the private sector who operate elements of the national infrastructure on how to manage the response to incidents. They are a holistic team who deal with

incidents relating to personnel, physical and electronic disciplines. Although GovCertUK are responsible for Government systems, CSIRTUK handle Government incidents of a personnel and physical nature and therefore the two work closely together.

The Commission has stated that it envisages a "national" CERT which covers more than just public sector infrastructure. CERTs, by their nature, need to share information amongst themselves, and operate in a "federated" environment. It is likely that the Commission are seeking to address the problem of Member States that have little or no CERT capacity. It is unlikely that they will seek in any way to impose a "one size fits all" model on Member States such as the UK that are far advanced in this area.

2f. *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

As noted at several points in this evidence, HMG has welcomed the Commission's promotion of national and Europe-wide policies to protect critical information infrastructures. The national policies proposed are all in line with what already takes place in the UK and therefore we do not see any adverse effect arising. Clearly, the policy involves additional effort at the European level with participation in two new organisations—the Member State Forum and the public private partnership—as well as the prospect of participation in cross-border exercises. This will be a challenge in resource terms but we do not believe that there is—nor should there be—and risk to domestic priorities in this area.

Overall, we believe the Commission initiative should lead to improvements as new thinking is brought to old and new problems and we have to benefit in the broader sense from greater protectivity and response capacity in all of the Member States.

2g. *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

Again, there is no one simple solution and various approaches need to be taken at all levels, which include work at a national level, but also collaboration at European and global levels. The internet operates as a global phenomenon and does not recognise borders; this is something which should be reflected in any work which takes place to ensure availability of internet services.

At a global level there is already significant work happening on enhancing internet (and communications) resilience and security. Clearly a global approach brings with it its own unique challenges such as the variety of economic systems, and technological development stages, as well as Government policy towards the internet, and therefore runs the risk in only succeeding in limited areas—however, that does not mean that collaboration should be overlooked at this level: good work has been achieved in this arena.

The Internet Governance Forum (IGF) is the annual UN forum for bringing together on an equal footing business, civil society, academia, parliamentarians and Governments to exchange views and share best practice on the opportunities and challenges for the Internet under five broad themes: access, openness, security, diversity and critical Internet resources. The IGF was established by the UN World Summit on the Information Society in 2005 to run for a period of five years. The UN General Assembly will decide in October 2010 whether to renew the mandate for a further period.

The UK Government along with the other European Member States believes that the IGF as a unique, bottom-up, multi-stakeholder forum provides the best means for sustaining the fast-moving dynamism of the Internet within an international framework. It has achieved remarkable progress and maturity as a global forum in just three years. A key factor is the absence of the political and negotiating constraints of a decision-making international organisation such as the International Telecommunication Union (ITU) which has much more limited stakeholder participation.

The third IGF was hosted by the Indian Government in Hyderabad in December 2008 and was considered to be the most successful of the three held so far in terms of focus on key issues and challenges. These include promoting access to the Internet for the next billion users, addressing cyber-security, trust and protection of children online, managing critical resources and examining emerging technical, social and economic issues, and climate change.

A European-centric approach will by its nature be able to achieve more within Europe, even if it is limited in the issues it can address (some issues—especially around security may reserved for Member States). An overly prescriptive European approach could also be problematic. Taking excessive measures on internet security within Europe will not prevent outside problems from affecting the system within Europe—as witnessed in

Estonia, but also during events such as the recent cable breaks in the Mediterranean which ultimately affected UK companies who had call centres on the Indian subcontinent. Nevertheless, preparedness for such eventualities will facilitate a faster recovery from any incidents, wherever they originate.

The US approach to protecting their Critical Infrastructure and Key Resources is set out in the Department of Homeland Security's National Infrastructure Protection Plan. The overall approach is similar to that in Europe, recognising that it should be based on risk management, and that partnership between public and private sectors is essential. The UK can add significant value at the level of European policy making by in promoting consistency where possible between approaches to ensure availability of the internet.

3. European Network and Information Security Agency (ENISA)

3a. *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

It is extremely important that any future developments of ENISA's role do not duplicate or conflict with existing regimes that have been operating successfully for some time. A successful European forum for CERTs that is already performing such a role is European Government Certs (ECG). However, it is recognised that EGC does not cover every EU country. The level of information shared by EGC members requires a high level of trust and all organisations have to meet a competency level. To increase EGC membership to cover all EU countries this degree of competency and trust would need to be maintained to ensure that early warning/ information sharing and response capabilities remain effective. ENISA may be able to assist in achieving this and supporting lesser established CERTs to meet the standards required to join. ENISA has been developing expertise in the area of CERTS and EISAS, and its main intention is to advise and help develop the capability within European Member States that are not as well-developed in this field as the UK.

As has already been stated—CERTS are a positive attribute, and are valuable in dealing with internet incidents. In this light, ENISA's actions to ensure that smaller and less well-prepared Member States should be welcomed.

The UK has contributed significantly to the work of ENISA especially in the field of CERTs, and a related concept developed in the UK called WARP (Warning, Advice and Reporting Point). ENISA promotes WARPs, in conjunction with CERTs, and for communities unable to afford the establishment of a CERT. The WARP concept also formed the fundamental basis of the EISAS model. UK has also played a leading role in steering the strategic role of ENISA through dedicated participation in the Management Board (BIS), and by contributing an large number of business and academic experts (far more than any other MS) to ENISA's Permanent Stakeholder group.

3b. *Is ENISA being effective in its role, or does it need reform?*

We have supported the creation of the European Network and Information Security Agency and have participated fully as a Member State in its activities. At the time of its creation, there was some hesitancy about the role of the Agency. The majority of Member States did not want an Agency that had powers that might confuse the responsibilities and authorities of national agencies in this field. For that reason, its role was seen as a centre of excellence and a networking hub to cross-fertilise the undoubted pools of expertise that existing in isolation in varying parts of the EU. It has been effective in bringing together communities of interest in the EU and has had some success in the area of risk management, CERT co-operation and identifying best practice on awareness-raising.

The Agency has had a difficult time becoming established and finding a way to get the best out of the limited resources it has at its disposal. The focus over the past two years on promoting infrastructure resilience has been a positive development and puts the Agency in a good position to assist in the tasks outlined for it in the Communication. Indeed, we are already seeing active participation by the Agency in organising the discussions around the implementation of the Commission's programme.

Looking forward, we now have a new Executive Director for the Agency and this gives scope to review and re-energise the Agency. We are expecting the Commission to offer a view early in the New Year on what to do after the expiry of the current mandate. We believe that virtually all Member States are sympathetic to the idea of continuing with an Agency in this field. It would be surprising if the Commission did not propose to continue with the Agency. The question will be whether we should look fundamentally at what the Agency does and what resources are devoted to it. The outcome of this Inquiry should be a valuable input to forming a UK view on where we should go with the Agency.

We know that the Committee has taken a particular interest in the location of the Agency in Crete. The decision to award the hosting of the Agency was taken by a meeting of the Heads of Government seeking to resolve the location of a number of Agencies. The decision was that Greece should host the Agency at a location of their choice. The Greek Government took the decision to host the Agency in Crete and have defended that decision robustly on the grounds that it accords with EU regional policy. The location is distant from the major population centres of the EU and the independent consultant's report into the performance of the Agency highlighted the management challenges that this posed.

At this point, we do not know whether the location of the Agency will feature in the discussions around the extension and revision of the mandate that are likely to take place next year.

4. Timescales

4a. *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

In the Explanatory Memorandum on the Commission's Communication, we noted the short time frame of the recommendations and planned actions and that this was challenging for such an initiative. We have now clear evidence that the Commission is seeking to make progress on all of the key activities in the timescale envisaged. We still believe that some of the ideas for what Member States should do—particularly in terms of carrying out exercises—will prove to be unrealistic.

November 2009

Examination of Witnesses

Witnesses: Mr Geoff Smith, Head, Communications Security and Resilience, Information Economy Directorate, Department for Business, Innovation and Skills and Dr Steve Marsh, Deputy Director, Office of Cyber Security, Cabinet Office, examined.

Q1 ***Chairman:*** Dr Marsh and Mr Smith, thank you very much for coming here. Dr Marsh, we have talked before.
Dr Marsh: Yes.

Q2 ***Chairman:*** Thank you for coming again. Welcome, Mr Smith. We understand that it has not been possible for you to submit your written evidence in the time available and if after this evidence session you wish to clarify or amplify any points you have made or any additional points you would like to make we would much welcome your submitting that supplementary evidence, or letting us know in one way or another. Perhaps you would both like to introduce yourselves at the beginning and just explain to the Committee what your remits are in the capacities which you fulfil.
Mr Smith: Thank you. I am Geoff Smith and I head up the work in the Department of Business, Innovation and Skills in our section that deals with communication and content industries and I deal specifically with national security and resilience issues in the communications sector. I think you have met my colleague, Alice Reeves, who today has to attend a conference in Stockholm on this very subject.
Dr Marsh: Good morning, my name is Steve Marsh; I am from the Cabinet Office. I have been in the Cabinet Office for a few years but over the last six weeks now, getting on for two months I have been in the new Office of Cyber Security, which was set up as a result of the Cyber Security Strategy that the government published in June, and we are taking a strategic overview of cyber security generally and trying to advise on leadership and coherence of HMG policy in this area.

Q3 ***Chairman:*** Thank you very much. I will begin and ask a basic question. Do you believe that Internet resilience is an appropriate topic for the European Union to tackle? And whilst most security issues are either local or global, do you believe that acting at the European Union level will be effective and should we not also be involving the United States and Russia?
Mr Smith: We believe that resilience of critical infrastructure is a vitally important issue for all Member States and it is only right that the European Union uses the influence that it can bring to bear to enhance the ability of Member States to protect their critical infrastructures. We have to be very clear on what the role of the European Union is and this is an area where we get into a well trod problem area of national security and what is the responsibility of Member States versus the role of the Community. That said, we very much welcomed the communication put out by the Commission on the protection of the critical information infrastructure; we thought that was a positive step forward, and I think you may recall that our explanatory memorandum said that we welcomed the initiative. We had some concerns around the action plan and the realistic deliverability of some components of that, but in terms of should the European Union be providing some degree of leadership in this area we have no problem with that in principle—we think it is a good thing. It is worth just diverting slightly on

to the Pillar arrangements, which I think will be obsolete on 1 December; but at the moment we have two parts of the European Commission with parallel initiatives in this area. Under Pillar 1 we have the longstanding work on network and information security, which has given rise to the ENISA Agency. We have the communication and we have the work that is going on in the framework regulations governing the communications sector to improve security through that route. So that, if you like, is under the commercial part of the Community. Under Pillar 3 we have the European Critical Infrastructure Protection Activity and information and communication technologies will eventually be covered in that process, and we will have the activity of identifying European critical infrastructure in the UK and providing some degree of comfort to the rest of Europe that we are sufficiently protecting that. To answer your question: yes, we do think that the European Union has a role but clearly we have to be careful not to stray into the territory of national security, so there is a fine line to be trod there. On your second point about is the European Union involvement enough or should we be involving other countries, clearly the European Union cannot solve all of the problems of the global Internet environment and I do not think the Communication pretends to do so, and we certainly would not support that line of thought. What we can do is encourage Member States to improve their protective activities and to encourage the laggards up to the speed of the front runners. So there is a lot that the European Union can do to improve national protection and deal with that local issue that you described. The Communication does look outwards; it does look at what we need to do on the global stage to improve Internet resilience. I think it is one of the least clear parts of the Communication and I think even today I am not sure that I could give you a clear account of where this work might take us. You will recall from the explanatory memorandum and the subsequent correspondence between Lord Carter and the House of Commons' Committee that we were concerned that there should not be a "land grab", I think were the words, by the Commission to gain greater influence in the international arena in this area. But that said, the idea of discussions at the European Union level to decide what we think is important in terms of protection and in terms of standards and in terms of how the international arena might be engaged, is something that we can do at a European level; we can have that kind of dialogue which will give us a European voice in these discussions. As far as individual countries go, we are not coming to this fresh—this has been going on for many years. We have strong relations with particularly the United States and other leading European countries and other countries elsewhere in the world, so we have some solid relations to build on, and we need to think how this agenda can be promoted through international fora such as the Internet Governance Forum, the International Telecommunications Union and, in a different way, the Organisation for Economic Cooperation and Development—the OECD. So there are a number of areas where we need to have the European voice and we need to develop relations on the global scale, including Russia although clearly there are issues there around the different approach that they had to some of these issues. But we need to talk to them.

Q4 ***Chairman:*** Would you just like to expand on the problems with Russia?
Mr Smith: We have in the past had issues with Russia in the United Nations where they have very much seen this as a military threat to their own security and the use of what they call information weapons. That is a possibility—and we may get on to cyber warfare later in our evidence—but we felt that they were promoting that for their own strategic purposes and that it was only part of a much broader threat profile which we needed to address, dare I say it, particularly cyber crime originating in parts of Eastern Europe, which I think is something that they did not particularly want to discuss. We have had that kind of issue with Russia and other countries in a multilateral forum.

Q5 ***Lord Mawson:*** Can you give us a practical example—you said that the EU has a role—of where actually it has made a practical difference to something in this area? Can you give me a practical example where the EU's involvement has made a real difference?
Mr Smith: I think that the creation of the European Network and Information Security Agency, which is not the biggest success story of all time, it has to be said—it is a small organisation—has had some impact in drawing people together in the European Union. Where you have isolated pockets of expertise they have started to make links between those groups so that there is a cross-fertilisation of ideas. They have advanced thinking in Europe on risk assessment, so there is an increasing commonality about risk assessment and risk management. So there are activities there. I think the forthcoming changes to the framework by which European communications industries are governed is going to be a step change in how it treats security, so this is again something that is happening at a European level.

Q6 ***Lord Mawson:*** I will ask my question. What is the UK Government doing to make the Internet more resilient and what role should the Internet industry play in this?

Mr Smith: Can I start by trying to describe what we do within the UK and the industry involvement with that? We look at the communications sector in its entirety, so that would be essentially the fixed line, data and voice communications, the mobile sector and the components of the Internet, primarily peering points and the domain name system. We in the department have the departmental responsibility for ensuring the resilience of that sector. This is part of a much broader government agenda to ensure the resilience of critical infrastructure, and we work with the Cabinet Office on broader issues around national capability in this area and how we reflect issues such as the outcome of the Pitt Report on flooding, which is quite a large piece of work in itself. So we work with the industry in a largely light touch regulatory environment compared, say, to the energy sector. We do not have the same degree of control of the sector that exists there. But we do have a strong relationship whereby the industry itself owns its national emergency plan and we have a standing group called the ECRRG—that is the Electronic Communications Response and Recovery Group—and that group meets regularly and is hosted by my department, but various departments sit together with the industry to discuss general issues of resilience and emergency planning and recovery. This goes down to quite granular issues about how you cross-police barriers in an emergency to get to communications and there are quite large issues around potential electronic attack, but that group is essentially the forum where we discuss these resilience issues. On a more detailed level CPNI—the Centre for the Protection of National Infrastructure—has relations with those parts of the infrastructure that it regards as critical and it has a very close relationship with the managers of those sectors of the industry. We work together with CPNI in establishing a programme of work by which they can work with the industry to deal with issues such as personnel security, an area in which we think that possibly the industry could be doing more, and we work with them to enhance their ability to manage personnel security. So we work with CPNI but CPNI have a direct relationship with the managers of the critical elements of the industry and they have mechanisms such as the information sharing activity which they sponsor, which has been a great success in that it brings people in the industry that actually understand the problems on their networks into the same room so that they can exchange real stories and experiences in pretty near real time, and this has actually given a lot of comfort to the industry that they are being supported by government in addressing these issues. Those are the main areas. Possibly just looking forward, I am sure you are all aware of the Digital Britain Report that was produced in the summer and somewhere towards page 150 there was a bit on Internet resilience and security and we are putting together a Digital Economy Bill which should be introduced after the Queen's Speech, and that will put new obligations on Ofcom to report to the Secretary of State on communication infrastructure. This will be part of its new obligation to promote investment in infrastructure; but we would be asking Ofcom to report on investment and particularly—and this is new—we will be asking them to report on issues relating to the resilience of those networks and services. So that is a new string to our bow, if you like; we are pushing the role of Ofcom forward in this area. The Cabinet Office is looking at the overarching legislation, which is the Civil Contingencies Act. That work is being done in two phases and we are approaching the end of phase one, which—perhaps doing them an injustice—is tidying up a few problems with the current arrangements and we are more fundamentally thinking about the scope of the Civil Contingencies Act and the role of responders in that, and I think that that kind of thinking will be starting shortly with possible adoption in 2011 or thereafter, according to the tastes of the incoming administration. Those are the forward looking activities.

Q7 ***Lord Hodgson of Astley Abbotts:*** The ECRRG and the CPNI are both public sector bodies or private sector?
Mr Smith: CPNI is hosted by the security service; it is part of government.

Q8 ***Lord Hodgson of Astley Abbotts:*** The ECRRG?
Mr Smith: The ECRRG is a group where industry and government discuss.

Q9 ***Lord Hodgson of Astley Abbotts:*** So it is a public sector body?
Mr Smith: It is not a body really; it is more of a standing committee.

Q10 ***Lord Hodgson of Astley Abbotts:*** Who initiates it all?
Mr Smith: We have recently passed the chairmanship to industry and it is chaired this year by someone from Cable and Wireless. Before that it was chaired by a Cabinet Office official. Thinking out loud, it may be that in the future it may be more appropriate for Ofcom to chair it with their new responsibilities, but the constitution is that it is an industry-government grouping. We host it and take care of accommodation and all that sort of business, but it meets every three or four months.

Q11 ***Chairman:*** Before I call on Lord Mawson again, would you not agree that in the report that this Committee makes to the House of Lords as a whole

that our report would be significantly more complete if we had taken evidence from CPNI?
Mr Smith: That is a very difficult question for me to answer, my Lord.

Q12 ***Chairman:*** I thought it was a very simple question!
Mr Smith: From your perspective would your report be enhanced by input from CPNI? Yes.

Q13 ***Chairman:*** Thank you; that is all I asked.
Mr Smith: You may be assured that the government's written evidence will incorporate masses of material written by our colleagues from CPNI. It is a matter of legal nicety why they are not here with us today, and obviously we regret that as much as you do; but I am sorry that I really cannot answer for their position on speaking to Select Committees.
Chairman: You have been most helpful, thank you.

Q14 ***Lord Richard:*** When do we get it?
Mr Smith: You have given us a deadline of 13 November. We will do our best to meet that deadline. We would have liked to have had it before this Committee, but of course given that next week is our big exercise we asked to be seen this week, so it has not been possible.

Q15 ***Lord Richard:*** Will you deal with the exercise in the evidence?
Mr Smith: We will certainly mention the exercise but two days after I am not sure how many conclusions we will be able to draw of use to this Committee. But the exercise takes place on 11 and 12 November, so one day after. We will definitely tell you something about that exercise; I am happy to tell you about it today.

Q16 ***Lord Mawson:*** My background is in entrepreneurship and I know that this industry is all about entrepreneurship and I know that in my experience, trying sometimes as an entrepreneur to engage with the systems of government and the civil service at a rhetorical and discussion level is one thing, but really engaging in any deep way has been very, very difficult because the cultures are fundamentally at odds with each other. I would be interested to know how many people from this entrepreneurial industry are actually involved in your department working with this because it is one thing to meet at round tables but another thing for these people to be really involved in the heart of what is going on in your department and understand this entrepreneurial business. Are they there in the midst of you or is it just a discussion that you are having with them?
Mr Smith: At the moment I do not think that we have any secondees directly in my area. We have in the past and we do employ people that have experience in the industry. I actually find it odd, to be honest, I think my department is possibly the one that is most in tune with the business way of thinking. You may disagree but—

Q17 ***Lord Mawson:*** The words are there.
Mr Smith: I think we do have a pretty good relationship with business in general and we have a number of opportunities in Whitehall and Brussels and elsewhere to speak with industry, both in formal and informal surroundings. If I can stick to this area I think that what we have done since we have recast this group ECRRG is to try and bring the industry more into the centre of it, rather than government leading this process. We have tried to make it more of a partnership and we sit down with the Chair and Vice Chair of that group and together try to work out the agendas and ideas for the forward programme. I am not sure if that really covers entrepreneurship but certainly someone who works in the engine room of BT would probably not regard themselves as an entrepreneur.
Dr Marsh: Perhaps I could also add that the Department for Business funds the Technology Strategy Board whose remit really is to try to bring in new ideas from industry with academia to solve pressing government problems, and the Technology Strategy Board runs something called the Network Security Innovation Platform where they have been funding particularly some proposals to help with some of the security issues that we recognise across a whole range of systems, and they also fund something called the Cyber Security Knowledge Transfer Network, which again is really set up to try to bring together a broad community of people to share ideas and best practice, but also to bring particular projects forward when they can.

Q18 ***Baroness Garden of Frognal:*** You referred earlier on to some of the laggards within the EU in this respect and I wondered if you could say whether the UK was ahead or behind the rest of Europe in making the Internet more resilient.
Mr Smith: One of our issues with the Commission on critical infrastructure protection was that there were a large number of assertions in there without a great deal of evidence to support. I think possibly their instincts are right but we did feel rather uncomfortable that there is a lack of evidence. So I have to start by saying that I am not sure there are enough metrics to be able to give you a scientifically based answer to that question. Anyone who has any dealings with this policy area will know that there are some leading countries within Europe, and I think that the UK is definitely one of those countries, along

with France, Germany, Sweden, the Netherlands and a very few others. So I think that the Commission have always looked to us for ideas to draw on our experience, and if you look at the work that was done in the OECD—and I am happy to give you that as part of our evidence—they did work on critical information infrastructure protection and they looked at a group of leading countries and I volunteered the UK to be in that group. I think that both there, in the OECD and in the Commission's Communication, we actually see a lot of what we are doing reflected back as emerging best practice: for example, the idea of public/private partnerships having an important role to play in Europe I think reflects the way that we have worked with industry in the UK in a non-regulatory and non-prescriptive way of achieving public policy goals. So I think that we are one of the leading countries in terms of policy. Whether we are in terms of real resilience on the ground, I hesitate to say because tomorrow we may lose Internet connectivity and I would look extremely stupid; but I do think that we are trying very hard to work with the communications sector to identify the important issues and to work together with them to solve it.

Q19 ***Lord Dear:*** I would like to turn your attention to the question of botnets and I have a number of questions about those so perhaps I can give you an omnibus and you can answer them in whichever order you like. We are concerned to know whether you think that botnets could bring down the Internet, which leads one to ask how widespread is the threat of zombie machines which, I have to tell you, I know not a lot about but I know the principle, and perhaps you would explain those to us in greater detail and indicate whether you think that they are operating on the public sector networks. And of course all of that wrapped together and then what is the government doing about it, if anything? Or is anything possible, I should say!

Dr Marsh: If I start with the question about whether botnets could bring down the Internet, this is one of the answers where you have to start off by saying it depends really what you mean by "take down the Internet". There were a couple of major attacks in 2002 and in 2007 on what is called the domain name service for the Internet. This is the way in which when you type in, for example, www.google.co.uk it is then how the computer finds out whereabouts on the Internet the target machine really is. There were, as I say, a couple of major attacks in those years that caused significant disruption at the time. As a result of that of course industry has responded and made that service much more resilient as a result. We have also seen disruption when there has been widespread infection of machines, simply because of the amount of extra traffic that was going on on the Internet. So I think there is no doubt that there could be disruption if a new vulnerability became exposed and was exploited, but whether that would lead to a complete collapse of the Internet or whether it would be temporary until a fix was put in place by the industry, it is very hard to judge that. One short term mitigation is that a lot of the botnets are exploited for criminal financial gain, and in a sense it is not in their interests to bring down the infrastructure which is earning them the money, so a lot of the activity around botnets I think is not going to be directed particularly at damaging the infrastructure itself, although of course there is always the possibility that a different group with different intentions might try to exploit those mechanisms if they could.

Q20 ***Lord Dear:*** I was thinking that botnets would be therefore targeted against an individual company or group of companies rather than the whole Internet. A sort of extortion or ransom.

Dr Marsh: That is right. There is a big criminal market investing in botnets, for example, and that is used for criminal gain, sending spam emails or extortion and phishing attacks trying to get people to enter their personal details into fake websites and so on. How widespread they are in the UK again is very hard to come up with very precise figures about that. The Internet security company Symantec in 2008 assessed that we were about ninth and tenth in the world for respectively what they called spam zombies and botnets; so the spam zombies are the machines that have been controlled by someone else to send out these fake emails to a large number of people. Those rankings tend to follow the take-up of the broadband across the world as well, so the US and China were high up in those rankings at the time. But they are really rough estimates. The botnets themselves are quite dynamic. When a machine is compromised we do not necessarily know whether it is going to be in a botnet straight away or whether it is going to be used at some future time or used for some other purpose. Also if a machine is compromised it could actually be part of a number of botnets—in that it may be compromised by several different bits of malware at the same time; although having said that the criminals, often having compromised one machine, try to protect it from compromise from other rival criminal activities as well, interestingly enough. As far as the public sector networks are concerned, I think on central government networks we believe that the numbers of zombie machines are actually quite low and that is because we have something called the government secure intranet (GSi) which has fairly stringent codes of connection that departments have to sign up to before they can connect up to this network. Of course, if zombie machines are discovered we clean them up as soon as we can. But having said that, we cannot guarantee

that public networks are entirely free of these machines because we cannot guarantee that all the machines that an agency or local authority puts on to their systems are actually connected through the GSi; they may, for business purposes, have stand alone machines that are connected direct to the Internet, and although clearly we would encourage them to adopt the stringent security policies that we have elsewhere we cannot guarantee that, particularly when you get out to the wider public sector beyond just central government. There are a number of things that we are doing within government which we hope will help as we go forward. From the Cabinet Office, for example, we have established something called the Public Sector Network Programme to try to put in place a framework for a common procurement of government networks as we go forward, and as part of that framework we are going to put a security policy in place that has been set by CESG, which is the protective security arm of GCHQ at Cheltenham, and as for those security standards we want it set up as part of an independent accreditation scheme so that the communication service providers, as well as providing those services into the public sector, can actually advertise them as meeting a certain security standard and then make those available to the private sector as well, if they so wish to avail themselves of that. Of course botnets are just one possible use of compromised machines as well and really there is a whole range of activities that we are also trying to engage in just to reduce the probability of compromise of machines anyway. I mentioned the Technology Strategy Board earlier on; that is funding both something called the Network Security Innovation Platform and also Cyber Security Knowledge Transfer Network. There have been a number of activities that have already been funded through those routes. There is some work on security economics because there is a perception that at the moment the economic model of providing information on security is in some sense distorted, and so the risks and the costs are not necessarily falling in the right place to fix some of these problems. We have done work on human factors in security, particularly with the phishing emails where you are very much relying on the individual sitting at a computer who can fall for the bait, if you like, and responding to this email. There is a big piece of work there that needs to be done about trying to make it easier for people to do the right thing from a security point of view, and there has also been funding and taking forward some work on secure software development to try to make software really more secure out of the box rather than trying to fix the vulnerabilities later on.

Q21 ***Lord Dear:*** On that last point—and also refer back to a point that Lord Mawson made about entrepreneurs—it occurs to me that with my own computer, for example, as with everyone else in this room, I guess, eventually you put in some sort of antivirus software, and there are a number on the market and I do not know whether there is software that would protect individuals or companies from botnet attack. Groping around in my own mind with that as a concept my question is largely to do with to what extent you can attract in really good entrepreneurial brains—companies, individuals—to help you to solve this obviously much bigger problem than just a virus on the computer because it is widespread.
Dr Marsh: Absolutely, yes.

Q22 ***Lord Dear:*** The industry I guess would have a deep interest in this itself. But can you help us as to how you can stimulate that and whether that is possible.
Dr Marsh: Indeed. The Knowledge Transfer Network is actually precisely trying to do that; it is trying to bring together individuals, small enterprises and academia; and to provide some core funding to form consortia aimed at solving particular problems that have been identified, both by government and by industry. But there is a range of other industry groups as well where we do try to expose the security challenges that we see from government and we try to encourage innovative solutions to those problems.
Mr Smith: Can I extend that slightly into the area of skills? Part of the agenda here is to get the right people in business with the right skills to take the right kinds of actions. Dr Marsh and I have been quite instrumental in helping the Institute of Information and Security Professionals get off the ground and I think that that provides a new framework for professionals in this area; but I think that there is a lot more we can do. It is quite interesting, the US have a cyber security strategy and one of the components of that was a challenge where they offered prizes to people—they were trying to attract people into becoming professionals in this area, so they had a challenge. Unfortunately some of them would try to break into this site, which is not what I thought we had in mind but some of the other challenges were more constructive and it was a surprising success, so we may look at that as another model that we might use in this area.

Q23 ***Lord Mawson:*** The reason I want to push you on this is because in the social enterprise sector, in which I work, there has been lots of reports and lots of discussion, et cetera, but those of us who actually build real things on the ground, some of these in some of the poorest communities in Britain, have discussed over the course of the years that to talk about it and produce reports, et cetera, is one thing, but in practice actually it has not got any easier and in reality the learning by doing cultures that are necessary are not

taking place, and it seems to me that this is a great opportunity to begin to develop some new cultures within government, the EU, the Civil Service, but to do that you need to embrace entrepreneurs within your system, so that actually it is not just a conversation around a table but you are actually dealing with real practical problems together and looking for entrepreneurial solutions that begin to drive new ways of dealing with those problems, because unless we create those sorts of new environments which is not the traditional way that government has been operating—and I suspect the EU has been operating—this world will continue to expand exponentially and will increasingly become disconnected and challenging to governments around the world. So I am wondering about how we actually begin to use this problem as an opportunity to really grow new cultures.

Mr Smith: I could not disagree with anything you say and I think it is a challenge for us. Can I just refer in passing to another output of the Digital Britain Report where we have committed to work with business and law enforcement in creating a new partnership to address low level cyber crime, and I think that will start to get us into this area of how do we help ordinary users of computers avoid the pitfalls that we see at the moment. That kind of entrepreneurial spirit needs to be applied to that kind of initiative, and I certainly take that point.

Q24 ***Lord Mawson:*** But it is not going to happen unless it is at the heart of your organisation with people with real hands-on experience who are in your office and people who are dealing with these things. It is all about the people and the relationships in my experience in this world.

Mr Smith: Yes.

Q25 ***Lord Marlesford:*** It is really on this point because I do look at the whole problem myself from the consumer protection point of view rather than the big scale cyber attacks. You have just referred to one of the points that I want to ask you about. To what extent can you educate and warn consumers of the dangers of computer crime and fraud and how they should protect themselves from things like phishing expeditions? Secondly, to what extent can you identify the source of these sorts of frauds and give the information to the police of the country concerned? Thirdly, it always seems to me that as criminals are trying to get information very often in order to get money that it ought to be possible for police forces to set up stings which would mean that they would actually catch the people at the point at which they get the money.

Dr Marsh: Shall we start with the advice aspect? We have for a few years now—four years—been running with the private sector a campaign called Get Safe Online and we do very much try to make simple, straightforward advice available to the public and to micro businesses. That I think has met with mixed success. In its class it is good but it is recognised that the awareness and penetration of those messages is actually quite difficult. I think there is almost a philosophical point here about whether it is reasonable to expect individuals and small businesses to become in some sense an information and security expert before they can be online. We need to certainly make people aware that there is danger out there and look for the warning signs for avoiding that danger; but I think at the same time we do need to make the software that they use actually easier to use securely. At the moment if you use commonly available anti-virus software it is always bringing up notifications that something is trying to communicate with the Internet and it is always very hard to know whether you should allow this or not; so people just tend to click on the button and say yes, let it go ahead. We saw this with the Microsoft Vista operating system as well; it was much more secure but it kept on asking the user questions about whether they wanted to allow some action to happen, and of course the reaction from the user was, "Just get on with what I am asking you to do," and they would just click the button and try to get it out of the way and it became unpopular just because it was seen as getting in the way of doing the business. In terms of identification, that is a problem and it is a problem because of compromised machines and botnets and so on because it means that the attack can actually be hidden quite successfully by the criminal at the far end; they can go through several layers of different machines before the attack becomes apparent to the user. So it is a hard problem to get through that initial smokescreen of machines and find where the attack is really being controlled from and sourced. The police do do that successfully and on occasion they certainly work with international counterparts and when they can identify controlling machines they will take those down. The criminals themselves are also very sophisticated and they will quite rapidly set up an infrastructure to replace the one that has been taken down. So it is a continuing challenge as far as the police are concerned to take those controlling networks off the air and to keep them off the air.

Q26 ***Lord Marlesford:*** And stings?

Mr Smith: They call them honey traps and I think the police do use them.

Dr Marsh: I do not have specific information about whether the police run sting operations or not.

Mr Smith: I was told that the FBI once penetrated a criminal network to the point where an FBI operative was asked to run the network and at that point they had a moral dilemma! So, yes, they do. Most of these operations are intelligence led and I think they do set

up traps. The problem has been the slowness of the law enforcement agencies in certain countries to be able to respond with requests. As we have found in the fight against child pornography, even if you know where it is coming from, where it is hosted it is a slow process to take it down—even something as obvious as that.

Q27 ***Lord Hodgson of Astley Abbotts:*** One issue in relation to low level criminal activity and low level attraction of money occurs with credit cards. Credit card companies are not obliged to provide a clear statement on the credit card statement of whom and what the amount was debited for. From time to time you get £1.75 on your credit card statement and you cannot recognise it and you pay it. I suspect there is as lot of this going on and a lot of money is being picked up at quite a low level, which could be much better noted if there was a requirement for credit card companies to give a clear statement as to what the money was for.
Mr Smith: It is an interesting idea. I am reluctant as a resilience expert to talk too much about credit card statements, but certainly we will take that point away. I should point out that I referred earlier to the partnership that we are establishing under the leadership of Alun Michael, MP to try to bring the law enforcement business, including the banks and credit card companies, closer together in solving these low level crime problems. We have greatly increased the capacity of the fraud authorities to deal with online problems. The OFT are looking to very much up their game in terms of online scams; so I think there is a lot going on. What should go on a credit card statement, we will have to take note of that and perhaps come back with more evidence.

Q28 ***Lord Richard:*** My Lord, can I just make a plea when it comes to the evidence, before I ask a question, this is obviously an area that is spawning initials and in the evidence can you be absolutely clear that we know what the initials mean and that we know where the particular body, whatever it is, fits into the overall structure?
Mr Smith: We will take personal responsibility.

Q29 ***Lord Richard:*** I am obliged. I want to turn to the possibility of cyber warfare and the threat. I assume that somebody in Whitehall or a group of people in Whitehall or the department or committee or what have you actually assesses the threat. Could you tell us who is on that committee or is that too sensitive? I assume that the Foreign Office is involved and I assume that the Ministry of Defence is involved and GCHQ and all the rest of it.
Dr Marsh: That is right; the normal suspects.

Q30 ***Lord Richard:*** Then I assume that you talk to other countries?
Dr Marsh: Yes.

Q31 ***Lord Richard:*** The Americans, the French, the Germans and friendly countries like Australia, New Zealand and South Africa.
Dr Marsh: The usual suspects.

Q32 ***Lord Richard:*** The usual suspects again.
Dr Marsh: Yes.

Q33 ***Lord Richard:*** Two questions arise. One is: are you satisfied with the amount of information that you get in order to come to these sessions? Secondly, if you are what assessment have you come to about the possibility of cyber warfare? Thirdly, dealing with the threat, where do you think it is going to come from?
Dr Marsh: The first question, are we satisfied with the amount of information, I think the answer to that is no; but that is not because of a want of trying. This is an area where it is fundamentally difficult to spot the indicators and warnings that one would normally see in conventional military activity. The development of these techniques goes on behind closed doors and it does not need a lot of resource to do that. It is very hard to get a good understanding both of the techniques that have been developed or the intention behind them. Of course cyber warfare is really just one end of a wide spectrum of threats. Perhaps again, unlike conventional warfare there is less of a distinction between the different phases of attacks on computers. There are some activities which may be a precursor to criminal activity could then subsequently be used for cyber warfare as well—you just do not know when machines are first compromised what that is going to be for. So we do not know as much as we would like to and that is something that collectively we need to address as we go forward. In terms of the overall risk that we assess, again in some sense because there is this continuous spectrum of attacks at some level, you almost do not mind what the intention is—you need to make the systems more resilient or more secure anyway, whether it is because you are worried about cyber warfare or because you are worried about serious criminality or cyber terrorism, or whatever. At some level you just need to carry on doing what you can to protect the systems that are critical. But of course once you get into what you believe to be cyber warfare there are a range of other national measures that you may start bringing into force. Just because you happen to be attacked in cyber space does not mean that you should not respond kinetically, for example, or diplomatically. But then again you get

into the problem of attribution—how do you know where the attack is coming from, who is behind it and what is their intention? So there are some very difficult conceptual problems around that and it is that area really where this new Office of Cyber Security is working very closely with the Ministry of Defence and other bodies to try to make some progress in understanding the full landscape.

Q34 ***Baroness Henig:*** On the same theme of cyber security, we have heard about the EU; should we be looking to NATO to protect the Internet, rather than the EU Commission?
Dr Marsh: Yes. There is no one way to protect the Internet; many organisations have a role to play in this and clearly NATO has a role itself in protecting certain networks, the EU has a role and national bodies have a role as well. Really everybody has to consider what they are able to achieve and act appropriately to make the Internet more secure.

Q35 ***Baroness Henig:*** Would a body like NATO in any way work with the EU? We have come across instances in other areas where collaboration is not necessarily as good as one would like. Is there scope?
Dr Marsh: I think there is a lot of scope generally for sharing information on vulnerabilities and the attacks that are going on and how you should best protect yourself against those, and there are a range of information sharing mechanisms that are in place and they are things that we support and we would continue to support and encourage others to join in as well.

Q36 ***Lord Marlesford:*** One danger must be nowadays the transmission of malign or dangerous information, whether between criminals or indeed governments of countries, in an encrypted form which may be extremely difficult to intercept.
Dr Marsh: Yes.

Q37 ***Lord Marlesford:*** Would you like to comment on where we are on that?
Dr Marsh: That is quite true. There is always this balance between protecting the individual and their freedoms and their right to privacy and so on, but also not completely crippling law enforcement in trying to understand what the criminal is up to. It is a difficult balance to achieve. For example, from the academic point of view the challenge is always to make more secure systems but we need to recognise that really the technology has no morals, if you like—it is the users who are behaving morally or not—and we have to be careful that we are not crippling law enforcement or our security agencies at the same time as trying to protect public privacy and the freedom to exchange information as they wish.

Q38 ***Chairman:*** What is your view of the sources of the attack a few years ago on Estonia?
Dr Marsh: That was one of these examples where it was quite hard to make a simple judgment of where this was coming from. Clearly there was a lot of supposition in the Press about where it was from, but without getting into some of the more sensitive ways that you may begin to attribute these attacks it is very hard to say whether these were state-sponsored or state-condoned or really people who thought that they would act patriotically for whatever cause they were supporting at the time.
Mr Smith: Including people within Estonia, of course. The cause of that problem was the removal of a Soviet war memorial within Estonia. There is a large ethnic Russian group within Estonia, so it was a very complex situation.

Q39 ***Lord Harrison:*** I do not think there was much evidence that it was state-sponsored. Gentlemen, I am interested in what is the added value of dealing with this matter at an EU level, and so I ask: the EU Communication talks about pan-European exercises on large scale network security incidents. Is the UK already running this sort of exercise on a national basis? What can be learnt from these exercises, say in particular from some of our colleagues in Germany, who have a strong interest there? Or from the smaller countries like Latvia and Malta, who may not be geared up in the same way but may derive sustenance from our being involved at that level and helping them with such information.
Mr Smith: That is a very good question. If I can answer what the UK is doing first? I referred earlier to the major exercise that we are running next week, which is called White Noise—that is the code name for the exercise. This is our first major test in the UK of a catastrophic communications failure. The scenario would be based on the loss of the Public Switch Telephone Network—that is the voice calls for which we use the telephone—and that will collapse nationwide in this scenario. We would still have data transmission, we would still have mobiles and secure resilient communications within government—otherwise we could not run the exercise.[1] This is the first time we have done this and it is giving rise to a lot of interesting discussion around Whitehall, around government departments' dependencies on this service, and it is going to give rise to a lot of thought and a lot of action down the line. So even before we have the exercise underway we have actually learnt a lot from this activity. What we will learn next week is whether we can as a government respond in real time to managing the information in from the industries and getting a clear

[1] Subsequently the witness informed the Committee that he had been mistaken in saying this; the true position was that the exercise assumed the unavailability of the mobile networks.

of idea what can be done to recover managing media and parliamentary expectations for answers on what is going on. So that is what we are going to be testing next week and we have several hundred people playing in this exercise—it is a big activity. We have spent a lot of money getting contractors to help us on this; the amount of staff time put in by other government departments and the industry is immense—it is a big activity. Apart from Sweden I do not know of anyone else who has tried an exercise on this scale. So, as I said earlier, when we talked about the Communication they are reflecting certain things that we and other leading countries are doing and the idea in there that you should be testing your ability to manage and respond to incidents is absolutely right. What we worry about is how realistic this would be to expect every country to do this by the end of 2010—frankly, that is not going to happen—how realistic it is to have really large scale exercises in Europe because of the differences that you and I have identified. Again, that would be a major challenge, to put it politely, to do that in the next 18 months. I do not want to sound negative because I think the idea that we should aspire to every country having this capability to test their emergency response arrangements has to be a noble aspiration. Similarly, I think the more we can test, a large regional or global incident and our ability to manage across borders, that must again be something to which we should aspire. There is some experience of this because the US runs a series of exercises called Cyber Storm, where they invite certainly friendly powers, including ourselves, to participate in a very large and very expensive exercise that they manage, on attacks on the Internet and how we manage that across borders. So there is some experience of global cooperation but, again, this is something that we have to build on. Incidentally, I would hesitate to tar Malta with that brush—they are a quite organised and well resourced country. We get on well with the Maltese!

Q40 ***Lord Mawson:*** You assume that the government communication system will actually work and I used to maintain that government communication system in the north of England 30 years ago in the face of nuclear attack, and invariably when we used to look at some of this stuff it actually did not work when we were trying to maintain it—there were lots of complications with it. Why do you assume that it will work?

Mr Smith: To be brutally frank we could not do an exercise if we could not communicate. We know that is the problem. We are working on the development of the High Integrity Telecommunication System. This has been organised by another part of the Cabinet Office to give us resilient communications. You know we have Airwave, which is a resilient communications network for the blue light services and we are creating a service within government and we are talking to the industry about how we would communicate to the industry if the Public Switch Telephone Network were to go down, and there are several solutions being actively discussed and after next week the momentum towards solving that problem will be greatly increased. Clearly we would be reduced to carrier pigeons if we did not have some means of communicating within government. Our assumption next week is that the data stays on and so there would be email and voice over Internet voice telephony, but it is possible to envisage an even worse scenario where even that would not be available.

Dr Marsh: Of course there was a bit of a wake up call in the 7 July bombings where the overloading of the mobile phones did show that a lot of people were relying on those systems working for purposes for which actually they should not have been relying upon them.

Chairman: Let us move on to ask questions about Computer Emergency Response Teams. Lord Mawson.

Q41 ***Lord Mawson:*** Is there a government CERT in the UK and how many incidences does it deal with from day to day?

Dr Marsh: There are a number of government CERTs. GovCertUK is the public sector CERT in the UK. That is housed within GCHQ. It works closely with the Centre for the Protection of National Infrastructure, law enforcement agencies and international CERT networks. Of course as the new Cyber Security Operation Centre stands up in Cheltenham it will work closely with that organisation too. There is also within the Centre for the Protection of National Infrastructure another CERT, CSIRTUK, which stands for the Combined Security Incident Response Team UK, and that advises the private sector on these events as well. Of course the MoD has its own CERT to look at defence networks and address the issues that arise there. All of those CERTs clearly communicate closely with each other and are also part of the broader CERT networks as well.

Q42 ***Lord Dear:*** Taking the subject of CERTs a stage further, there is a suggestion, I believe, from the EU Communication Group which envisages that National CERTs should be involved not only with the public network but with private as well. Do you think that is valuable, given the extension of breadth there? And what you are doing, if anything, about that?

Dr Marsh: It is certainly valuable that the CERTs communicate with the private sector as well as the public sector, and we already have that mechanism through CSIRT UK. We have not yet brought those together into one body and I think that we are not

necessarily convinced of the value of that either way. CERTs absolutely need to communicate and share information amongst themselves and with the community that they are serving; so in a sense they always have to operate in a federated environment.

Q43 ***Lord Dear:*** Linking public and private? Linking international and national.
Dr Marsh: All of the above. They have to share information really as widely as possible with as many partners who are engaged in the same sort of activity. They do that because the attacks are not constrained by national boundaries or by private or public sector boundaries; so the more broadly you can share information about attacks and vulnerabilities within a trusted environment the better prepared you are for when attacks come your way. So as well as the large CERTs and the private sector CERTs that are also operating in the UK, we have also been encouraging over the years the formation of what we are calling WARPs—Warning Advisory Reporting Points—which are very low costs CERTs, that small communities, perhaps in local government or a particular sector of industry or academia can set up themselves to serve a particular community and get the feed of information down from a larger CERT and tailor it then to what is most valuable for the community that that WARP is serving. So we absolutely need to offer that and, in a sense, there are so many of these different CERTs which are tailored to particular communities and activities that trying to bring together a national CERT does not necessarily seem to add a lot of value. It does not take away value either, but at the moment we have not felt the need to do that. We will keep it under review. If the European experience suggests that that it is a better model, then certainly we will be very happy to consider that.

Q44 ***Baroness Garden of Frognal:*** There are 16 other CERTs in the UK who are members of FIRST, which is the CERTs umbrella group, as we understand it. Can they be trusted? You have mentioned that they survive on trust, but can they be trusted and why and how do you monitor that?
Dr Marsh: FIRST is the Forum of Incident Response and Security Teams. It is a global community of CERTs; there are over 200 CERTs in that community, as you say, 16 in the UK. They have a well-defined and stringent membership process. They rely on CERTs being nominated to join. The CERTs then have to adhere to an operational framework. There is a site visit when the CERT is first accepted into the network, and so on. This framework also defines how the information that they receive can be handled and further disseminated. So I think that gives an additional initial level of trust, which is very important for getting into that community. Then, as that goes forward, the communities very much rely on continuing feedback about that trust. I think they see how people behave in other CERTs and they see how the information is handled. Of course, the big reputational risk, if you like, is that if any particular CERT were not to abide by that framework, not only does FIRST have the mandate to exclude them from the network but I think they would find it very hard to re-establish themselves as a CERT within any other shared body. There is a lot of peer pressure I think to behave properly. We are confident that, on the whole, they do that.
Chairman: We come towards the end. Let us turn to the European Network and Information Security Agency.

Q45 ***Lord Hodgson of Astley Abbotts:*** I think you touched on this before when you responded to Lord Mawson's question and you emphasised the relative slimness of resources of ENISA. Therefore, I think it would be helpful if you could give us your impressions of their work and whether they are going to be able to fulfil the duties and responsibilities that are imposed as part of this programme going forward.
Mr Smith: I declare an interest. I am the UK's board member for the agency and have been involved with it from day one, so I am very close to the agency. Yes, it is small; I think it is the second smallest in terms of staff numbers of all the European agencies. It has a relatively small budget by European agency standards; I think we are talking about €8 million for accommodation and staff costs. That does not actually leave a great deal of money for project activities. If I can go back to the origins of the agency, it was, if you like, a response to events and the surge in security activity following 9/11 and it was one of the flagship activities that we would increase our capability on network and information security. The idea started to emerge from around 2001–02 onwards. At that time, there was a great deal of hesitancy in the smaller community we had at that stage about the role of an agency in this field, and indeed I think those countries with large national security agencies, like the UK, France and Germany, were concerned that this agency did not confuse the relationship between local and central government and those national agencies so that they were not, if you like, receiving two kinds of advice. We did not want the agency to be operational in the sense that we would regard a CERT as an operational entity doing real time monitoring and offering real time advice. There was that kind of hesitancy at the outset which led to us looking for where it could add value, which we believed was as being an independent centre of excellence available in all of Europe and a networking hub so that it would bring together isolated pockets of expertise within Europe and create a kind of European body of thought on

individual subjects. For that reason, we initially saw it working in areas such as awareness rating where there were pockets of activity, particularly in Germany, the UK, Ireland and in a few other places, and they started to learn lessons from those awareness campaigns. Dr Marsh has referred to Get Safe OnLine, which I think is one of the leading awareness campaigns in Europe. They started to come up with best practice in this area. Similarly, with risk assessment and risk management they started to bring experts together to try and get a better understanding of risk management throughout Europe, and that is a very important activity. They also started to work alongside the European CERTs to see if there was anything they could do to create a better community of European CERTs and provide them with more standardised tools. I think we have been reasonably successful in that regard and they are very well regarded in the CERT community. Within a very narrow focus and with the limited resources, I think the agency has been a force for good. It has been bedevilled by problems, the problems that you would expect for a small agency in a remote location becoming established. It has taken a lot of time for the board members to deal with this but I think generally the agency is now at the point where there is a majority amongst the Member States that would want it to continue. At the moment, we are in this half-way house of having extended the mandate of the agency until 2012, and that was done purely for mechanical reasons, given the overlap with the review of the framework regulation governing the communication sector. Early next year, we are going to be looking seriously, when the Commission give us their ideas, about where to go next with ENISA. My feeling is, just reading the rumours, that we will see it more focused on network activities; it will be more clearly focused on supporting the protection of critical information, building on some of the activities that have already been pointed in its direction in the communication. That is just a feeling. You usually start to get indications from commissioners' speeches, but of course they are all a bit preoccupied at the moment, so we are not getting that kind of feedback. Just reading the signs from what we have seen and informed discussion, I think that will possibly be the next direction for ENISA. As a Member State, our view on agencies is that we want hard evidence for the need and for that budget to be spent. I think we were seen as a bit of a stick-in-the-mud in that regard and that the majority of Member States are already indicating that they are supportive of continuing with the agency. I think that discussion is due to take place from next year onwards. You asked if we thought it was capable of doing the work ascribed to it in the communication. Yes, I think we have already seen signs that it has started to accept that challenge.

Q46 ***Lord Mawson:*** Having built an IT network across this country, having an organisation that is small and focused it seems to me is a great opportunity because you do not want things big; you want them small. Also, do you really want them miles away from anywhere if their core business is about networking and bringing experts together. I just wonder whether really the very location of this organisation is an illustration of the conflict between an entrepreneurial industry and how it works and actually government and some of the systems in the public sector which are meant to protect us. This is partly why I am pushing this point about how do you really help the entrepreneurial skill set to come into the European Union if it is going to be the European Union in a way that is far more dynamic that can really reform the nature of this beast?

Mr Smith: May I take that contribution in two components? The smallness and the entrepreneurial nature of the agency: I only wish, my Lord, that you were writing the rules for the European agencies because they are bound by bureaucracy, which I think dates back to the 1950s French bureaucracy, and it is very difficult to move; every cheque has to be signed by five people. I am sorry, I am exaggerating slightly. We have struggled with this. Many of us on the board would like a much more flexible approach to the way the agency works, less hierarchical and models within the agency more project working, but we always bump up against the rule book. The good news is that we have had a change of Executive Director in the agency and as recently as yesterday I had indications that he is moving to a flatter management structure,. I think he is sending signals to the staff that they need to be more flexible in the way they work, so there are good signs. I would accept that we do not regard a big agency as a successful agency. There comes a point, given the administrative overheads, where you have to have a certain number of people just to do nothing. When the Commission asked for an analysis by an independent consultant, they said it is almost not worth having an agency of less than 100 people. I am not sure I totally agree with that but I think there is a kernel of truth in it, that you do need a certain size to have any kind of real momentum as a European agency. I suspect we might see a slight increase in resources made available to it going forward from 2012, but hopefully it will not become one of the mega agencies. Yes, I agree and as a member of the board I continue to grow an entrepreneurial spirit and direct contact with business. The location is a very sensitive question. I pick my words very carefully. The agency came at the end of a big log-jam of agencies that did not have homes. It was called the "agency package" and they all sat in Brussels waiting to be housed. ENISA came towards the back of that queue. The geometry on finding homes for all these agencies was something that only two or three people

in the UK understood. As we approached enlargement, it suddenly became crucial that we solve this problem. It was solved very quickly and no-one expected Greece to be given ENISA, but it was as part of this deal for housing the agencies. It was a surprise to everyone when ENISA was given to Greece and the terms under which it was given were that Greece would decide the location of the agency. It chose to locate in Crete and that was the decision of the Greek Government and I have no reason to challenge that decision. The report that the Commission asked for from IDC consultants said that there were difficulties with the location in terms of attracting good staff and the very issue of travel to and from northern Europe to which you have referred. On the management board, that is something we can only see as a challenge; we cannot question the location of the agency. I think it would be a political decision taken at the highest level to try and seek a new location for the agency. The Greek Government regarded that report by IDC Consultants as anathema, an insult to their nation, so you can see why I am treading sensitively around this issue. Yes, the location does have its challenges.

Q47 ***Chairman:*** On that last point, perhaps for the record you would just elaborate why Crete is such an awkward place to have it?

Mr Smith: It is quite easy to get to in the summer but very difficult to get to the rest of the year. You have to change planes in Athens; there is usually several hours' wait, and then Crete in the winter has problems with cross winds at the airport; flights are cancelled and I have seen a lot of Athens Airport over the last few years. It is not that easy to get to but it is a lovely place.

Chairman: Thank you very much. We have already been made aware of this problem and I think that is an issue which this committee will pay a good deal of attention to in putting together its report, but I must not pre-empt that. There are no further questions. That brings us to the end of this session. Thank you both very much for coming. I think we have had a splendid morning. You have been very clear and we are most grateful to you. I know you have come at relatively short notice and for that too we are most grateful. You have certainly given us a great deal to think about.

Supplementary memorandum from the Department of Business, Innovation and Skills

Exercise White Noise

1. In oral evidence, Geoff Smith of BIS referred to an exercise on the response to a major telecoms failure. He offered to provide more information after the conclusion of the exercise.

2. Exercise White Noise took place on 11–12 November 2009. It tested the UK Government's strategic response to a widespread failure of the UK telecommunications system, lasting for a number of days. The exercise was part of an ongoing programme of UK civil contingencies exercises that rehearse and thereby improve the efficiency of the UK response to a range of emergency scenarios.

3. The exercise did not involve any real impacts on the networks and was delivered via simulation. In every other respect the exercise was played as realistically as possible between the teams taking part.

4. Exercise White Noise was a Tier 1 exercise (that is one of the series of major exercises that involve Ministers as players) involving activation of the Civil Contingencies Committee (CCC) and the COBR facility. The following departments participated fully in the exercise: BIS, Cabinet Office, DCLG, DECC, DEFRA, DH, DfT, FCO, HO, MoD and MoJ. The Welsh Assembly Government, Scottish Government, OFCOM, CPNI and Government Offices for the East Midlands, North East and South East also took part.

5. An important aim of the exercise was to test the information flow between government and the telecoms industry during an emergency. The following companies took part in both the planning and execution of exercise White Noise: Airwave, BT, Cable & Wireless, Global Crossing, Kingston Communications, Telefnica O_2 UK, Orange, Vodafone, Virgin Media and Verizon. Overall, including both government and industry, more than 250 people took part in the exercise.

6. The exercise scenario focussed on the consequences of a widespread failure of the UK Public Switched Telephone Network (PSTN). The (hypothetical) failure was introduced through an unspecified technical error by a foreign operator with a connection to the UK. The effect of the failure was that all fixed line and mobile operators in the UK lost the ability to connect calls both within their own networks and between each other's systems. The failure took place during the morning of the first day of the exercise; by 13:00 no voice telephony, either fixed line or mobile, was possible within the UK for the rest of the exercise unless it was over either a private wire/network or Voice Over Internet Protocol (VOIP) telephony system.

7. The simulated fault meant that the internet and other forms of Internet Protocol communication (eg email and VOIP) were possible; however fax, dial-up internet, mobile phones (including mobile data), international connections and access to the 999 service all failed under this scenario. The focus of the exercise for government (and specifically BIS as Lead Government Department for telecoms) was to mitigate the effects of the failure on UK citizens, while ensuring that the telecoms networks were restored to normal operation as quickly as possible.

8. During an incident of this type, telecoms operators need to isolate their systems from each other in order to correct the fault and re-establish their ability to carry traffic over their networks. The UK's telecoms network is in fact a complex set of interlinking networks, all owned by private companies. The interconnections and the flow of traffic between networks are determined by commercial contracts between individual telecoms companies. This makes establishing priorities for reconnection and co-ordination between the telecoms operators and government following a major incident complex. This process was the focus of play in the afternoon of day one and through day two.

9. The exercise was a success, as judged by both the participants (over 95% of whom stated in the post-exercise survey stated that they had learned from the exercise) and by Exercise Control and BIS as Lead Government Department. Some key areas where the response could be improved were identified by the exercise. These are being reviewed and action through the coming year will be taken to address the issues identified.

December 2009

WEDNESDAY 25 NOVEMBER 2009

Present: Garden of Frognal, B; Hannay of Chiswick, L; Harrison, L; Hodgson of Astley Abbotts, L; Jopling, L (Chairman); Mawson, L; Richard, L

Examination of Witnesses

Witnesses: MR CHRIS GIBSON, Chief Finance Officer, Forum for Incident Response and Security Teams (FIRST) and MR ANDREW CORMACK, Chief Regulatory Adviser, JANET (UK), examined.

Q48 ***Chairman:*** Can I say to our two witnesses, Mr Cormack and Mr Gibson, welcome. It is very good of you to come, we very much appreciate it. As you know we are in the early stages of our inquiry on protecting Europe from large-scale cyber-attacks and we are very much looking forward to hearing what you are going to say to us. Perhaps you would like to begin by introducing yourselves if you would because we have just been asking ourselves what JANET means and also FIRST which we have had explained to us. It might be helpful for the record if you would introduce yourselves please. Mr Gibson.

Mr Gibson: Thank you very much for inviting me to come here; I am very glad to come here, it is certainly very interesting. Chris Gibson; I am the Chief Financial Officer of FIRST which is the Forum of Incident Response and Security Teams. FIRST is very much a forum, I would emphasise that fact, there is no standard FIRST view on things, it is very much a grouping of teams, people very disparate in multiple communities, multiple constituencies. I have been the finance officer for a number of years now; I have been involved with FIRST for 10 years and I would like to hope that I could bring something to the table in terms of the general view but it cannot really be said to be the FIRST official view. I work for a large multinational bank, that is my day job, but this is something that we as a bank are a member of, we have been in there for a number of years and we think it is extremely valuable for the incident response community to bring people together, to talk about incident response and so on, so that is what we do. We are a US non-profit organisation, we have very much educational outreach, bringing incident response teams together and making the Internet a safer place is our watchword.

Q49 ***Chairman:*** Thank you. Mr Cormack.

Mr Cormack: Andrew Cormack. JANET was originally the Joint Academic Network. We are the UK's education network and we connect all universities, colleges, regional schools networks and research organisations together and to the Internet. As far as they are concerned we are the Internet so we are a large computer network and, depending on how you count potential users, our marketing people have recently suggested up to 16 million people in the UK use JANET either as school pupils, as students, as teachers or as researchers. Most of them are probably unaware that we exist because they will see their school, college, university network, but the way that those organisational networks are connected together and to each other is us. We are probably, in terms of infrastructure, equivalent to large corporate organisations, telcos, and the capacity of our backbone is equivalent to any of the national telcos, it is a very large network. I have worked there for just over 10 years. For the first three and a half of that I ran the incident response team for the network so we as an incident response team were members of FIRST and in fact we still are. Since then I have moved into more of a policy regulatory role (as indicated by the job title) but I am still very much involved in international incident response discussions. I was invited to become a personal member of FIRST after I had ceased to be a member as part of the team. Also, at the request of the European incident response teams, I have offered to be a member of the permanent stakeholders group with ENISA and I have been doing that for five years now. I am also a member of the TERENA European incident response group. The other relevant thing probably is that for the first year when I worked for JANET we operated a pilot of a pan-European incident response team for research and educational networks to find out how effective that was. Possibly the fact that the pilot only lasted a year after I joined it indicates how successful it was. Unfortunately we could not get sufficient agreement on what such a team should do to justify continuing funding for it, but it was an interesting experiment and the lessons were useful.

Q50 ***Chairman:*** Thank you very much indeed. You both realise that this is a Sub-Committee of the European Union Select Committee and a number of us are members of that umbrella committee as well, and that means that all the activities of that Select Committee and the Sub-Committees are involved

with European Union affairs. To what extent do you believe that Internet resilience is an appropriate topic for the European Union to tackle and get involved with?
Mr Gibson: I believe it is certainly of value. I certainly believe that the European Union has a role in expediting and jump-starting, so to speak, incident response teams, but I am not sure that I would agree that a pan-European response team is the way to go. Our experience has taught us that that is not the way to go but in terms of getting teams to start building a structure, helping incident response teams to build the relationships and make the Internet a safer place, absolutely I agree.
Mr Cormack: Internet resilience is not something that any country can do on its own. The idea of the UK Internet is technically meaningless, we are so intertwined with other countries' networks through large companies, through telcos, just through the way that networks happen to be connected. Incident response eventually is something that will need to be done globally in terms of teams globally working together to fix problems. One thing we have found is that regional activities are actually a very good place to discover good practice. There are very simple pragmatic things like it is quite easy to have a meeting of European CERTs, we are all within a couple of hours flight, we are all within two time zones—plus Iceland which is in another time zone—and what has happened over the past four or five years is that there is a European CERT activity, there is an Asia-Pacific CERT activity, there are some joint activities in the States. Each of those is focusing on particular issues of interest to them and the other regions can then learn a lot from those. We have done a lot in Europe on training which Asia-Pacific and South America through FIRST are picking up on; Asia-Pacific have done quite a lot on exercises, particularly around the Olympics, and they are passing that information on to us so it is a good way to try out ideas to find out what works.

Q51 ***Lord Hannay of Chiswick:*** Could you perhaps just say a few words about your one year's experience of getting involved at the European level which did not justify continuation of funding. What were the problems that you hit and were they problems back then or are there still problems going forward? If you could just say a few things on that it would help.
Mr Cormack: They are continuing issues. We were looking only at the research and education networks which were a handful of networks that contributed to the pilot—I cannot remember the exact number, but fewer than 10. What the pilot ended up doing was we had a desk where any national research network could send incidents or parts of incidents that it did not want to handle, that were outside its constituency. That gets less useful as teams grow and develop because they will develop their own direct connections, their direct relations with other teams in other countries, in other areas and actually inserting a third party slows things down and increases the risk of miscommunication and things like that. Once you can establish a mesh of trusted peers that is a more effective way to deal with problems. The pilot was quite good for establishing that trust because gradually the members of the pilot got to know each other better. They tended to develop at different speeds, so JANET has had a CERT since 1984. Even then we had been in existence for 15 years; we were pretty well established and we were really just passing incidents on to the room next door as it happened, to have them dealt with through their workload. Other countries were interested in whether a pan-European team could provide them with out-of-hours cover because that was something they wanted; we were English and Croatian-speaking as it happened and we could not provide out-of-hours cover or first line support for a Spanish network in Spanish and to cover all the nationalities with a level of knowledge and understanding of their communities that you need would not have been feasible, and there would not have been much interest by other countries in funding that. At the time it was a difference of expectations, plus this fact that actually there is a better way of doing it which we did look into.

Q52 ***Lord Richard:*** I am simply wondering whether "resilience" is a term of art or does it mean what we all think it means?
Mr Cormack: I would say that most people understand the same thing by it until they actually want to sit down and define it, at which point there are a lot of variations.

Q53 ***Lord Richard:*** What do you mean by it?
Mr Cormack: I would mean by it the ability to not fail catastrophically under an incident, under attack, under natural disaster. A resilience network can degrade but it should do so in a relatively benign fashion.

Q54 ***Lord Richard:*** Capacity to resist.
Mr Cormack: Capacity to resist.

Q55 ***Lord Richard:*** And survive.
Mr Cormack: Yes, but those who demand that resilience means that an attack on a network is completely invisible to its users are setting too high a barrier and I do not believe we can do that.

Q56 ***Lord Hodgson of Astley Abbotts:*** My Lord Chairman, I wonder if it might be helpful if I took question 7 here because we are onto the local or global straightaway and we are in danger of re-ploughing the field a bit later. My question is about

local and global and whether drawing up plans at an EU level makes any sense—which you have been partially answering—or whether we should be immediately involving the USA or Russia and others. We have had some interesting evidence from the Chairman of the Board at Arbor Networks in which he says that none of the Internet's problems respects national boundaries and talks about the need for international co-ordination. "Such teams need to be allowed to freely communicate with their peers in foreign countries. At present, barriers exist between allies that prevent information sharing at the pace that is needed, of the order of minutes and not weeks." Could you say a bit more about that and the global local issue and what are the barriers that are preventing collaboration and, indeed, is such collaboration a good idea?

Mr Gibson: I personally believe that collaboration is very much what FIRST was set up to do and that is what we have always aimed for, we have brought in teams from China, from Russia, from South America, North America, India et cetera to bring them together to enable them to build those relationships. As a member of a large bank when phishing first started hitting us we would ring up people in China and get absolutely nowhere because we would be talking to an ISP in China, the wrong time zone et cetera, et cetera. Once I had met people through FIRST who worked for the Chinese team and I had shaken their hand and bought them a beer I was able to get a very fast direct line on something and get things done, whereas going the official route—I could talk to the NHTCU for law enforcement or I could get my US counterparts to talk to the FBI and it percolates across. It just takes too long, it is very bureaucratic and my personal view is that that personal interface, the fact that I have met them and talked to them and so on is absolutely crucial. That is where I am very loathe to look at things like formally saying it is a European problem, you have to go this route, through a European group, across the water to an American group, down the chain there, I do not think it works, especially for an international bank. We are in 100 countries and the thought of having to channel an incident in Europe this way and an incident in America that way just does not fly, it would not work.

Q57 ***Lord Hodgson of Astley Abbotts:*** The barriers that you think are being referred to in this paper are bureaucratic barriers.

Mr Gibson: I believe so, yes.

Q58 ***Lord Hodgson of Astley Abbotts:*** Not legal barriers, just organisational obstruction.

Mr Gibson: I think so, that is my gut feeling.

Chairman: Lord Hodgson, you will have the opportunity on 9 December of pursuing this further because Arbor Networks are coming in to give evidence to us at that time. Lord Mawson?

Q59 ***Lord Mawson:*** Thank you, my Lord Chairman. What does a CERT have to do and could you give us some practical examples?

Mr Gibson: It very much depends on your constituency. The CERT that I belong to in my day job so to speak is a bank. We look after any kind of information incident within the bank and that could include faxes being sent to the wrong fax number, which in Japan is an issue because of the privacy laws. It can involve someone trying to hack into our network, it can involve someone internally trying to break into systems, it can be a multitude of things and we encompass that under SIRT (Security Incident Response Team). We call it that rather than a Computer Emergency Response Team because we try and cover all of the information leakage issues through that—such as someone putting people's personal data in a folder and dropping it in the trash can outside the office because they cannot be bothered to shred it and so on. We try and encompass everything. To us any incident is a very serious incident, we are a bank and we have, obviously, a vast amount of electronic information and any incident, anyone breaking in or any information leaving our business is remarkably serious and gets escalated a long way up our management chain very quickly. That can be very different to, say, a university network. We own the computers on our network, we control them, we can make sure they are patched et cetera et cetera; in a university you have a crowd of people turning up with their own computers that may be patched, may not be patched, it is a very different ballgame, so to try and say a CERT is this and neatly encompass that in a three line sentence is a very difficult thing to do.

Mr Cormack: I accept that. I was trying to generalise, knowing that I was going to be sitting alongside Chris who has actually got a very nice example of the breadth because JANET's CERT sits in the network operator. We have no ability to see individual machines—the laptop that is sitting in my bag will be within the constituency of JANET's service at the moment but they have no authority over it, unlike Chris who I imagine can seize any machine, shut them down, kick them off, do what they like. I think the general thing that a CERT does is it receives reports of incidents, it then understands what is actually going on to the best of its ability and it then passes on relevant information to the people who can make the incident happen. That is the only standard thing.

Mr Gibson: Within the context of its organisation I suppose.

Mr Cormack: The organisation—or the constituency tends to be the term that is used in FIRST—may be a single company, it may be customers of a network like ours, it may be users of the product. Cisco have a CERT for users of Cisco products so they have even less control over what their users do, but if their users do not respond to a vulnerability Cisco is one of the major providers of equipment that makes the Internet work so there is a strong incentive for Cisco to try and make sure that their customers do respond to warnings, respond to events and incidents, even though they have no formal ability to say "do this" at all. There is a lot of variation, therefore, in the amount of control you have and the amount of visibility you have. We would contact a security contact at each university and say "We have had a report, it looks like this sort of incident, please can you fix it?"

Q60 ***Lord Mawson:*** I am just trying to understand exactly how JANET works; is JANET connected in a diagram a bit like petals so that you control the core bit and then there are different petals connected to it? Is that how it looks?
Mr Cormack: I think you have seen one of our network diagrams by that description. We actually control the petals in that we have 13 or 14 regional networks that, under contract to us, deliver service to our customers who actually do not connect to the core network that we run, so those are the petals. Contractually therefore we control them. The universities and colleges will then connect off those petal networks.

Q61 ***Lord Mawson:*** My experience of IT networks is that the technology is one thing but the personal relationships are really, really important.
Mr Cormack: Yes.

Q62 ***Lord Mawson:*** It is just a tool and I am just wondering how you facilitate the coming together of the key people so that actually the human interaction is happening as well as the technology?
Mr Cormack: Down to customer sites, when a site connects to JANET they are required to provide a number of contacts; one of them is the security contact and it can be a role, it does not have to be a single individual, though we like to know the names of the people who do it precisely because it is a human interaction, it is not an interaction between roles or mailboxes or whatever. We run various events where we get to know them; I was up in Glasgow running a training course yesterday with people who are site security contacts, so we try to get to know them so that if we phone up and say "You have a problem at your site" they recognise our voice. It is very simple, they know it is JANET CERT phoning and not somebody trying to make them do something stupid. That is part of the establishment of a trust, a recognition, so that we can immediately get on to actually fixing the problem rather than going through some of the bureaucratic process that was mentioned which is who are you, what authority do you have. It also works on the international level. One of the things that really impressed the UK Government when they started getting involved within the international CERT community, there was an incident where machines on JANET and on DFN, the German research network, were attacking the university in Bosnia with a level of traffic that took Bosnia off the internet. Because the Bosnian traffic was routed through Slovenia it was causing Slovenia considerable distress as well. The head of the Slovenian CERT—I think they were members of FIRST at the time; we certainly knew we had met them—could just get on the phone to me as the head of JANET CERT and the head of DFN CERT and say "There is no legitimate traffic from your network coming to the University of Tuzla". I could phone my network operations team and say "Please block all traffic from us to that address" and the attack was stopped within five minutes. That is the sort of thing that a bureaucratic process really just cannot do in that timescale.

Q63 ***Lord Richard:*** You are in effect an academic CERT to a certain extent and you are a banking CERT.
Mr Gibson: I am.

Q64 ***Lord Richard:*** But they are teams as I understand; how many have you got in each team?
Mr Cormack: In ours for the network we have nine posts at the moment.

Q65 ***Lord Richard:*** That is in the CERT.
Mr Cormack: Yes.
Mr Gibson: We have a model where we have a team of seven or eight people in New York who essentially manage incidents and they are the central point, all incidents are reported to them. They can then call out—they have a daily call, we go through all of the incidents that have come in in the last 24 hours. If they are of a certain severity then we will be on a call within an hour or two hours or three hours—as soon as it is reported we will take a view like this one is serious, we need to do something now, otherwise they are reviewed daily. We can invite people onto that call, the subject matter experts internally, so if it is a network issue we will call in the network folks, so the core team is about seven or eight people in New York.

Q66 ***Lord Richard:*** How many here?
Mr Gibson: I am part of that team as a subject matter expert for forensics, but the official team is seven or eight people in New York. They are on 24-hour call,

we can get them day or night, but we have always tried to do that so that we have got one place that we know where everything is going on. We have had incidents in the past where something has been reported up this chain, it will hop through senior management and come down the line in New York. They wanted to know what was going on and the right people had not actually been informed at that moment, so we spent a great deal of time mandating this—you know, we wanted to go into one central point in New York, that 24 by 7 group you can call them day or night on their mobile phones and they will immediately react. If that means escalating it or actually taking action, that is not a problem, it happens.

Q67 ***Lord Richard:*** I am just trying to see how it works. Something happens at a bank in Britain, whatever it is, and that starts alarm bells ringing. It then goes to New York and it comes back from New York to you.
Mr Gibson: Depending on the issue. As I say, I do the computer forensics, that is what my team does for the bank. If it is a networking issue they may call out to someone else in London but from New York the folks there can essentially call the right people and get the right things done anyway. If it means taking a computer off the air and literally disconnecting it from the network electronically, they can do that from New York anyway.

Q68 ***Lord Richard:*** Is that the same with JANET? You have not got people in New York, I understand that, but is there some central body which then passes it back down?
Mr Cormack: Not really because our equivalent to Chris's countries or banks are universities and colleges so we have a central team of eight or nine people in Oxfordshire who will function like Chris's team in New York. One other difference is that I guess you have mandatory reporting.
Mr Gibson: Absolutely.
Mr Cormack: Any member of staff in a bank who discovers a problem must report it to the bank CERT whereas in JANET we exist as a service to the community. If the community wants help, if any member of the constituency wants help, they can come to us. So we have no mandatory reporting, but some universities may have their own internal teams. I should say that a team does not have to be as big as that, it can be very effective. A CERT is a process and needs enough people to run that process according to its desired service level, so there are some universities who will have one fulltime CERT person and two or three others, and part of their job is to help there, and they can be highly effective. Those would be sort of equivalent to Chris's branches and we would pass on reports to the relevant customer organisation.

Q69 ***Lord Mawson:*** My second question is why can CERTs be trusted and should the Government be getting involved to make sure they stay trusted? Is not the danger that this is a lot about relationships and is there not a real danger that the Government will try to turn it into the usual systems and processes which are absolutely alien to what a network is and they will frankly undermine what this is all about? Is there not a real tension here?
Mr Cormack: There is a tension but I do not think it necessarily is a bad idea. There are three ways in which trust is established. You mentioned person to person which is probably the foundation of everything. More recently there have been two different ways of establishing organisational trust; one is by simple declaration—JANET CERT is the CERT for JANET says the network operator, or CERT/FI is the CERT for Finland says the Finnish equivalent of Ofcom, so there is a sort of declarational, this is the responsible body. The third one I think of as expectation of delivery, so if somebody pops up and says "Hello, I am the CERT for such-and-such a network or country", if I have an incident with them that does not involve too much private information on my side I will send it to them. If having sent it to them does not make things worse and makes things a bit better then I may send them more and you slowly build up something according to my expectations of what a CERT does. That is another way that it can be established. In the past three or four years there have been some attempts to codify that into best practice and there is a CERT maturity model being worked on which looks at relationships, funding, technical skills and position in the organisation is the fourth, so there are attempts to formalise "We are a CERT, we are capable of behaving like a CERT". I glad you said Government coming in and messing things up so I do not have to. That could happen; however, we have a feeling for the number of internet addresses in Europe and the proportion of those that are covered by a CERT—or ISPs tend to have things that they call abuse teams which are more used to handling bulk incidents—is still only about 25% of European IP addresses that have a CERT or an abuse team sitting somewhere above them. There is, therefore, definitely a role for Government, European bodies, anyone, please, to try and help fill in those blanks on the map, the 75% of IP addresses which, when I get an incident from them, I can do nothing about because I have no trusted contact. I am trying to encourage the UK Government to use the phrase "CERT of last resort" which does not sound as grand as national CERT but if you cannot find anybody else in the UK, ask us. There is a definite role there; there is a role in encouraging other sectors to develop their own teams, there is a role in putting teams together, there are organisational roles but there is less in an

operational role because, as you say, it is a third party in a communication that maybe does not need to be there and may impose more bureaucracy than is needed.
Mr Gibson: We would very much like to see governments pushing "You should have a CERT" both for ISPs and for organisations because they are extremely valuable. Whether they get involved in the communications with them is another question but we would very much like to see more CERTs.

Q70 ***Baroness Garden of Frognal:*** Just following on from Lord Mawson's question is there any sort of person specification for the individuals who work in CERTs and is there any vetting procedure?
Mr Gibson: To join FIRST, for instance, for a team to join they have to provide various pieces of information. They have to be sponsored by two existing members, there is a site visit, there is a document to go through where they look at terms of reference, is this genuinely a CERT, does it have a charter from its organisation to do the right things or is it one person pretending to do something they cannot, so it is very much sponsoring—do you know these people, do you trust them to join the organisation?

Q71 ***Baroness Garden of Frognal:*** Is that knowing the individuals or knowing the organisation?
Mr Gibson: Both I would say. There is a site visit, one of the two sponsors should visit the site and talk with the people and get to know them, and by sponsoring them they are essentially saying to the rest of the organisation "I know these people, they are good people, they should be members of FIRST", so very much so. As FIRST has grown bigger and bigger that has become somewhat harder. Back in the old days there were 16 members, everybody knew everybody, you all knew each other by your first names and life was very easy; on the other hand you were only 16 teams and covering a tiny percentage of the Internet. Now we are 200 plus teams, we are covering a bigger proportion but that level of personal trust is harder because you do not know everybody. That is one of the reasons why we put on regional and global meetings every year, to get people together, to get them talking, to present, to learn about each other and to meet each other but that personal trust is harder and you have to work at it, but it is certainly doable.

Q72 ***Lord Hannay of Chiswick:*** Following up the same line of questioning is there even a theoretical possibility that a CERT could be taken over or established for criminal purposes and that this would escape the notice of other CERTs? If so, what would be the possible implications of that?
Mr Cormack: I think it would be detected fairly quickly by my test of when I send them information does it do good or does it do harm? They would have to make sure that they were visibly still doing good while covertly doing harm elsewhere.

Q73 ***Lord Hannay of Chiswick:*** My assumption would be that if they were a successful criminal organisation they would obviously have a cover, i.e. they would do some good in order to prevent you immediately discovering that they were there for negative purposes. I just wonder whether you could explore this thought because it is relevant to the issue about whether governments should be in any way involved at any stage because clearly it is governments who basically take legal action against people who transgress within their jurisdiction.
Mr Gibson: I should have added actually that when the two sponsoring teams put the membership forward for a new team it is then sent to our entire membership who effectively have the ability to blackball that applying team. It has rarely happened, I can think of only one case recently that I am aware of and certainly should someone start suspecting a team that would very soon become known. Some of our teams have very, very wide contacts and spend a great deal of time doing this, and if they sent something and action was not taken it would very swiftly become known. We have the ability to revoke their membership, certainly, but it has not happened to my knowledge. Given that CERT teams are reactive, if they do not react then you take a view on why they are not reacting. If that is because you believe they are doing something nefarious that would soon become known and they would essentially be blackballed through the network. One other point is that FIRST builds these personal relationships so if I have an incident I do not send it to the whole of FIRST, I will use the contacts I have made through FIRST to send it to the right people so bad teams would not be picking up information I was sending out so to speak because I probably would not be sending it to them. If I did send them something it would be specific to their network and if they did not fix it then I would start suspecting their motives and integrity.

Q74 ***Lord Harrison:*** Is there anything useful we can learn from the recent instance you pointed to where, in effect, a CERT was blackballed by the rest of the community?
Mr Cormack: There are confidentiality agreements.
Mr Gibson: Yes, as part of FIRST membership.
Mr Cormack: The issues that were raised were both over the past history of individuals involved in the team and that people were doing things in there outside their day job that were felt to raise questions. That has happened actually on a few occasions, that

teams have got informal suggestions that they might like to encourage their staff not to get involved in certain activities in the evenings, plus a feeling that they were not fully committed to making things better which is the formulation—there is an expectation that you will not do harm, you will actually do good, and for the team that was refused membership it was not a single veto, it was a general thing, quite a lot of people had concerns so it appeared in that case that the personal networks were working quite well.

Q75 ***Lord Hodgson of Astley Abbotts:*** We had an inquiry into money laundering and, during that, we received evidence that in certain cases law enforcement agencies were part of the problem not part of the solution. Has this issue arisen in your area, that is to say there are jurisdictions where perhaps there are activities which cut across your wish to keep the party clean?
Mr Cormack: Let me take it from the other end. If you are a customer of JANET CERT I hope that people who report to us know that things go to JANET CERT, they do not go to JANET the company. When I was running the CERT I told the chief executive of the company "That is not your business, that is confidential information." There are other organisations in other countries that are members of FIRST where I would not have that certainty, I would expect that information I sent to the incident response team, Chris's group of seven people, would also be coming to the attention of higher authorities within that organisation or within that company, just as a matter of corporate, national or regional culture.

Q76 ***Lord Richard:*** I am getting a bit lost, my Lord Chairman, and I hope you can put me back on the right track. You are the banking CERT and you are the academic CERT, you have talked to each other but how? Is there some sort of central organisation into which all the CERTs link in?
Mr Gibson: FIRST has a mailing list, it has various websites and you can talk in a number of ways, and we see that as part of our role, to facilitate those conversations, but I know Andrew because I have met him many times and if I need to talk to Andrew I will pick up the phone and talk to Andrew, there is no requirement for that to go via FIRST, FIRST has served its function in bringing us together and building that relationship.

Q77 ***Lord Richard:*** Each CERT in effect acts for its own organisation or business or whatever you call it.
Mr Gibson: Constituency.

Q78 ***Lord Richard:*** And acts independently from all the others unless you want to pick up the phone or send an email or whatever.
Mr Gibson: It would depend on the information. If we see something happening that we think is Andrew's systems attacking our systems type of thing, we may put that across the mailing list and say "We are being attacked, we are not sure from where, can anybody help us?" so we would use the FIRST network there, but if I have identified it as Andrew's—

Q79 ***Lord Richard:*** There is no central clearing house.
Mr Gibson: No.

Q80 ***Lord Richard:*** Do you think there should be?
Mr Gibson: Some of the privacy issues would just cause nightmares. Some of the EU pieces where IP addresses would perhaps be considered personal information have always been an issue for us. Our banking CERT covers over 100 countries: trying to nail that down would be ghastly and trying to formalise that and sending it to a very global list may not be the right thing to do.

Q81 ***Lord Richard:*** But you have a clearing house in New York.
Mr Gibson: We have in New York, yes.

Q82 ***Lord Richard:*** And you are the clearing house for the academic community.
Mr Cormack: If they want to use us. There is also a distinction between personal contacts and organisational contacts because every team will have an official contact email and contact phone number and they will have some level of service on that, whether it is nine to five or 24/7. So I can either report something to Chris if it is a general enquiry of are you interested to know that—maybe our users have reported that they have emails trying to phish their credentials for Chris's bank—or I can formally report it from my CERT to his CERT.

Q83 ***Chairman:*** Can I just come in here because is there not a problem which could arise because information about vulnerabilities could be shared and become available to undesirable people? Is it not the case that if Cisco pre-announces a problem so that CERTs can react there is a serious problem with that?
Mr Cormack: The general feeling is that the malicious people know about the problems already and in general our problem is not knowledge of vulnerabilities, it is getting people to act to fix them. Certainly Microsoft announce vulnerabilities on the second Tuesday of every month and it is widely understood that the day that that information is released a large number of people start trying to reverse engineer to work out what the vulnerability actually was, because all Microsoft will give you is "Here is the code you need to fix it" but it is possible

to work it out from which programme that is changing, which routine within that programme, you can start drilling down to workout what the vulnerability actually was, and it seems pretty widely understood that that happens in the malicious community. The vendors are converging on the idea that there has been a lot of variation between them as to how they treat vulnerabilities, but they are coming towards the idea that actually there is no point publishing information before there is a fix, that just frightens people, that they can do nothing about it, but once you can offer a practical way of fixing a problem then the balance of interest is in spreading that information as widely as possible. Microsoft have 200,000 on their mailing list for notification of alerts plus every Microsoft system by default will call in and say are there any updates and get that information out. Certainly Microsoft boxes run by malicious people will also go and fetch those updates but the balance of the world's good is now felt to be once you have a fix, get that information out as soon as possible. Until you have a fix you try and keep things as confidential as possible and what seems to happen is that as Chris described, building teams with the skills to look at a particular incident, there seems to be a process of building teams to look at a particular vulnerability if there is a vulnerability that affects multiple products. You might find a general vulnerability in a protocol and every system that implements that protocol is likely to have the vulnerability so you then need somebody to co-ordinate at what point do we decide that we have fixes for 50, 60, 75% of them and the balance of interest is now to get those systems fixed even though that could increase the exposure to risk of the others for which fixes are not yet available. There are half a dozen teams worldwide, I think, who do that sort of co-ordination. JP/CERT do it in Japan, the Finnish CERT did a lot, CERT/CC in Pittsburgh—that is probably it.

Q84 ***Baroness Garden of Frognal:*** The EU communication envisages "National" CERTs which cover more than just public sector infrastructures. Do you see this as a valuable sort of institution to create and how does it compare with the UK's approach of multiple CERTs?
Mr Gibson: Andrew's phrase of a "CERT of last resort" covered that quite well. If I have an incident within my organisation in the UK realistically I need to co-ordinate that within my organisation and I may not want to talk to the UK one and multiple other national CERTs that may be involved because that is going to complicate matters. However, there is a problem here, there is no CERT team, who can I call? That is a very valuable idea, so I am all for CERTs but I do not think it should be mandated that every incident I have within my organisation in the UK has to go through that CERT because that is just not going to work. Obviously there are regulatory reporting requirements and so on and so forth and if it is in a number of countries then I am reporting into multiple CERTs and just complicating everything. Obviously if we need the assistance we will call it and our regulatory requirements will require us possibly to report into the New York Fed and so on and so forth, but I cannot see the logic of reporting it to 26 different national CERTs because it happened to be in 26 countries.
Mr Cormack: There is also a very valuable role that is still being performed by CPNI as they are now, which is having meetings of UK CERTs. They have a UK CERTs group and there are a few FIRST member teams within the UK so they are getting those together in a room to discuss in a reasonably confidential forum new discoveries, new incidents, new ways of tackling incidents, ideas about co-ordination, creating that sort of trusted forum. CPNI now call them information exchanges and there are things in the States called ISACs which are somewhat similar—Information Sharing Advisory Centres—but the co-ordination of it is good. It is not about dealing with individual incidents, it is getting people to know each other, to share good practice, to share ideas, to bounce ideas off each other. It is very useful.

Q85 ***Baroness Garden of Frognal:*** You are focusing again on real meetings with real people going to places rather than virtual meetings.
Mr Cormack: I am getting less hung up about technology. There is an additional value once in a while to getting people together in a room but FIRST works pretty well when we meet once a year face to face and the communications in between do tend to reference back to the last time we met. The call may well be about an incident but it may well start with a "Do you remember the conference dinner in Kyoto?"
Mr Gibson: If I have an issue in a country where I do not know the team I may know someone in another team there who may know someone in that team, so you have that extended level of trust that you have from past encounters.

Q86 ***Lord Mawson:*** What you are saying is to emphasise the point that it is the building of networks and relationships, making it easier for people to meet as part of the process, so I presume the last thing you want is a facility on a remote island somewhere that is meant to be responsible for some of that.
Mr Cormack: I assume you have a particular remote island in mind. It is not that hard to get to, I go there once or twice a year as well. I do not think you have to meet very often and most of the work I guess it would be fair to say is done by electronic communications, in which case it does not matter

where you are. The face to face stuff is getting to know people as people rather than as job titles.

Lord Mawson: Having built a network in my experience that face to face stuff as you describe it was really critical, not all the time but having those moments when people could come together and understand each other and then they used the tool of communication—it was that inter-relationship. Certainly when we began to develop the network we thought it was just the technology but we soon discovered that actually it was not.

Q87 ***Lord Hodgson of Astley Abbotts:*** This is about systemic risk. The evidence we have received suggests that on the one hand we should pull it all together and try and guard the whole thing or on the other push it all apart and make it safer that way. Could you give us your views on that and also in that sense whether botnets or a natural disaster or a cyber-war attack could bring down the Internet, or does the present diverse structure mean that it is safe from that sort of destructive, systemic difficulty?

Mr Cormack: I am not sure what bringing down the Internet would look like. Certainly I would be confident that a botnet could take any university off our network. I did a back of an envelope calculation on sizes of attack a couple of years ago and came to the conclusion that by the time a botnet was big enough to break JANET's external connections then the networks that were bringing traffic to us would have their own problems that they would be motivated to fix. I am pretty sure you could take off a single organisation, possibly a single class of organisation if they were too tightly coupled, if there was too much of a central point. The Internet is such a diverse network or networks that I do not know. More likely—I was watching the news this morning and watching pictures of the flooding in Cumbria; there was a little throwaway line about that bridge that is going to have to be taken down contains communication cables and I thought ah, does that include ours? I cannot remember and I have not checked back to base. In fact the way our network works—the petals that were described earlier—it does not matter, traffic will go the other way round. The backbone infrastructure is designed to be completely tolerant and completely invisible of a single break, there is always a second route. Two breaks, choosing a bad point, will cause problems. I have not been directly involved in any of the attacks on countries that have taken place but my understanding is that they have focused on high profile systems organisations within the countries so if there is a single government website you take that down. Whether you take down a national broadcaster I do not know because if you are trying to have a high impact attack, actually the thing that is telling people that there is a high impact attack is one of your tools so it is trying to understand the motivation. I suspect I would leave the BBC website where it was.

Mr Gibson: I do not think we have seen in the past—9/11 for example when the network interconnections in New York were taken down it did not bring the Internet down. It slowed it down but obviously there was a great deal more interest and a great deal more traffic, but that did not bring the network down and I have not seen anything that tells me the Internet will collapse. Bits of it possibly.

Mr Cormack: That turned out to be two of my badly chosen cuts because it turned out that our main link went one side of the World Trade Centre site and the back-up link went the other side, but we had a link to New Jersey as well.

Mr Gibson: In my bank we build the network to cater for that, we will have satellite connections that are wholly separate from the ground connections until they get to the building so if someone takes a JCB and drives through it, fine, we have a satellite connection and it will work. It is a design issue.

Chairman: Let us move on. Lord Richard.

Q88 ***Lord Richard:*** My Lord Chairman, before I actually ask this question I have been gnawing away at the construction of these things so I wonder if I could just ask FIRST one or two questions about that. FIRST is a forum as I understand it, is that right?

Mr Gibson: Yes.

Q89 ***Lord Richard:*** How many members of the forum are there?

Mr Gibson: We have about 205 teams and 20 or so liaison members such as our group.

Q90 ***Lord Richard:*** How often do you meet?

Mr Gibson: We have an annual conference and that is a global conference—this year it is in Miami, last year was in Kyoto in Japan. We typically have about 450 attendees to that and in the regions that we are holding the global meeting we will have regional meetings, so in January we have a meeting in Hamburg.

Q91 ***Lord Richard:*** What sort of agenda do you have?

Mr Gibson: It is very much driven by the members. We have a call for papers, people put up things that they want to talk about, the programme chair will go out and get people to talk, so there are talks about things that people have done, things that people are doing, the latest tricks and tips on how to handle incidents, legal issues may come up.

Q92 ***Lord Richard:*** How big is the organisation's centre?

Mr Gibson: It is purely a volunteer organisation.

Q93 ***Lord Richard:*** But how big is it?
Mr Gibson: There is a secretariat, the people who arrange the meetings and do some of the hard work, four or five people, but it is very much a volunteer network. None of us get paid to do it. There are 10 people on the board or the steering committee who try to co-ordinate things.

Q94 ***Lord Richard:*** Are they elected by the members?
Mr Gibson: They are elected by the members, five every year—they have to serve a two-year term. It is very much a members do—if you put in you will get out. If you choose not to attend the meetings and if you choose not to make yourself known you will not get a great deal out of FIRST. If you get to the meetings, liaise and put information into the mailing list and so on you will get a great deal out of FIRST.

Q95 ***Lord Richard:*** What is the spread of the teams that come there geographically.
Mr Gibson: Right now it is approximately 40% North America, I would say 20% Europe, 20% Asia-Pacific. Africa is the hole on the map at the moment; we have two or three teams in Africa and we are very much pushing to move into Africa—especially due to the enhanced Internet connections that are going into Africa we are very concerned. Up until now their connectivity has been so bad that they could not really do any harm. Now they are putting very large Internet connections into Kenya and Tanzania and various places; we very much want to push into there and we are looking at holding one of our regional meetings in Africa next year.
Mr Cormack: And South America.
Mr Gibson: We have South America too.
Lord Richard: Can I ask the question now that I was supposed to be asking?
Chairman: Before you do Lord Hannay wanted to come in at this point.

Q96 ***Lord Hannay of Chiswick:*** I just wanted to follow that up by asking whether in your experience you think that people at the top level of government or business or the military actually understand all this.
Mr Gibson: That has been a bone of contention within FIRST for many years. In fact we started an offshoot called the CEP—Corporate Executive Programme—because some of our members are very senior. We have got some people who have been very senior within various telecoms and so on and they recognised that they would walk into boardrooms and say "You are a member of FIRST" and the board would look at them blankly and say "What?" Most boards would understand that they had someone somewhere buried in a dark cupboard, looking at computers and keeping the place safe, but they did not understand that FIRST existed and that FIRST was doing all this good work and all the rest of it and thereby these teams may not be getting the resources that they need and the ability to travel to the conference and so on. We therefore started this group as a means of bringing more senior people into the mix, to learn both ways really, for them to learn that there is a group out there doing this and that they are part of it and also to get their take on the risks. Obviously most of our teams sit in bunkers and look at computers and field attacks and so on and they may not see the bigger picture from the board level and vice versa, so we wanted very much to set up this group to allow that interchange to take place.
Mr Cormack: I was going to move on to the government side. One of the things that has been seen by the community as very positive is the establishment and involvement of ENISA as an indication that it is seen as an issue. ENISA cannot join FIRST because it is not an operational body and as I understand it has no desire to be so, but there was a very strong welcome given to the members of ENISA staff who, like me, are now personal members of FIRST, so they are very much involved there.

Q97 ***Lord Richard:*** I suppose the question I am going to ask you is really a reflection of whether you think yourselves successful or not: how safe is the Internet for consumers?
Mr Gibson: If you practise the right things. Would I go and use a computer in an airport lounge to do my Internet banking? I do not think so. Would I use my home computer to do so, yes, so as long as you are cautious and careful in what you do—I do my Internet banking on-line, I do various things on-line, I am quite comfortable with doing that, so I do not see an issue with that. Some people take a more paranoid view, some people do not, but I certainly would not use any old computer that I happened to bump into to do it. Experience has taught us that a lot of the customer incidents we get in the bank are on such systems, so I think so, yes. I would not say that the sky is falling, do not use the Internet.
Mr Cormack: How a user behaves significantly affects their safety in the same way as how a driver behaves or a pedestrian behaves affects their safety. I am pretty confident that my parents are safe Internet users—they do email, they exchange information with us, they are not technically savvy at all—they may be watching. I would not regard them as technically skilled in the way that some of your witnesses may be but it is possible for the average citizen, exercising appropriate caution, to conduct their business safely on-line.

Q98 ***Lord Richard:*** Pretty confident does not sound too confident.

Mr Cormack: Accidents happen. There are reckless drivers on the Internet who put other people at risk in the same way as there are reckless drivers as I walk across Parliament Square.

Q99 ***Lord Hannay of Chiswick:*** In the EU paper we are looking at—which you are presumably familiar with—one of the suggestions is that there should be pan-European exercises carried out on large-scale network security incidents. Are you aware whether these exercises have ever taken place and have you participated in them yourselves? Do you think they are useful?
Mr Cormack: They certainly have taken place. Some European countries have been involved in American-based exercises; my only involvement has been, again, one of these face to face meetings where some ideas about a scenario were being bounced around and they were in an area where I had more technical knowledge than the others present so I was able to feed in some information which I hope made the exercise more accurate, more realistic. There was certainly a large one in the Asia-Pacific region as part of the preparations for Beijing which was co-ordinated by the Chinese CERT and they have been doing useful presentations on the outcomes of that that they found very useful, both in discovering hidden assumptions. You assume that a certain person will always be available, or you will be able to get at the FIRST website to get the encryption keys of the people you want to talk to and an exercise is much the best place to discover that those assumptions are not correct. The other thing is that it is another part of the building knowledge of other teams' understanding and having those contacts. Again, it is a point you can refer back to. We have not spoken since the exercise but I have not had a real incident so again you are straight into operational mode, trusting mode within 30 seconds of the conversation.
Mr Gibson: Again, FIRST is not an operational group so FIRST does the communications but FIRST as an organisation has not been involved although a number of our teams have. In my day job for the bank, yes, we have been involved in some of the American cyber-storms as they call them, exercises where similar sorts of things are done and they have proved very useful. I would certainly say, yes, they are a good thing.

Q100 ***Lord Hannay of Chiswick:*** If you were to hear that the EU idea had been taken up and that they were going to carry out a big exercise like this you would not recoil in horror and think it was a waste of time?
Mr Gibson: No.

Q101 ***Lord Hannay of Chiswick:*** You would actually think it was quite useful and that it would extend and deepen your own knowledge.
Mr Gibson: Exactly, yes.

Q102 ***Lord Hannay of Chiswick:*** You have mentioned a little bit about ENISA and that you yourself go there a couple of times a year. Of course it is one of the areas we are looking at; could you just say what your impression of it as an organisation is and whether they are really able to deliver what the objectives of their programme set out, whether they are well staffed, and well situated geographically et cetera et cetera. Do they have the right powers and mandate to enable them to deliver the objectives that have been set for them?
Mr Cormack: One of the issues is that the objectives have changed significantly in the last year or so because, as I said, I have been involved in the stakeholders group for five years and for the first four of those years the words "network resilience" were banned, we were not allowed to discuss network resilience because that was a third pillar issue which was for Member States. They were resourced and their programme set up to exclude network resilience; they have now been instructed to make it a major focus so there is a challenge to work out whether they need to redeploy resources they have got. They are a very small European agency; I suspect there are some corporate and national CERT teams that are bigger in staffing than ENISA so it is a small organisation. The timescales that partly the stakeholders group was involved in setting on the programme I hope are realistic. The paper, however, seems to set quite an aggressive timescale in that everything could be done by 2010. With their current resources I suspect they would struggle to do that but the skills they have would certainly enable them to do that, and the relationships they have with communities. Again it is this building up trust thing; they have spent five years going from most people in the community being scared that this was going to be an attempt to impose an operational organisation on top to actually discovering that they are really good at gathering good practice and identifying good practice, getting it written up and then disseminating it. I was mentioning to Chris earlier they have a guide to setting up a CERT which is now available in all the national European languages and Russian and they are working on further translations for extending areas. They have run exercises and training courses across the extreme points—in Dublin and Vilnius, I cannot think of the North to South but essentially covering the whole continent and beyond where people have particular interests. The Polish team have worked very closely with them on running exercises and training in the former Soviet republics, within any community referred to as the Silk Road

area. That had immediate operational benefits when there were the cyber-attacks in that area, that suddenly there is a CERT, it has a basic set of skills, it is known. That is almost entirely through ENISA's work, I do not think that would have happened otherwise.
Mr Gibson: ENISA had the mandate to do the training throughout the EU; FIRST took that training material and then has given that training around the world as well—we have done it in Tanzania a number of years ago, we do it at our conferences, it is essentially a three-day course on how to set up and run a CERT team. It is classroom-based training that we have done around the world, using the material designed through ENISA where they did not have the mandate to go outside Europe to do so.

Q103 ***Lord Hannay of Chiswick:*** So in what they do they are skilful and professionally good?
Mr Gibson: Yes, and they certainly made a very big effort to get out and to make the relationships with people that we have talked about. They have done that many times, they have come to conferences, they have joined as individual members.

Q104 ***Lord Hannay of Chiswick:*** Could you just comment on this question of the geographical location which comes up all the time and usually causes a good deal of merriment when it does come up. To what extent is it just a distraction in this particular field, or is it a real problem?
Mr Cormack: In this field in particular it is a distraction. The relevant staff are extremely well-known in the community, they come to meetings. They run an annual summer school which is a mix of academic and practitioner presentations in Crete which is actually a very good place to run a week-long conference, if you can get it past your finance people—"I really am going to work". Most of the CERT work is done by electronic communication so it does not matter, it can be done on the train, it cannot yet be done on an aeroplane, and in some airports.

Q105 ***Lord Harrison:*** My Lord Chairman, it has been a fascinating morning and I wonder whether we might invite our witnesses to give advice to the Committee about the thoughts that we will come to put in our report. One of the questions we have to ask is whether there is added value in this European Union connection and some of the proposals that have arisen in the Communication. Listening to the two of you, you are clearly engaged in a network that is successful partly or mostly because of personal connections but you have a fear of any imposed bureaucracy that might arise from the EU level. In so far as you learn information and indeed, as in your case, you impart information to those who perhaps need to know and be better acquainted with some of the pitfalls, what are your final views on the question of the added value of what is proposed here?
Mr Cormack: If I am feeling optimistic I can read the communication as very positive in supporting and extending the existing networks. I do not think there is anything in there that automatically gives me nightmares but as with many communications from governments it can be read in many ways so it may be a trite to say the devil is in the detail. It is positive that the Commission recognise it as an area that needs action, needs help. I think the Commission also appreciate that there is an existing, thriving, pretty successful community covering 25% of the European Internet and I hope that they will see that as a model that they can follow to try and extend it to the missing 75% and to increase the capability of what already exists. On the other hand it could be trying to impose on Europe something that is actually worse than the sort of thing that we tried in the late Nineties because the European CERT that we ran then was still voluntary, it was if you want to send incidents to us please do. The nightmare scenario would be an operational by mandate body that imposed itself at the top of the tree.

Q106 ***Lord Harrison:*** A recommendation would be that we use the successful 25% to pass on as a model for the remaining 75%.
Mr Cormack: Yes.

Q107 ***Lord Harrison:*** That certainly has utility.
Mr Gibson: Yes, and to use that European base as a kick start incident response team, absolutely.
Mr Cormack: While not being parochial—can you be parochial about something as big as Europe—and being willing to learn lessons from other areas of the world where they have had slightly different priorities and they have had different starting points. Asia-Pacific is different because largely they started with a completely blank slate, there were very few CERTs in Asia-Pacific until five or six years ago at which point governments and APEC-TEL stated that every country shall have a CERT by the time we meet next year. They came and looked at the rest of the world and said "How can we train these people?" and we said "Here is training material, here are trainers."
Mr Gibson: Here are conferences, here are meetings, come and join them.
Mr Cormack: We took the conference to that area twice in that period, to Singapore and to Kyoto. We are willing, happy and interested to learn how others use the material that we use; we get a lot of good feedback from South America on the use of the European training materials that we will then try and

incorporate. It works really nicely because of the shared languages—Spain and Portugal work is a very good channel to Latin America.

Lord Harrison: That is very interesting; thank you very much.

Chairman: Thank you, that brings us to the end of our session and we are most grateful to you. May I remind you of what I said to you at the beginning, that if afterwards you want to clarify or amplify any point please do so. I would also say, thinking of one question you were asked earlier on which I guess you were somewhat reluctant to answer fully, that we would be very content if you were to supply answers to that particular question on a confidential basis and we would give an undertaking that we would neither publish nor quote from it, but it would be helpful from a background point of you. To both of you, you have been very frank and very clear and we have had a really interesting morning. We are all extremely grateful to you, thank you very much.

WEDNESDAY 2 DECEMBER 2009

Present	Dear, L	Jopling, L (Chairman)
	Garden of Frognal, B	Mawson, L
	Hannay of Chiswick, L	Naseby, L
	Harrison, L	Richard, L

Examination of Witness

Witness: Mr Andrea Servida, Deputy Head of Unit, Directorate General Information Society and Media, European Commission, examined.

Q108 ***Chairman:*** Welcome Mr Servida; it is very good of you to come. You have come from Brussels this morning and we are particularly grateful; you must have got out of bed extremely early in spite of the fact you gain the hour coming this way.
Mr Servida: That helped.

Q109 ***Chairman:*** Welcome. May I just give you a few background notes? You will know that this session is open to the public, although there is no member of the public present at the moment. A webcast of the session will go out live and as an audio transmission and is subsequently accessible on the parliamentary website. You will be sent a copy of the transcript of your evidence; this also will go on the parliamentary website. If, after the session, you want to clarify or amplify any of the points you have made, we would very much welcome that but could you let us have it as early as possible. You will hopefully check it for accuracy and, again, let us know as soon as possible, if you feel there are things which need to be changed. The acoustics in this room are particularly bad. I am rather deaf so if you would be kind enough to speak up that too would be most welcome. Perhaps you would be good enough to introduce yourself to begin with to the Committee and for the record and then we will start our questioning.
Mr Servida: Thank you very much. My name is Andrea Servida. I am Deputy Head of Unit on network information security, internet and ".eu" within the Directorate General Information Society and Media of the European Commission. I feel honoured to be here in front of you today.

Q110 ***Chairman:*** Thank you. That is admirably brief.
Mr Servida: If you want to know more, I am Italian and can speak for much longer.

Q111 ***Chairman:*** Could you tell us why you believe that internet resilience is an appropriate topic for the European Union to be tackling? Surely this is really a matter for individual Member States. What is the added value that the EU and the Commission in particular will bring to this whole issue?
Mr Servida: I will start with the political dimension and then the more urgent dimension, which is the nature of the problem with which we are confronted. In terms of the political dimension, I must recall the request by the Council in 2004, after the bombing attacks in Madrid, to the Commission to come forward with a programme to help Member States work together to coordinate their activities better in order to face terrorists and the possible risk to the critical infrastructure. This led to a number of statements by the Commission. I must also recall that the Council requested the Commission to develop a programme, in cooperation with the other institutional bodies, in particular the High Representative for Common Foreign and Security Policy, that is the Second Pillar dimension, as well as the Member States, which are important, and the European Parliament. That led to a number of activities which materialised towards the end of 2006 in a communication from the Commission, as a response to the request by the Council, putting forward a programme to engage the Member States in coordinated activities in respect of their responsibility to work together in order to address and take on the challenges relating to the protection of critical infrastructures. Then there was a proposal for a directive which somehow was meant to provide the framework for Member States to identify on what they would like to work together and to exchange practices and good policy measures. This directive was adopted towards the end of 2008; it is the directive on the identification and designation of the European critical infrastructures and under this directive two sectors, transport and energy, were identified as critical ones to which the directive provisions had to be applied immediately. The next in line was somehow identified to be the ICT (Information and Communication Technology) sector. Why was this approach coming forward in the directive? Because, very much in the way that had been adopted by other countries, particularly the US which I think had opened the way back in 1997 with the PCCIP (President's Commission on Critical Infrastructure Protection) report on critical infrastructure protection in the context of the

reflection on how to deal with the Y2K vulnerability, the Commission proposed to go about engaging the Member States and stakeholders in protecting the critical infrastructures via sector specific approaches which means designing policy that would somehow address the specific vulnerabilities, including the interdependencies which had been identified in 2006 as one of the horizontal sectors, to engage the stakeholders to look at the specific sectors of transport, energy, food, utilities and all the rest. In this respect the political dimension to the urgency to look at security and resilience comes from the fact that the policy statement, policy proposal, which was put on the table in March by the Commission, tried to articulate in anticipation of what would be the implementation of the directive and anything that may come as a result of the implementation of the directive, which could only happen after 2011. Then, in anticipation of all this, we came forward with a set of measures we considered important and which were to some extent alluded to in the preparatory activities that the Commission have carried out since 2006 on how society, in general, should prepare itself in order to be able to withstand disruption. I am talking about disruptions because I think what it is important to highlight here is that the proposal that is on the table, which was adopted by the directive, is to some extent instantiating, in terms of immediate measures that it would be worth considering and pursuing, as they address at the European level the specificities of the IT sector for what it means in terms of critical sector for society. This is where indeed we have to frame this proposal and we have to frame this proposal from the perspective of how society should act in order to make the work of law enforcement, police, judicial systems more effective and simpler when dealing with possible threats due to criminal activities or terrorist activities and other possible realisations of malicious intentions that may exist in society. Why did we take this approach? Because we believe that if we want to make our society more secure, safer for everybody, everybody should pick up his or her own responsibility. Security and resilience are conducive to the message that everybody should act. We cannot just think that the protection of other critical electronic communication networks, our information infrastructures, whatever you like to call them, could be delegated just to law enforcement, defence or any other national agency or even international endeavour of national agency or governmental agency. Why? It is so pervasive throughout our society that we have to take a measure as a stakeholder. It is of course not only up to the end user to do something. That is the weak ring in the chain. It is up to everybody, but in particular the private sector. Why? Because, as a result of the liberalisation of the electronic communication network and service market, the owners and the operators of networks are in the private sector. We do not have any more monopoly type situation where it is easy for governments to act and to maintain a grip on these critical resources. The private sector is acting; we are favouring the development of new markets. This leads, particularly in this sector, to a globalised market to globalisation and new opportunities for society. However, everybody should somehow take a step and understand that we are not just talking about commodity services, we are not just talking about new gadgets and new opportunities for business growth, we are more and more relying on these services, products or resources, as if they were really the nervous system of society. In this respect everybody should take responsibility. This is why we put the focus on security and resilience and this is why, as we said in the communication, this policy proposal is complementary to everything that is ongoing and which is in the pipeline in terms of European initiatives, intergovernmental initiatives, in the area of coordinating and making the cooperation between the police and the judicial system more effective and efficient. This proposal is not just what would be sufficient to protect the critical infrastructure; it is to some extent developing the societal, the business dimension which is needed to understand and to take the citizen into account in order to make us as Europeans able to withstand the problem.

Q112 ***Lord Mawson:*** I would find it helpful if you told us just a bit more about your background before you took this post. Second, is not one of the problems that the European Union structures and systems and processes are quite slow processes and by the time you have worked out your policy the whole thing will have actually moved on? It is a bit like an elephant trying to chase a ferret; actually these things are totally different and is that not a problem?

Mr Servida: I talked about the background because I thought this would explain why there is a European dimension. The real dimension is a global dimension but we think that there is no possibility for Europe as a region to cope, to work in the globalised environment of electronic communication networks and services unless there is first a kind of unified way of approaching the problem. This does not mean harmonising everything and this is why the proposal is not regulatory but by preparing and enabling Europe to work as individual Member States and as a region. Of course what you say is very true, but it is true for any government which has a policy responsibility in this area. This is why I think it is important for any government and for any administration, including the European Union, to set the framework conditions which on the one hand would help society to develop and the internet to bring all the innovation which is needed but at the

same time would ensure that we look at the way in which our digital society is developing in such a way that we will retain in the way in which the society is developing type of safeguard, whether technological, legislative or other, which would help everybody to benefit from these developments. This is why we need to stimulate everybody to understand that they have a role to play and to find incentives. This is why the policy that we have there does not rely on the Commission to do much, to be honest; it is more for the Member States, it is more for the private sector to engage with Member States. I must say that I am here speaking before you in a country which is a leader in this area worldwide for a number of reasons but across Europe we are not all running at the same speed. The pace of development, in particular in terms of our security policy is really varied. Just to give you an example, there are countries where the first ever policies in the area of network information security were developed during the course of 2007, a couple of years ago. If that is the case, what could the understanding be in those countries with respect to the nature of the issue, how to engage resources, in particular the business and private sector resources? That is where Europe is trying to support. The Commission and the European Union are trying to stimulate the Member States to act, building on the good experience and the understanding that have been developed in those countries who have done more in this area and therefore they are leading. Of course, we also have to look at the whole picture. Just doing more yourself domestically does not make you safer because you are interconnected; you have interdependencies with other countries, with other regions. Unless we are somehow making sure there is no vulnerability or risk getting to you because other regions are not considering the measures which have to be taken, then you will never be able to be safe. Nor, I suspect, and we can build on the experience of the US in this area, no individual country could sensibly consider itself to be in a position to take on all the risks, all the threats alone just because we are so interconnected, so global and it is so easy to cause damage across the world. Something should be done to put in place without fencing, those measures which would help to keep the environment a little more secure, more resilient.

Lord Mawson: And a bit about your background.

Q113 ***Chairman:*** You did not cover that bit of Lord Mawson's question. I think I am right in saying that you are one of the authors of the Communication which is the subject of this inquiry.

Mr Servida: Yes, I am; indeed.

Q114 ***Chairman:*** You did not tell us that earlier. Could you just enlarge on your experience and what you did before you did your present job?

Mr Servida: My background is as a nuclear engineer. I did PhD studies here in London on artificial intelligence. I was always dealing with issues related to risk, in the nuclear sector, in the chemical sector, before joining the Commission. I have been working in my country and in collaboration also with companies in the UK on the implementation of the directive on risk management and on the protection of society from hazard, in particular in the chemical sector. In 1993 I joined the Commission as a scientific officer in the research programme in the domain of software engineering technologies where, because of my background, I was immediately put to deal with the area of safety critical systems, in particular with transport and avionics applications. From that I also developed my involvement in the area of security of information systems.

Q115 ***Chairman:*** Thank you; that is very helpful.

Mr Servida: And I am one of the authors, with my colleagues, of the communication.

Chairman: It is helpful that the Committee knows that.

Q116 ***Baroness Garden of Frognal:*** My question follows on from some of the issues you have touched on already. Most security issues are either local or global and although the Commission communication does have some plans for globalisation they are a little vague. You have explained why action at the EU level is justifiable, but I wonder whether you could say something about whether we should be paying more attention to other global important players such as the US, Russia or China, which seem to be playing an increasing part in cybernet activities.

Mr Servida: Absolutely; yes. This is to some extent in the spirit. The policy statement is in the framework of the EPCIP (European Programme for Protection of Critical Infrastructure) directive and the directive sets, as the first step, full cooperation at the level of Member States and the identification of European critical infrastructures, in this case for the ICT sector. We are not there and we will not be there until after 2011. Two options: we can stay away and in the meantime pursue the development of the sector-specific criteria which are needed in order to implement the directive when the directive applies to the ICT sector, which is indeed the legal framework in which we operate. Of course this is a decision by the Member States because the Directive was adopted by the Council in 2008. Or, we try to anticipate, in relation to what might come, the self-evident or the undeniable facts we are confronted with, we can start looking at how we need to prepare ourselves to deal with whatever would be then identified to be the European critical infrastructure or not for the ICT sector. This is why, for the international dimension,

we jump ahead. If you do not know what the European critical infrastructures are for the ICT sector, how can you go international? On the other hand, it seems established, and I think this is common knowledge, that the internet, whatever type of understanding we may have of it, whether physical infrastructure or a platform for supplying services for access communication, whatever, the internet itself is global and, even more importantly, it has been developed in order to be resilient. In itself, genetically if I may put it that way, the internet was built to be resilient, to be resilient to nuclear bombing, as I understand it. I was not there at the time. That was the original need which led to the development of ARPANET (advanced Research Projects Agency Network). Because the internet is global, we need indeed to start thinking of how Europe would be more influential in the way in which the internet is developed. Let me give an example. You mentioned China. China is introducing a number of regulatory measures which are extremely difficult to understand in terms of what would be the effect with respect to the overall security of the internet. On the other hand, all these regulatory developments are pursued in the name of national security. The Chinese Government is there to protect the Chinese citizen and these aims are legitimate. We cannot say they are not. However, the big picture is not there so China is pursuing this development and is introducing a number of trade issues, trade barriers, which are extremely bad. To answer you—and this is my personal understanding and understanding that I have gathered from discussion around the world—we need to make sure that this does not happen, because fencing the internet is not going to help anybody. This is why one of the pillars, within the limited responsibility we have for information activities, we are proposing Member States come forward with their priorities and our priorities as a region. One of the questions is whether we can really bring down the internet. Perhaps we may not bring down the internet as a whole system but of course regionally we may be disrupted. We are seeing cases due either to attacks or to failures of technological systems like submarine cable breaks in 2008 and before. There we thought, indeed the Commission thought, that in order to be influential we really needed to gather more information and we needed to engage ourselves more with other regions but we cannot do it via 27 bilateral discussions because that will not help and will lead to fragmentation. This is actually what we see in certain international arenas where the different perception of what is critical in the internet, whether it is the service provision or the cables and the wires or other things, is making the position of Member of States a bit contradictory one to the other. This is why, we have put there a seed for what could be the development in the area of the internet via the establishment of priorities, establishment of what the guidance could be that you, Member States, at the European level could agree would be important to secure the resilience and stability of the internet and to promote this inter nation via the strategic alliance. This is why in the declaration of the EU/US summit which took place on 3 November in Washington there is actually one clear reference to the effect that the US and the EU agreed to strengthen the cooperation on cyber security resilience and trustworthiness of the communication networks and the internet. We need to go via a strategic alliance—and I think personally but these are views to some extent shared in Brussels—that if the EU and the US can do it together the others will follow because there will be sufficient power and weight in the way in which the two regions would act together to make the others follow. This would also possibly embrace in the discussion those regions which in a way feel themselves isolated and therefore they feel they have legitimate grounds to think of the internet as a kind of private garden and to plant whatever flowers they want in their garden without thinking that perhaps this might not be good for everybody. This is very worrying because we see a regulatory development but we also see technological development. I learnt when I was in the US just before the summit at the end of October that indeed there is a proposal coming from China, at the ITU (International Telecommunications Union), to modify the BGP (Border Gateway Protocol) protocol, which is an IETF (Internet Engineering Task Force) protocol not an ITU standard to introduce counting methods and controls possibly for anybody to monitor and count the flow of packets to introduce possibly a remuneration mechanism and to make everybody pay for the flow. This is a technological development. But, what is behind it is the policy assumption that if you put in more technological controls in certain critical resources of the internet we may of course do something, which might not perhaps be so evident in what is declared to be the very purpose of such a development but which could be easily done if there is an hidden agenda.

Lord Hannay of Chiswick: May I just for a moment look at a discrete part of this threat, that is leaving aside the criminal and the natural disaster aspects and looking just at cyber warfare. We have received a certain amount of evidence about the Estonian incident, about what went on at the time of the Georgian hostilities and so on, none of it particularly conclusive. I wonder how seriously you in the Commission take this concept of cyber warfare, of attacks being made by cyber warfare outside the EU, either on one of its Members or the whole of it. If you do take it seriously—and a lot of people do now seem to and the British Government certainly do and the US—should it not really in the first instance be for

NATO to do most of the coordinating on that rather than the Commission? Is there not a risk of some confusion, overlap and so on? How do you deal with that?

Q117 ***Chairman:*** May I just say that this Committee over the last year or so has been very concerned indeed about the lack of cooperation and coordination between the EU and NATO. We have put this in reports and I have also, with another hat on altogether, drawn attention to this lamentable relationship between the EU and NATO. If you could put that together with the question from Lord Hannay of Chiswick, I should be obliged.
Mr Servida: I will try to do so. I do not know whether you have seen the report that the NATO Centre of Excellence in Estonia completed on the case in Georgia. It concerns the legal analysis of whether the attacks could actually be considered as leading to all the elements which would trigger article 4 and 5 of the NATO Treaty. The analysis is not conclusive of course. When it comes to cyber warfare it is very difficult to establish the chain of command as being the head of a government and saying "Do this, this and this". Even if that were the case, there are issues about the way in which you can ensure traceability of what is happening and understand what is indeed the actual target that was aimed at. In terms of cyber warfare, for national governments this is to be one of the areas to be looked at for sure and that is the primary responsibility of national governments and it should stay so. We as the Commission have no mandate to do anything in this area. The relationship of the institution with NATO is mostly with Solana, the Office of External Relations and I must say that, in preparation of the policy proposal that is on the table today, Commissioner Reding, actually met the Secretary-General of NATO at that time to address a very specific aspect, that is the aspect of how to work with the private sector. NATO also has initiatives to engage the private sector because at the end of the day even Estonia has shown that top-down intervention does not really fit the timescale and the pace of development and the type of cooperation and resources that you need to have readily at hand and to make them work in the scenario like the attacks which were carried out on Estonian networks. We had these discussion with NATO to see how, at least when addressing the private sector, which to some extent has owns the resources, the electronic communication networks and operates them, how we could make sure that cooperation would cover all the aspects, those aspects which are closed and related to defence needs and capability, because at the end of the day NATO will have to interact with them. Why? Because cyber warfare is not considered to be just addressing the critical governmental resources as such but a will impact society, internet banks. We have seen what happened in Estonia with attacks on banks and we should not forget the attacks on Estonia lasted for three weeks. Even in those three weeks the cooperation which was put in place was not mandated top-down from the military and a defence perspective. Of course there was a joint effort with law enforcement but really the people on the ground were mainly those who were really cooperating at the level of CERTs, governmental CERTs, international CERTs and others, telecom operators and all the rest. In short, cyber warfare activity is a national priority. There is need to look into it and to see how that could be tackled. I think the only case we could gain some understanding on cyber attacks combined with an act of war was indeed the case of Georgia; it was clear that was a coordinated effort. But, coming back to Estonia, the analysis of today is really very elusive, not conclusive and it would still be very difficult to act on it. Of course we and national governments will have to take into account that, because of the pervasiveness of the technology and services which might be subject to attacks, the realisation that a cyber warfare type of scenario would primarily impact on society and there is where, as I understand from the analysis that I have read, everything becomes more complicated because to decide whether it is an act of war or not might indeed take longer than for the attacks to impact on society and possibly be fought and mitigated.

Q118 ***Lord Hannay of Chiswick:*** Presumably the entry into force of the Lisbon Treaty yesterday will to some extent simplify a bit the divisions between the Commission on the one hand and the Council Secretariat on the other because you will presumably be trying to produce a unified approach to these matters in the future. I am still missing slightly an answer to the question which has been put to us quite often by witnesses and others as to why it is that the EU should be involved when so many of its members are members of NATO and there is clearly quite a lot of ongoing work being done in NATO.
Mr Servida: If I may, I think that the purpose of the policy as spelled out by the Commission is to bring forward and to raise awareness of the fact that because of the nature of the problems that we are confronted with we cannot just delegate defence to do it or a national security agency to do it. If we don't have the civilian society, in particular the private sector, but not only the private sector, the users, even the public administration to take up some sort of responsibility for making the environment a bit more secure, more resilient, to be able to withstand more the potential disruption, whether from attacks or technical failure or natural hazard does not really matter but we have to raise more awareness that we are not isolated. It is not that by connecting ourselves to the net without any protection we possibly only

bring harm to ourselves only, but that our resources could be exploited to carry out attacks on others and we do not even see it. There is where we try to intervene. Of course on the more cyber defence-related issue, the Lisbon Treaty would facilitate but I am not sure whether on the war-related aspect there would be any difference. I am ignorant in this respect whether we do gain any further competence, I am not sure we do. This has always been outside the scope of the Treaty.

Q119 ***Lord Richard:*** I wonder whether I might just follow this up briefly. Several times you have said that the object of the negotiations was to produce a unified way by the individual Member States, to assess regional priorities, to present those regional priorities to the United States if they have different ones, though frankly it is very difficult to see what different ones there could be. What I am wondering is what sort of structure you see within the EU to try to deal with this. Do you see a new kind of organisational structure, a director-generalship, a DG? How?
Mr Servida: My personal reflection is that we do not need a European structure in place. Member States have the primary responsibility, the democratic safeguards that have to be there to ensure that any action that governments take to fight possible disruption is to be theirs and we have seen it with Estonia. When things happened people did not turn their face to the ISPs but to government. Why? When you are disrupted in your daily life of course you turn to the government. I think that is where any and every European citizen would indeed be looking. In the UK people would turn to face your government, in Germany it would be the same.

Q120 ***Lord Richard:*** Given that, which I entirely agree with, what is the role of the EU there except a coordinating role almost an intellectual coordinator as opposed to a practical coordinator?
Mr Servida: The role that we are trying to articulate there is indeed one of not even coordinating but supporting the Member States to work together by providing the resources which would make them work together. In the policy document we are inviting Member States to act. As an example, the analysis of the Estonia and Georgia cases showed that one of the key resources to mitigate the impact and to overcome the attacks relied on the cooperation with certain governmental CERTs or national CERTs. It is always the same. There were very few, in Georgia even fewer, less than the Estonian case, but then if we look at these types of resources they are to some extent a key element of any sensible public policy at the national level, if we look at what we have on paper, on paper we have about 15 or 16 Member States which have already established national governmental capability; 11 others are being developed. Then, if you look at how these work together, we have very few working together, coordinating in a very formal way the exchange of information, they have protocols to work together; we are only talking about seven countries, we are not talking about 15 or 18 out of 27 but seven countries among which is the UK, for the very reason which I gave earlier. This is reassuring in a sense that there is already this development, but it is worrying at the same time because we do not know where things may happen and unless we get the Member States to act and possibly to be stimulated to do what they are doing then of course it will be difficult to ensure that Europe will be safe. There is where I think we do not need somebody to be at the top in Europe to coordinate; at least this is my personal view. However, we do need to some extent to have a platform, to have a body which would help the Member States to retain the responsibility but to act.

Q121 ***Chairman:*** Let me put a practical suggestion to you. You say to provide a platform to help States who are being affected. I am sure you will know that NATO, to use a dreadful acronym, have something called EADRCC, which is the body which NATO have to go to the aid of a stricken state which has been affected by a terrorist attack or a natural disaster. Each year they have an exercise. I attended one some years ago in Croatia where 17 nations participated; they had simulated hijack, biological attack, earthquake, chemical crisis and so on. This year in September their exercise will be in Armenia. If that exercise included a simulated cyber attack and if NATO, EADRCC, gave you an invitation to attend, to observe and to participate would you be keen or would you be anxious to go or have a representative from the EU go? If you were to go, I should be delighted to entertain you for dinner.
Mr Servida: What can I say? Perhaps I may say that personally of course it would be a huge opportunity to learn because nobody has a solution here. I must say that personally I would be delighted, provided that there is no problem with security clearance or whatever, because that is the other side of the picture when you have this type of exercise. Apart from this, our interest is to learn and how to put the framework in place for things to happen. When I was in the US and I was talking with DHS (Department of Homeland Security), they were actually considering inviting the Commission as observers for Cyber Storm III because they now have an extended programme of observing countries. Of course, we are not a government but nevertheless they see the opportunity to engage with us in a way that would be up to the US to decide. As I said, I felt honoured and interested. For us the participation would possibly be instrumental in designing or possibly supporting

Member States on how to work together. Indeed in that respect, in view of the fact that Member States had requested the ENISA agency to help them plan and organise the first pan-European cyber security exercise, I might say that it would be even better for them to be there to observe and learn than for us. I think that this type of event is always very enriching because they help to deepen the understanding of how complicated the issues are and, more importantly, who has been forgotten outside the room. That is what I learn at least by talking to the experts from those countries who have already conducted this type of exercise.

Chairman: It seemed to me that opportunity followed on exactly from your previous answer.

Q122 ***Lord Dear:*** I am quite sure you have covered a lot of this ground already and your answer may be relatively short as a result but I am interested in the resilience of the internet as a whole and your views about it. Do you think that it is so diverse now that it is incapable of being collapsed or brought down or do you think that incidents like "botnets" or natural disasters or cyberwarfare could in fact irreparably damage the internet?

Mr Servida: The internet speaks for itself. It has shown to be resilient and robust as a global system. So if the question is: can the internet as such be taken down as a global system? Touch wood, I would say no. I do not have all the information but the experience shows that is very unlikely. However, regionally you may have strong disruptions and that goes for any region. We have seen this in Estonia; very national. We have seen the cases of submarine cable breaks in 2008 which happened in the Mediterranean Sea which put communications into darkness in quite a number of regions. I must say that even the US are considering the issue of looking at the way in which the internet could be withstanding possible challenges. The internet is not something monolithic or static, it is evolving, which is the value that we need to ensure would stay so we should not stifle innovation in this respect. However, we are assisting a number of developments including transition to IPv6 including the possible introduction of new top level domains and the introduction of IDN (Internationalised Domain Names) characters code and all the rest of it. With the advent of the internet of things we are seeing the connection of billions of names and billions of addresses even more than in the past, so it is a fair question to look at how this is possibly going to strain the internet, not just as a whole system, because that should be robust, but in particular with respect to regional interests. It is not just that a little local or regional intervention would make sure that the internet would stay up and running; on the contrary.

Q123 ***Lord Dear:*** Forgive me if I am wrong but I take what you mean about the internet as a whole, globally, being almost impossible to bring it down; I understand that. Taking examples like Estonia, small countries, Lithuania perhaps, Albania, if one were going to attack any country of that size or indeed a larger country, presumably what I imagine would happen would be that you would attack the critical parts of the infrastructure which would mean that country or that group or that region effectively ceased to exist. You would presumably still have pockets of applicability, maybe private individuals, but you could bring down those critical parts—you are nodding; I think you are agreeing with me—within a country or a region or a company, whatever the grouping was, to such an extent that you would cause that entity to cease to exist temporarily. Is that the way you see it?

Mr Servida: It is one way of seeing it. In the case of Estonia for instance, because the issue is what are the critical or vital services.

Q124 ***Lord Dear:*** So it could be banking, it could be communication, airports.

Mr Servida: Yes; absolutely that is an easy target. However, the analysis of Estonia showed that taking down media websites was actually more alarming to people than not having transactions done digitally. We should not forget that one of the systemic vulnerabilities of Estonia was actually due to its strength of having nearly, if I am not mistaken, 95% or 96% of payment transactions done digitally. When they became independent they decided to develop the information society in a way that perhaps was not very much considering the resilience or the redundancy issues but that led to digital cash being the common means of transactions. The fact that the media were not up and running was even more alarming. Again, we can easily think what the vital services are for what we understand as society today, electricity, banking, communication but it is only really by testing and seeing how the scenarios develop—I hope that we shall not go through it—only by analysing incidents and attacks that we can really understand what is worrying and what is vital and for what purpose it is vital. That is where we come back to the issue of making sure that we learn from what is happening and we learn also from near misses, those events which perhaps do not reach the front page of a newspaper fortunately but nevertheless they are instrumental to understand the picture and how things may go wrong. That is why we, in the policy proposed at the European level, invited the Member States to equip themselves with those bodies which would make them able to learn from the process as well as to act. Of course there is not much to be taught to a country which is already well equipped, but nevertheless drawing attention to

the fact that there is a need to cooperate beyond the national boundaries, which in this country would be like preaching to the converted, is a message because it shows what the responsibilities are. It not just for a little country "A" which may be self confident that it is done everything for its citizens may be deferred to or whatever. If they do not do it, they are at risk of making others vulnerable.

Q125 ***Lord Mawson:*** The internet has really been developed by entrepreneurs who are very hands-on and are not generally writing policy papers. This thing is growing exponentially. I suspect, as an entrepreneur, that the solution to some of these questions is going to lie with entrepreneurs.
Mr Servida: Absolutely.

Q126 ***Lord Mawson:*** How do you intend to involve the internet industry in your plans and indeed in your thinking in a serious way? My experience, not in the EU but in this country, is that the world of entrepreneurs in the business and social sector and the world of government are like two worlds actually passing in the night. We may be using similar words but in terms of communicating and understanding there is quite a gap. How do you intend to involve the internet industry, if that is true, in your plans?
Mr Servida: We have to, everybody has to. In particular at the national level the internet industry, whatever it is embracing, should be involved in the discussions. There are two main reasons. First, there might not be the same understanding or there might be a communication problem, or there might be a problem of how to share the objectives, how to understand each other's objectives. Business is there to make money, to grow, to be in business, to compete globally and that is where it is important that we understand any possible consequence of a regulatory framework that in the name of other possible legitimate and important objectives could somehow put industry in a difficult position to compete globally. At the same time industry should also understand that security is not an option. We need to understand the economics behind this, what the incentives are needed. The market really does not seem to be leading to overall security. Let us take an example. If we look at the old telecom, the German telecom and the British telecom, of course they come from monopolies where there is a culture of security, of reliability which you do not find when you move to ISPs. A realisation of this, just without saying what is bad or what is good, in our discussion we try to involve all European industry across the food chain and when we talk to ISPs of course for them security is a cost. Why? Because for them the service is a mere conduit which is indeed important but at the same time there is no incentive to act. This is well represented in the way that the European organisation of ISPs, which regionally has some good practices, comes from a certain area in Europe, is unable to promote good practices in terms of security, is unable to promote this as good practice for the whole sector across Europe. Why? Because they are so diverse; we have small ISPs, the big ones coming from the monopoly, so the culture is not there. We need really to engage everyone, but we need to engage everyone in order to understand from the governmental side what the business model is, what the industry is already doing, because a lot of what major industries, in particular the ones coming from the old monopolies, are doing is not highly visible, not visible enough I believe to make everybody confident that indeed they are doing something. At the same time the sector has to react and to be engaged. That is where the difficulty lies. At the European level we think that by bringing into the picture the economic, the business, the market dimension to the way in which public policy objectives, which are legitimate and should be understood by industry, could be articulated, to the way that a baseline approach could be developed, that might be the way for industry to find a gain.

Q127 ***Lord Mawson:*** What are you doing practically with the piece of the world where you are to make those practical relations? We can talk generally about what should or should not happen, but my experience about the internet is that it is about those who begin in small ways to do really practical things that make those relationships and engagements. The internet is all about relationships and engagements.
Mr Servida: Absolutely.

Q128 ***Lord Mawson:*** What are you doing practically to try to make those interconnections between entrepreneurs and the EU?
Mr Servida: The very pillar for intervention is the European public/private partnership for resilience for which we have launched the idea. We have started a process to engage at the European level with private sector and public bodies in Member States in order to see how to establish it. By the end of this year we will come forward with the road map and the plan is to launch it by mid 2010. It is not easy and it is not easy because indeed we need to marry at the same time sharing the public policy objectives and sharing priorities on operational measures and the operational measures stay where the private sector stays. We need to make sure that there is an economy of scale so what is decided in the UK will not be different from what is decided in Spain. I suspect there are several players acting in Spain and in the UK and they may find it difficult and costly to have to fulfil or to meet requirements which are defined top-down without any understanding of the very systemic issues there and for the industry this will be a cost,

will be a way to be less competitive in the global market. That is where people like to get. How to mount it is the challenge and this is why we are talking to the private sector but, even more importantly, to Member States. The partnership should first of all be national. You are lucky enough here to have public/private partnership initiatives, the CPNI is working well and that is a pillar but we need to draw from that in order possibly to address in the European pillar those global issues which are not just UK based. We had a discussion on the public policy aspect of vulnerability disclosure and in CPNI I understand that there is a process there which is replicated by the same players in Finland in Sweden and in Germany. Is this effective or does it bring a cost? Is it not the case that there is some sort of baseline that if it works in the UK it works also in Spain, in Italy, in Sweden and in Denmark? Having the discussion once and for all and having everybody agreeing on it in terms not of regulation but in terms of voluntary commitment to what would be the practice to be followed, which is stemming from shared public policy objectives and shared understanding of the economic dimension, the market dimension, the competition dimension, we think will help industry to compete but at the same time to meet up their responsibilities. Otherwise it might become a requirement should something go wrong. We always catch the train. Estonia happened; unfortunately we did not have regulations put in place. Should something happen again, then politicians will need to introduce something and if that is introduced top-down might stifle innovation. This is what we believe and this is where we would like to get the internet industry, not only at the European level but globally though if you do it at the European level you have the voice, the weight, to pursue a similar discussion across the world. This is why in contacts that we had with the US we will talk to government but also to the private sector. DoC, the Department of Commerce, is extremely interested to see how we can align the way in which we can indeed bring the incentives forward to the private sector to make a global policy because there is an economy of scale to be gained.

Q129 ***Lord Mawson:*** You only learn about that by doing it.
Mr Servida: Absolutely. This is why we need to engage the private sector. This is why the private sector should come forward and say "We are already doing this and this is what we believe is a good practice because it is affordable, is going to bring these gains and, even more importantly, is helping society to be resilient". If just one small slice of the industry is doing this and the other part of the food chain does not do it—again we are only as good as the weakest link—I do not think that would be a gain. This is why we talk about the sector, it is not individual champions. There are champions and you had one or more here in the UK.

Q130 ***Lord Richard:*** This question may not actually be for you and if it is for you, I think you have probably answered it quite a lot already. In your view is the internet safe at the moment for consumers to use?
Mr Servida: That goes beyond my remit but we contribute a bit of course in terms of defining the point. What is safe?

Q131 ***Lord Richard:*** Usable, works, does not break down, is not attacked, that sort of thing.
Mr Servida: It depends for which purpose you use the net. When searching for information, if you just look at what information is posted there or where the information comes from, whether it is quality we do not know. Let me put it this way. I think the internet should be safer and should be safer because the user is the very weak ring in the chain, not in terms of being the one who does not understand anything about security or whatever else, but he is the one most exposed and we see this happening all the time. There are business models which push for more and more profiling and once your personal data have gone off, they have gone off for ever. In addition the user may not really fully understand what is exposed so there is an asymmetric imbalance between those who have actually retained information, because they are providing the service, and the one who is possibly benefiting from services who sees perhaps the screen or whatever or might have difficulty understanding what it is that is happening beyond the screen. That is where it should be much safer and in particular because this is a tool which is not only for computer science PhDs but for children more and more and elderly people; anybody who may not have the understanding or the knowledge to master all the technological issues and concerns and risks that there are. This is where, coming back to the private sector, I think that the private sector has a huge role to play. In our communication which preceded the one of 2009 we invited the private sector to consider the value of going for more security in services and products and to look at the way in which they train their people as a way to bring good practices and knowledge to society. We all work in a way and we all use these means in our daily activities. If you were helped and if you trained and before that you were trained in our curriculum—but this more for the Member States—then there is the possibility for us to build an understanding and culture because it is a cultural issue not a technological issue. There is no technology, at least from what I see, that could solve all the problems. It has to do with the process, with the way in which we understand and we actually

relate to this environment. So it is a culture. This is why to some extent the kids are more exposed but they are more cunning in a way in dealing with certain issues. This needs to be considered as a priority and this is why we said in the communication that one of the key elements is that trust is not just security of procedures but security of resilience; trust is more process, knowledge, culture. We need to behave. We need to understand that if you are trespassing into certain areas it is like throwing stones at the windows in the street. This understanding is not there yet.

Q132 ***Lord Naseby:*** You have convinced me that there is a role for the EU on small countries and bringing them up to speed and helping them. You have also put a very strong case for the commercial world to be working together within certain boundaries which are set. My Lord Chairman raised the question of NATO on the security side. I should like to raise another dimension of security which does seem to me either to be local or global and not necessarily just European and that would be the terrorist situation. It does not matter whether you go back in history to the Baader Meinhof or whether you go back to the IRA or whether you are more current with al-Qaeda and, something I do know quite a lot about, the Tamil Tigers, all of those issues are primarily either local or global. I have some difficulty in understanding what the role would be for the Commission in relation to the terrorist dimension.

Mr Servida: As I tried to explain right at the beginning of my evidence, the policy which was put forward in this communication in March was not addressing how to go about terrorism. On the contrary. It takes for granted that Europe is engaging, is understanding how to deal with, how to fight terrorism, how to fight cybercrime, how to improve the cooperation between law enforcement agencies and the police and that is happening. Until the end of last month it was under the Third Pillar; there are several initiatives in which the Member States have engaged themselves and the Commission is helping in terms of exchanging information, reinforcing the investigation capabilities in Member States and all the rest of it. This is to happen and that would address exactly your aspect. What is on the table here is in addition to it. We should not forget that there is no civil defence capability in any country that would be able to intervene in a crisis in the country unless we have a good engineering code for buildings construction. If these will not withstand or are not designed and built to withstand the weight and the risk, whatever the risk—not the nuclear bomb risk because there is a risk trade-off there—but will withstand the wind, the snow whatever, without this type of cooperation between society and civilian resources and an understanding of that risk and the public bodies which have to intervene in the area of fighting cybercrime and cyberterrorism, if we don't the understanding that we need to do both, not just going after terrorists but also to make sure that we have a more secure and resilient and safer society in which we have to prevent terrorists doing whatever they want to do whether locally or internationally, unless we do this we will not be able to make our society safer. It is like pretending in the civil defence we have to go after any crisis without having an engineering code deployed by society on the way in which buildings, bridges, railways and infrastructures are built. That is where we intervene. This is why we look at preparedness, we look at resilience, we look at the way in which civilian resources, the private sector, should take up responsibility to make the overall environment more secure, to make it more possible for law enforcement, judicial system, intelligence, to do everything that should be done in order to prevent and fight and go after terrorists and cyber criminals. This is why we say it is complementary; it is not replacing. On the contrary, the type of issue that you are raising, issues where—I do not have any understanding because I do not deal with terrorists-, of course terrorists are using resources for communication, they even bring destruction; they do. If you are disrupting society, it is one way of upsetting the order of society, to upset it even more now that you are interconnected, economic systems, the financial system. Disruption in a country is tremendous. Everybody looked at what happened because of the attacks on the Twin Towers, the financial losses. Why? Because there is a reverberation globally. It is not like in the good old days where there was a dampening effect of time, geography, distance. No, no, I plug in, whether I am in New Zealand or in Bristol, to me it is all the same, we are on the same timescale.

Q133 ***Lord Naseby:*** What I am trying to get at and the one area I do know quite a lot about is the Tamil Tigers. The Tamil Tigers have websites in the UK and France, Germany, US, Canada and probably half a dozen other places. They are different websites and each one was cultivated for a particular market. I asked a question the other day of my Lord West of Spithead here: how many terrorist websites have we closed? We have not closed any. We have modified them, we have leant on people, we have not closed any. My question to you is: are you saying to us as a committee that the EU, that is a specific area, in relation to terrorist websites will have a role to play or do you envisage that it will remain with the individual national governments coordinating between themselves on controlling terrorism?

Mr Servida: What I am saying is that aspect is not in my field. I know that at the beginning of the Barroso Presidency Commissioner Frattini wanted to

introduce measures to close down websites instigating terrorism. That is a legitimate concern but this may turn to be against freedom of speech. I am not following that part of the work and I know that the Commission are doing something but to be honest, I will not be able to answer your question because it is not directly within the scope of what we are doing here. What we are doing here is everything that is needed in order to make the environment, then the specific intervention is what is being done by our colleagues in Justice, Security and Home Affairs, who normally confer with you on their legislation. I know there were discussions and they had one proposal and I remember the one of Commissioner Frattini but to be honest I would not be able to tell you in a way that is assertive whether or not we have a role there.

Q134 ***Chairman:*** Your communication talks about "National" CERTs which cover more than just the public sector infrastructure. Could you explain to us why you have chosen that route rather than the route which the UK has followed of having a series of sector-specific and company-specific CERTs rather than the arrangement which you envisage in your communication?

Mr Servida: Business is business. The last count that was done, the inventory that is available from the web of ENISA, says that in Europe we have more than 130 CERTs, industry, academia, governmental, national, you name them. This is growing, in particular the work between the private sector and academics. In view of what the needs are, the business model, the provision of new services, what we were addressing there was building on the experience that we see internationally, first in Europe but also internationally, how Member States should consider putting in place very basic services which are needed on top of which they may articulate not just policy in the area of protection of critical information infrastructure, but, even more importantly, which can engage this society to be more responsive in order to prevent, fight, mitigate and recover possibly from disruption. What might our Member States need to consider in terms of having an operational capability, which is essential. If we look at the analysis of Georgia and Estonia, NATO did not intervene, nor the ministry. We had a CERT, a CERT in France in the UK in Finland, Georgia, the CERT in Estonia, so those capabilities are there and they will always have a responsibility to manage the networks but at the governmental level, it is important that governments realise that they need to have some operational capability in place. How do you organise it, whether it is just a national one or, the model which is in the UK, different ones, is really up to the Member States. This is why we say National/Governmental CERTs. This is to us a basic component which is operationally needed in order to make each country capable of cooperating with other countries at the European level but, even more importantly, to make their policy effective at the national level because it is only via these operations with people on the ground, those who actually have the problems and own the networks that indeed you can really work out a solution. These CERTs, computer emergency response teams, are those who are in contact with the private sector and those who manage the network. This is why we said it is not just a need for Member States to establish whatever they like, but they need to have it and they need to have this resource not just as an operational resource, but to become a key element, key tool in the public policy development which is needed to engage again the private sector and the other stakeholders in enhancing the level of security resilience nationally and the European and then the international. It is a more a plea to the Member States to understand that it is important and this is built on the realisation that, despite what we see in the paper, the cooperation at the pan-European level is very limited; we have seven or eight countries where these capabilities are working together. What about all the others? Is this good? We do not think that this good because if we need to react as a region, it would be good to know to whom country A could indeed relate and how to relate. It is not just via the highest political level that a relationship should be established; here we are talking about events which happen at the speed of light so we need to be there in the field and know with whom to engage. This is where the experience in the UK, in Finland, in Sweden and in Estonia now, who did not have much capability, shows that is the way in which you can really be operational and effective.

Lord Harrison: Have ENISA been given the resources to be able to deliver what is asked of them in this programme? Will they manage to deliver it on time in your view?

Q135 ***Chairman:*** Before you answer you might just say a word about the criticism we have heard about the impracticability of basing ENISA in Crete.

Mr Servida: Two aspects. On the last point, I see the issue as not related so much to the location in itself but more to the way in which the body needs to be at the heart of the processes. I will try to explain myself. In the internet society, an information society as we are now, there is no geographical impediment but you need to know to whom to talk and how to engage with those with whom you want to talk and to do business and cooperate. The problem of the location beside what might be the issue of accessibility, getting there physically, is more an issue which has to do with the way in which a body, an institution like the Agency, would be, could be and should be effective in terms of helping Member States and the private

sector and institutions to progress and advance in this area. I think that in terms of effectiveness or impact of ENISA we think that there is a need to reform this body which was established under different type of conditions. The idea and the consolidation of the regulation in place happened before the enlargement. With the enlargement we had more countries coming into the Union with a completely different set of needs and expectations and even the evaluation report which was conducted by external experts towards the end of 2006/beginning of 2007 reads clearly that the enlargement, the joining of new countries with new needs, strained the environment because the regulation and the mandate was rather different. Having said all this, we need to make this institution work. It is clear that it is your money, it is our money and, even more importantly, it is a resource which could play a unique role in supporting the Member States but they need to support the Member States and work with the Member States. They need to work with the private sector. This is why the problem of the remote location is more a problem of the remote positioning of its working practices than the location in itself. You can work without having to move geographically around Europe but you have to be at the heart of the process; you need to understand your constituency, you really have to find yourself in this area and understand the needs of the Member States, the priorities for the private sector. This is why, in the communication, both of 2006 and the one of 2009 we try to give an impulse to ENISA to focus on certain European challenges for which there is a role for a platform like this to help Europe to progress. Why? Again we have tried to shine the light on issues where Member States should act individually, but they also need to work together. We do not need somebody at the top to coordinate that, we need somebody to make them work together and find a way of engaging the Member States. More importantly, we need to engage the private sector in this area. Coming now to the first part of your question on whether they have the resources, I think that the problem is more an issue of the focus and the way in which the resources have been used and affected. That is where we need to work. Of course if we all had more resources to do what we would like to do, it would be much better, but even with the current regulation, with the current level of resources, there is quite a lot that ENISA could be doing and to some extent is trying to be doing now with the new management. Even with the new work programme structure which has somehow been put in place since 2008 with a programme with the focus on resilience, for instance, they have done an interesting stock-taking exercise on the security and resilience regimes in Member States. That was important for us to have at our disposal in order to articulate where to intervene. We need to have data on which to act and in order to have this data we need to have a body like ENISA but this whole focus should be the good one ENISA should not position itself to do everything that covers every possible topic. It should really try to focus on where it could make the difference because it is there to help Member States and the private sector.

Q136 ***Chairman:*** That completes our session. We are most grateful to you and you have answered our questions very fully indeed and we appreciate that. We shall look forward to hearing from you again in the event of you wishing to expand on any of the things you have said or to reflect on them. I hope I shall be able to give you dinner in September.

Mr Servida: I look forward to that.

Chairman: Thank you very much indeed for coming; we appreciate it very much.

WEDNESDAY 9 DECEMBER 2009

Present	Billingham, B	Harrison, L
	Dear, L	Jopling, L (Chairman)
	Garden of Frognal, B	Mackenzie of Framwellgate, L
	Hannay of Chiswick, L	Richard, L

Memorandum by Symantec

Today the very foundations of the UK and Europe's modern society and economic stability are built on electronic communication infrastructures that span across national, European and international borders and the data that is shared, processed and stored within these networks. The move away from closed, nationally protected computer networks to a more borderless, open, accessible, Internet based, networked environment means that safeguarding electronic networks and systems from possible attack or disruption is a crucial component of nations critical infrastructure protection. This relatively recent shift towards greater dependency and reliance on internet based systems and networks across Europe means a change in the approach to critical infrastructure protection that recognises that cyber related risks and attacks could now impact and affect more than just one nation.

It is particularly important that such risks are identified quickly and addressed effectively particularly given the significant increase in criminal use of the Internet for purposes such as identity theft and extortion. For example targeted attacks on systems have been seen that are designed to prevent their legitimate use such as "denial of service" attacks. These and related crimes are committed through the infection of computer systems, used by citizens and organisations, with malicious computer code, viruses, worms and Trojan horses. Such infections generally occur as a result of poor security practices on the part of system owners and users and enable the spread of spam, phishing and the establishment of networks of compromised systems that are under criminal control called "botnets".

This current online threat reality and the pervasive nature of internet based technology within European society was recognised by the European Commission in its publication of the recent Communication on "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience". Symantec supports the approach taken by the EU Commission Communication on the steps needed to protect the resilience and robustness of EU information and communications networks. Given the current online threat environment only by industry stakeholders and government working together can the security of the critical infrastructure within each Member State, across Europe and globally be protected. The suggestion of holding common exercises and collaboration with the private sector in the area of information exchange and early warning is seen as a key element of the approach. It is felt that the EU's approach could also provide an opportunity to consider and address possible legislative obstacles or challenges in this area and ensure an appropriate legal framework is in place. Furthermore it is an opportunity to recognise private sector activities and efforts underway and highlight examples of best practice in addressing the need for greater co-operation and collaboration in this area.

Clearly there is a role for Member States to address possible cyber related risks to national systems as well as a role of the European Union to consider the protection of European networks and systems. However, given that it is understood that up to 90% of critical infrastructure assets in some countries are privately owned and operated, public and private sector collaboration is a key factor to critical infrastructure protection issues. Addressing Europe's cyber security challenges is not something that can be solved or addressed by one Member State, European institution, law enforcement body, business or individual acting alone. Protecting Europe from cyber threats and attacks requires a co-operative effort and an understanding of the current online threat environment.

Current Online Threat Environment

For the last seven years Symantec has produced its Internet Security Threat Report which provides an overview and analysis of worldwide Internet threat activity and a review of known vulnerabilities and trends in activities such as phishing, botnets and spam. The report is based on the most comprehensive source of internet threat data which is gathered from Symantec's Global Intelligence Network. This network is based on 240,000 sensors in over 200 countries that monitor attack activities through the deployment of Symantec's products and services which actively protect businesses and consumers online.

According to the latest Internet Security Threat report, published in April 2009, cyber threats continue to be aimed at exploiting end users for profit with attackers refining their online activities and abilities to conduct online crime such as fraud and large scale attacks. The continued growth of the internet and the number of people increasingly using it for an array of activities presents cyber attackers with an ever growing range of targets and also various means to launch malicious attacks. Web based attacks are now seen as the main vehicle for malicious activity over the internet; users visit legitimate websites that have been compromised by attacks in order to spread malicious viruses or infect machines in order to create botnets that can be used for other online criminal activity. That does not mean to say that risks from more traditionally understood cyber threats have decreased. In 2008 Symantec detected 55,389 phishing website hosts which is an increase of 66% over 2007 when 33,428 phishing hosts were detected. Also there was seen a 192% increase in spam detected across the internet, from 199.6 billion messages in 2007 to 349.6 billion in 2008.

Overall cyber attacks are becoming increasingly complex, sophisticated and organised. Information is now the key target for cyber criminals. No longer are online attackers motivated by notoriety but by economic gain. Individuals and businesses are being attacked to gain access to information which has become a valuable online commodity that can be used to conduct phishing, spam attacks and online identity theft. Cyber attacks are also becoming more organised and running operations as a business. For example cyber attacks are known to have contingency plans in place in case to relocate their activities around the world if their activities are detected.

Threat analysis

— *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?*

From the perspective of the computer security industry, and on the basis of experience to date, it is suggested that the Internet has been resilient. However it is suggested that the view of others, such as the ISP community that are particularly involved in the administration of Internet infrastructures, are sought on this question.

Overall however the Internet is simply a series of interconnected computer networks, systems and essentially large servers based all around the world. Therefore as with any electronic or computerised system these computers are reliant on electrical power to function. Therefore it may be possible that a natural disaster that impacts or disrupts power within a country or region could potentially affect the ability of the Internet users to gain access to online networks or systems. Physically, therefore the internet is susceptible to regional interruption such as when cables are broken. In such an incident, although routing information may be updated to route internet traffic around the broken connection, entire countries could be left unable to access parts of the internet for many hours or days. Such outages have occurred when an undersea cable providing network connectivity to the Middle East was damaged.

A possible technical threat was seen in 2008 with the publication of a fundamental flaw in the DNS system. This incident underlined that many of the protocols necessary for the internet to operate may possess weaknesses that could be maliciously exploited. Internet protocols are implemented by a relatively small set of programs, BIND for DNS, Apache for http for example. It can be suggested that even if an underlying protocol is secure, there may still be weaknesses discovered in a program that implements the protocol for the vast majority of users on the internet. These weaknesses may be open to malicious exploitation which could cause harm to a large number of internet users. However in such an incident and despite the impact on some users, it is suggested the internet overall could continue to work correctly as internet traffic would simply be routed away from the weakness until the incident is resolved.

Clearly though the risks and threats to the security, integrity and resilience of the Internet have certainly increased over recent years. This together with the shift towards greater interoperability between internet based networks and systems means that a targeted cyber attack has the potential to have a cascading effect and impact on other connected systems in the event of a major technical fault or network compromise incident to one system or network such as in a denial of service attack. It is therefore vital that adequate levels of protection are in place that can identify and minimise possible single points of failure and that rapid recovery plans are introduced to pre-empt any large scale incidents.

— *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

It is suggested that ensuring the ongoing resilience and stability of the Internet is a responsibility that must be shared by all those using the Internet, whether they be businesses, governments or individuals. However Symantec recognise the responsibility we have to develop and implement tools and solutions that can protect our customers and as a result play a role in ensuring the overall security and robustness of the internet.

Overall Symantec believes that a modern approach to internet security must be balanced between protection and preparedness to address incidents. As a result security tools and solutions are increasingly being designed and incorporated at the beginning of the process of building critical online systems. In addition early warning capabilities, incident response services and real time online threat intelligence capabilities have been developed by industry to enable organisations to address cyber incidents quickly and effectively. Having technology in place that is part of an organisations every day operations and provides a multi-layered defence against possible online threats is seen by Symantec as vital to protecting or limiting the possible impact on systems may be affected by any cyber related attack.

Symantec believe that regulation can have a role to play in ensuring an effective regulatory and legal framework is in place that enables the information society to flourish. The recent steps taken by the EU review of the Telecoms Regulatory Framework to clarify that the computer security industry can process traffic data for network security purposes has particularly been welcomed by Symantec. However, just as the online threat environment continues to evolve at an increasingly fast pace so too does the Internet and information technology. Therefore given the rate at which the Internet is maturing it is important that legislators do not try to intervene to address a specific threat or risk that industry may be better placed to address by the development of a tool or solution that could be applied more quickly than a regulatory measures. Although there may still be areas where increased international harmonisation of laws may be beneficial to assist cross border co-operation, prosecutions and mutual legal assistance in areas such as online crime. Overall however it is suggested that legislators do not try to run behind, or even ahead of, technological changes but rather support industry efforts to address Internet threats.

— *How concerned should be we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

Bots[1] are programs that are covertly installed on a targeted system that allow unauthorized users to remotely control the computer for a wide variety of purposes. Computers that form part of a botnet are under the control of the botnet operator and can be commanded to execute any function the botnet operator wishes, or any function dictated by whomever pays the botnet operator for access to the botnet. Attackers often coordinate large groups of bot-controlled systems, or bot networks, to scan for vulnerable systems and use them to increase the speed and breadth of their attacks. In 2008 Symantec observed an average of 75,158 active bot-infected computers per day which is a 31% increase from the previous reporting period. Bot networks were also responsible for the distribution of approximately 90% of all spam email.

It is the fact that attackers can use botnets to perform a variety of tasks, such as enabling a Denial of Service attack or distributing spyware or to harvest confidential information from within an organisation's network, that makes botnets such a threat. Also botnets are inexpensive and unfortunately relatively easy to create and manage. In 2008 Symantec saw botnets being sold online for as little as $0.04 per bot.

Bot networks create unique problems for organisations because they can be remotely upgraded with new exploits very quickly, which can potentially allow attackers to outpace an organisation's security efforts to patch vulnerable systems. Also Symantec is seeing a move from botnet owners moving from traditional IRC based botnets, which are easier to detect, track and therefore block, towards botnets based on HTTP traffic. This essentially means that a botnet controller is communicating to the computers under his control using HTTP communications which can be hidden within other legitimate internet web traffic. It is therefore increasingly harder to distinguish bad messages to botnets from legitimate HTTP traffic. This shift in the communication channel by which botnets are being controlled means it will become increasingly difficult to identify and locate botnet controllers.

So far the major botnets that have been observed have been used primarily for the distribution of spam. We have yet to see the impact of a major botnet comprising in excess of 100,000 infected computers being used in a wide spread denial of service style cyber attack against a nation or region. The number of bots required to conduct a significant attack against an organisation are relatively low and the potential damage an individual bot can inflict is dependent on the bandwidth available, rather the upstream bandwidth.

Clearly botnets are not solely a European problem and therefore this is an area where international cooperation is needed. In fact the country with the most botnet computers is China which has 13% of the worlds botnets followed by the US. The UK was ranked 9th in the list of 10 countries for botnet computers in 2008. This is in comparison with September 2005 where the UK was ranked the highest country in the world for botnet computers. It is suggested that the high concentration of botnets in the UK at this time may have been related to the roll out and take up of broadband with users going online for longer periods of time without adequate security protection, making these computers perfect targets for botnet controllers to develop a bot network.

[1] Bots, short for "robots" are programs that are covertly installed on a user's machine in order to allow an unauthorized user to control the computer remotely.

Given the constantly evolving online threat environment and the way in which bot networks evolve (as seen above with the change from IRC to HTTP communications) there is no simply solution, or silver bullet, to solving the problem of botnets in Europe or internationally. However the decrease in botnet computers in the UK warrants further consideration as it may suggest that there may be ways of addressing botnets. It is suggested that the decrease in botnets in the UK may be a result of users putting in place online security that is appropriate and adequate to their online activities. Therefore raising awareness and understanding of the importance of having a multi-layered defence against online threats is seen by Symantec as an important message to communicate across Europe: particularly in those newer Member States that may be taking the first steps in implementing a broadband network.

— *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

According to the latest Symantec Internet Security Threat Report 49% of the top 10 attacks on government and critical infrastructures are Denial of Service attacks.[2] For example eGovernment services continue to be a key target of large scale attacks against their infrastructure. It is also expected that such large scale attacks are likely to be targeted against those providing crucial societal functions across different member states. In addition in a number of cases there have been reports of massive attacks in scale but not aiming at causing disruption, but rather at collecting intelligence and stealing confidential information.[3] The perpetrators of such cyber attacks can vary ranging from criminals, to terrorists to even hostile nations.[4]

Clearly however the events in Estonia and Georgia are real life examples of how sophisticated and targeted large scale cyber attacks can be. It is also suggested that these attacks are not the only incidents seen around the world of its kind. Given the impact that such large scale attacks can effectively have, the Commission's concern about the security and resilience of Member States critical systems and ability to address cyber attacks is justified. Particularly as it is still unclear to what extent relevant parts of EU Member states national administrators possess the technologies needed and e-skills to address cyber-attacks if they occur or address issues related to the protection of the internet.

— *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

As stated earlier, addressing cyber security challenges is not something that can be solved or addressed by one European Member State, institution, law enforcement body, or industry acting alone. Each actor has a different role to play depending on the type, or level, of incident taking place and the appropriate level of measured response required. For example service providers, security providers, law enforcement, security services and national critical infrastructure protection authorities may be the first port of call and have clearly a role to play in dealing with an incident. At the same time however we must not forget that the cyberspace is increasingly becoming an area of military importance and an area whereby different countries have developed capabilities and even command structures to address the perceived threat. It has been seen that NATO has become increasingly active in this area from the national security and national defence standpoint. This move is recognition of the fact that by the moment the threat becomes military in nature there is a role for military involvement and appropriate response.

International Responses

— *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

Given the cross border nature and interdependence of Member State critical infrastructure systems (ranging from communications mechanisms linking citizens to water and power and other Supervisory Control and Data Acquisition (SCADA) systems[5] and in the near future pan European e-government services) Symantec believe that effectively securing Europe's critical infrastructure network means having in place a common European-wide approach and strategy. This is seen as particularly important given that many Member States are at different stages of internet development and levels of understanding regarding the interconnected nature of networks and level of risk to possible cyber-attack. A European wide approach to critical infrastructure protection would enable the development of a common, shared level of understanding and recognition of the

[2] Symantec Internet Security Threat Report Volume XIV at http://www.symantec.com

[3] See recent reports on Ghostnet http://www.symantec.com/security_response/writeup.jsp?docid=2009-033015-5616-99

[4] See reports on DDoS attack incidents in Estonia, Lithuania, Georgia and more recently in Korea and US http://blogs.zdnet.com/security/?p=1533, http://searchsecurity.techtarget.com/news/article/0.289142.sid14_gci1361258.00.html

[5] Supervisory Control and Data Acquisition (SCADA) networks are comprised of remote software and hardware elements (including sensors, relays, switches, databases, networks and applications, among others) whose functioning enables the automated delivery of essential goods and services, including energy and power, water, and waste treatment. They are thus a key component of Europe's critical infrastructure, and their security is integral to European citizens' ability to access key services on an uninterrupted basis.

specific critical infrastructures within Member States that need to be protected from online attacks. Also more importantly a pan-European approach is necessary to identify the interdependencies that currently exist in the critical infrastructures shared across Member States to ensure risks are identified, assessed and addressed in a way that protects these critical systems against possible attack.

However, while cooperation at a European or international level is important, this should not be a substitute for countries take a national approach that is approach to their level of maturity, identified risk and therefore specific requirements. The recent publication of the UK's cyber security strategy was welcomed by Symantec as an important move forward in helping to co-ordinate, and maximise, efforts already well underway across government that currently seek to address cyber security related issues. Also supported was the important place throughout the strategy of finding ways for government and industry to work together to realise the Government's vision.

— *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

European critical infrastructure is a patchwork of private and public operators, spanning across Member States. In many countries is it suggested that up to 90% of critical infrastructures are in fact privately owned. Therefore in order to effectively address the security challenges of Europe's critical infrastructure assets Symantec believes a co-operative approach among industry and government is necessary. Fostering co-operation and effective public-private working relationships both within and also between Member States will help to ensure expertise in the area of critical infrastructure protection is identified, information on cyber related threats can be shared and common approaches to dealing with threats that have an impact on more than one sector, or Member State, are developed. However finding ways to create a trusted environment between public and private sector partners that enables information sharing to occur will be a key factor in ensuring the success of public-private partnerships.

It is suggested that the obstacles to developing such partnerships at a European level may be both technical and legal. Currently it is felt that there are inadequate incentives for cooperation at European level and the current legal framework does not foster or encourage information exchange. There is also an inherent issue of trust however clearly there is no silver bullet to addressing this issue and it will take time to resolve.

— *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

From the security industries perspective it is felt that the market has, and continues to, develop technological tools and solutions that are appropriate to deal with threats and risks identified and address these accordingly.

It may be that while critical Infrastructure Protection has traditionally focused on the protection of physical infrastructures and material assets, the move towards greater reliance and use of internet based networks and systems has required a shift in understanding and recognition by organisations of the risks they face in an increasingly interconnected threat landscape and the need for a new approach to defending and protecting critical infrastructures. As a result it must be recognised that different organisations, sectors and even Member States will be in different stages of their technological development. Therefore these organisations or Member States may not recognise that the likelihood of a cyber-attack occurring, such as a denial of service attack, may still be low but the potential negative impact on the ability of an organisation's networks to operate and communicate with other partners may be very high. While the security industry have developed tools and solutions to address the resilience, availability, security and integrity of networks and systems, it is suggested that organisations must first understand the need to shift towards a security approach that recognises the interconnected nature of European networks before they can consider how to prepare for such incidents and put in place appropriate, or adequate, security measures.

Symantec believe it is more important than ever for organisations to prepare for incidents by taking a risk management approach to addressing online threats and risks to ensure the security, integrity and availability of network and services and protect the resilience and robustness of EU information and communications networks. A risk assessment is a proactive mechanism that can help organisations to effectively evaluate current vulnerabilities, identify upcoming threats and consider their level of risk, establish appropriate processes and procedures and define proper countermeasures. Conducting regular risk assessments is an important element of any organisation's ability to identify, understand and appropriately address known, and unknown, risks they may be facing. Symantec has supported the moves taken in Europe to introduce into the reviewed Telecoms Regulatory Framework the importance of taking a risk assessment based approach to addressing security requirements of communication networks.

— *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

Symantec strongly believes that information sharing is a fundamental component of critical infrastructure protection. The online threats we see today are dynamic, changing rapidly and therefore require unprecedented vigilance and early detection and response to risks. Having the right information at the right time can enable a timely response to an attack on critical information systems. For instance real-time information collection, correlation, analysis and response capability can help to identify abnormal or irregular behaviour on networks that could be the indication of suspicious activity or even an attack to critical infrastructure systems before it occurs. Symantec supports the creation of EISAS as an important resource for sharing information and providing alerts that could help Member States to protect critical infrastructures proactively and therefore help to minimise the potential impact of cyber-attacks.

An example of an effective Information sharing system is the US IT—Information Sharing and Analysis Centre (ISAC) for which Symantec is a founding member. The IT-ISAC established a common standard for information sharing which provides systems and interfaces to allow information to be securely exchanged. This partnership ensures that organisations have a broader view of the online threat situation than any single organisation and can provide early warning services to its partners. It is suggested that any European initiative in this area could be developed in a way that is complementary and mirrors the success of existing systems in this area.

However, to assist in the development of EISAS and as a way to ensure greater effectiveness in information sharing between European partners, Symantec believe consideration should be given to the development of a common language, or terminology, for security incidents, response and escalation. It is suggested that the ability of stakeholders to speak the same technical language in the event of a cyber-attack could help promote greater cooperation and cohesiveness in responses to incidents. It may also assist in alleviating any challenges posed by the use of different technologies across Member States.

— *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

CERT's play an important role within Member States for providing a national focal point for information, guidance, providing warning, reports and alerts. A reason why CERTS may seem to work well could be that they are fairly small communities and the prestige of being first to report a vulnerability within the peer group can be reward enough. Overall the CERT model is also flexible to enable Member States to develop multiple CERTS, or different types of CERTS, depending on the particular requirements and needs depending on the type or risk or threat activity that may need to be covered. Symantec supports the CERT model and sees it as an appropriate means of sharing information and encouraging a collaborative approach to addressing cyber related issues within, and between, Member States.

— *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

It is suggested that the introduction of a European wide system would not hamper the UK's efforts but in fact could do the opposite and enable the overall improvement of the level of resilience across Europe. For example a EU system could act as a means by which the overall level of cyber security and resilience is raised and set (harmonised) at a higher level while still allowing for national flexibilities. As a result the UK's existing approach would still apply but simply other Member States activities could be raised to replicate the same level of security and resilience.

— *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

Clearly internet threats and risk of attack is not a problem that Europe is facing alone. Internet security is a global problem that requires a global approach given that threats and attacks can travel around the world simply at the click of a button. Therefore it is suggested that any European approach that is developed should be discussed with other countries to encourage greater co-operation and collaboration between countries before and after a cyber incident occurs.

European Network and Information Security Agency (ENISA)

— *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

Since its creation in 2004, ENISA has played a valuable role in bringing together government, industry and academia to share experience, knowledge and good practice. It provides a forum for discussion, platform for education and information exchange, and an environment where greater co-operation and awareness raising can be encouraged and enhanced. The role of ENISA is to help the development and deployment of national CERTs and not to act as a systems integrator. However, Symantec does possibly see a role for ENISA as providing a co-ordination role between Member States and stakeholders with concerns about cyber attacks and incidents and the corresponding national CERTs. For example ENISA could work with CERTs to gather anonymised information and data on cyber attacks conducted in Europe which could be reviewed and discussed with ENISA's industry working groups as a way to develop and promote examples of best practices in addressing and dealing with cyber attacks across Europe. However, it is suggested that ENISA should not attempt to replicate or reinvent efforts that are already ongoing by industry but rather find ways to identify and promote best practice and encourage industry efforts.

— *Is ENISA being effective in its role, or does it need reform?*

ENISA has been effective in its current mandate but it is understood that this mandate is currently under review.

Timescales

— *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

It is understood that the Commission's approach has a number of different areas of focus. Progress going forward may depend on whether priority issues or specific targeted areas of activity are identified and whether adequate resources are made available.

November 2009

Examination of Witnesses

Witnesses: Mr Ilias Chantzos, Director of Government Relations, Symantec (UK) Ltd., and Dr Jose Nazario, Manager of Security Research, Arbor Networks, examined.

Q137 ***Chairman:*** Good morning. Dr Nazario and Mr Chantzos, we much appreciate the time you are giving us to come and give evidence. You have given us very helpful written evidence, which we appreciate very much indeed; but, as you will realise, we are very anxious to have a face to face discussion and we are looking forward to this morning. If after this session is over you feel that you would like to clarify or expand on some of the points you have made we should certainly very much welcome supplementary evidence. Let me ask the first question: it would be helpful if you could introduce yourselves and explain briefly how your companies fit in within the Internet industry, and to try and give us a verbal picture of what actually your companies do.

Mr Chantzos: My name is Ilias Chantzos. I am the Director of Government Relations of Symantec for Europe, Middle East, Africa, Asia Pacific, Japan. So I have responsibility for the government relations programme of Symantec for the whole world outside Americas. I am a barrister by training and before joining Symantec I used to work in the European Commission. I was responsible for information security policy within DGU Information Society. In that capacity I have done a number of legislative activities in this area. That is a bit of background about myself. In terms of who Symantec is, if you do not mind we have actually prepared an opening statement answering the first question, if you do not mind me walking you through that. First of all, we would like to extend our thanks to the Committee for the opportunity to provide oral evidence to this important inquiry. Founded back in 1982 Symantec has evolved to become the world's leader in information security. We are providing information security, storage and system management to help our customers to secure and manage their information driven world against more cyber risks at more points and more completely than any other company. We are a company that provides solutions for government, for the large and medium enterprises and also for the consumers at large. Symantec believes that all stakeholders have a role to play in addressing cyber security at all levels, given the ever evolving online threat in the environment. Effective information security from our end relies on the multilayered defence against attacks but also recognition that technology alone is not the solution to the problem. Equally important from our perspective is to address the people-related issues through education, training and awareness, whilst also ensuring that our organisations have been effective and appropriate

policies and procedures to address the different incidents when those occur. We are committed to search developing solutions and technological solutions that will help address the online security availability and integrity concerns and also we are committed in supporting the public policy efforts across Europe that promote network information security. In that regard we are very pleased to have this opportunity to be here today and I am more than happy to try to answer any of your questions.

Q138 ***Chairman:*** Where is the company based and who owns it?
Mr Chantzos: We are a global company and we employ approximately 17,000 people across the globe. We have a very big presence in the UK where we have also, if you like, our business headquarters for Europe. We employ roughly 1,000 people in the UK. The company globally is headquartered in Mountain View, California. But, as I have said, we have operations across the globe and if I look at Europe, Middle East and Africa we probably employ a good chunk of our total number of employees in the region.

Q139 ***Chairman:*** Is it publicly quoted?
Mr Chantzos: That is correct. We are on NASDAQ—I think we were listed in NASDAQ back in 1987.

Q140 ***Chairman:*** Dr Nazario.
Dr Nazario: Thank you very much for your time, Lord Chairman. I am Dr Jose Nazario and I have been with Arbor Networks since about 2002. Prior to that I was in biochemistry doing a PhD in the field in 2002 as well. Arbor Networks was founded in the year 2000. We have been a company for about nine years now. I am currently the manager of security research of the company working for the Chief Technology Officer of the company, Dr Rob Malan, who was actually also one of the founders of the company. His research, together with Professor Jahanian and others led to the founding of the company after many years of research into detecting and thwarting denial of service attacks at the carrier scale—the ISP scale. Arbor Networks builds products, among them including the Peakflow product line which helps large providers—so these are Tier 1 backbone providers to the Internet; and Tier 2 providers, broadband providers, mobile providers and many others and large enterprises. We measure their traffic, detect denial of service attacks and filter them out using our products or even partners' or competitors' products as well. We also build devices to provide service control for the broadband edge in our e-Series through an acquisition early last year. Arbor Networks chiefly focuses on the availability part of the information security space. We employ about 270 people around the world. We are headquartered in Chelmsford, Massachusetts in the US, just outside of Boston, with a major engineering office in Ann Arbor, Michigan, which is where I am located. We have people in the UK, in Europe and globally as well. Our customers include large ISPs, including British Telecom and many others around Europe and around the world, as well as governments and, as I mentioned, large enterprises.
Chairman: That is very comprehensive; thank you. Lady Garden?

Q141 ***Baroness Garden of Frognal:*** That is a very helpful introduction. Do you think that the programme set out in the EU Communication on large-scale cyber attacks is going to make any difference to Internet resilience? Or do you feel that this is something which the Internet industry has well in hand already?
Mr Chantzos: I think we need to begin by making a very important distinction. The Commission Communication on Critical Infrastructure Protection is a policy statement; it is not a programme itself, it is a statement of intentions. It is what the Commission would like to do in this particular area. So the first requirement for the Communication to have an impact is actually the Communication to be followed through. It is the Commission to do the different things that it talks about; it is the Commission to do work on early warning; it is the Commission to do work on common exercises; it is the Commission to do work on information exchange, and the ENISA mandate to be reviewed and so on and so forth. There is a list of something like ten items which are foreseen in the Communication. From our perspective we need to bear in mind that the Communication is aiming at first of all raising the level of awareness and the level of security within the Member States and in the work that the Member States are doing with each other. I am saying that because that will indirectly, hopefully, also raise the view of the level of resilience within the European Union. I think it is also fair to recognise that when we talk about a European Union of 27 Member States we talk about 27 Member States that have a variety of approaches and also a variety of their level of development in terms of how they understand issues of network and information security and how they understand issues of critical infrastructure protection. So in that regard also things which are obvious perhaps in London about how we need to be working and collaborating with people like industry, which is what the Commission Communication is calling for, with public and private partnerships, may not be that obvious in other places in Europe. To conclude, (a) the Communication can

have an impact but it needs to be followed through; and (b) the Communication in terms of where it is targeting, its first and foremost audience is we will take the Member States, so the impact that that would be is more likely to be interacting on the overall work that the Member States do with themselves and with the industry.

Q142 ***Baroness Garden of Frognal:*** Presumably coming from industry you have to make the balance between collaboration across industry and competitiveness because obviously you are in business to make profit.
Mr Chantzos: Clearly. From our perspective there are a number of issues when one is looking at this cross-border collaboration. Is cyber security, is critical infrastructure protection a pan-European problem? Absolutely. Is critical infrastructure an area that the industry needs to be working on? If I just look at the telecoms environment it is fully liberalised, so from that point of view the infrastructure is owned by the private sector and therefore it is a question of public/private partnership in collaboration. At the same time no single industry has the solution to the problem but also when we talk about collaboration we need to make sure that (a) we do not violate our competition obligations in collaborating; but also that there is the framework in place to do collaboration. What do we mean by that? Collaboration, examples like information exchange, exchange of best practices, building of trust require a framework to do that conversation at European level. The framework does not necessarily exist. They require the financial incentives to do that at a European level which also would exist; but most importantly they also require the legal basis or at least the lack of legal obstacles to be in place at European level in order to be able to do that. When it comes to legal obstacles, for example, if I can give a very concrete example for your Lordships' consideration, data protection legislation. The way that we implement and understand data protection legislation in a country like the UK, whereas in principle it is harmonised, may be somewhat different to what we understand it in a place like Sweden. So whereas you may want to have a country like Sweden and the UK cooperating, on the other hand you need to be thinking very carefully as to whether you are doing something which in terms of information exchange that UK and Swedish law would allow.

Q143 ***Chairman:*** Dr Nazario, do you want to come in?
Dr Nazario: The programme described by the EC in the report earlier this year will, we believe, start to make a difference, although it is insufficient in some respects. The goals or the descriptions that Promis has outlined, all of which we agree with in principle based upon our experience with regard to public/private partnership, regarding the role of CERTs and regarding the role of the need to harmonise legislation for providers and for security in mind, as an example, all of these are key instruments as well as data sharing. However, it is vague in many places and it is incomplete as well. I would have liked to have seen it, based on my own experience, suggest more cooperation, for example, with the existing organisations, such as FIRST, and really stress these participations, as well as some of the other larger organisations that have emerged over the years to provide either industry-wide or operational communities and stressing these as points of cooperation, in particular for the public-private partnerships as well as models of how the data might be gathered and shared. So it is a broad outline that we agree with in principle; we figure it is a decent foundation but insufficient to really be a complete impact.

Q144 ***Lord Richard:*** Could I take up the second half of Lady Garden's question where she said is resilience something that the Internet industry has got well in hand already? Do you have it well in hand?
Mr Chantzos: So let us take a step back—in what sense? We talk about Internet resilience but what do we really mean? Do we really mean whether the Internet is in a position to withstand a major attack? I would answer that the Internet is probably one of the most resilient networks that has ever been built. I would argue that the Internet has been designed to withstand a nuclear war; so from that point of view the work that the industry has done around the Internet is actually quite good. There have been incidents where there have been large-scale attacks against the Internet infrastructure and also there have been incidents which have been literally accidents that have to do with Internet infrastructure. For example, I remember that there has been an incident whereby an anchor of a ship was dropped off the coast of, I think, North Africa, and as a result it cut the underwater sea cable and basically lost connectivity. Is that an issue for the industry to address? We are dealing here with the situation of an accident and maybe there should have been more resilience for more alternative routes to channel that. So, from that point of view, it is a question of economic efficiency—do we need, do we have, should we have? The enemy of the good is the better and I would argue that the industry has already done some good enough work but it is not just industry issues that need to be addressed, and it is also a question of a risk management approach.

Q145 ***Lord Richard:*** Can you tell me what work it is that the industry has done on this?

Mr Chantzos: Before I answer the question, however, for what kind of industry would you like me to focus on? Would you like me to focus on ISPs? Would you like me to focus on our industry?

Q146 ***Lord Richard:*** Yes.
Mr Chantzos: For the industry at least that I can speak of, when I look at the security industry, our work around resilience has primarily been in trying to make our software much more efficient and as much as possible least vulnerable. So if I look at the work that we have done I can point to activities around a number of companies in order to make their software less vulnerable, either through software management life cycles or through engineering and processes within the software building capabilities of the companies in question. I can point as well to organisations like SAFECode, which are designed to bring the different parts of the industry together in their changing best practices on how they can build the applications that will either run on the Internet or protect the Internet from being more vulnerable.

Q147 ***Chairman:*** It may be that you would feel after this session you would like to provide a supplementary paper on this.
Mr Chantzos: Provide more data on this; sure.

Q148 ***Chairman:*** Dr Nazario.
Dr Nazario: I would like to focus on the ISP operator community aspect of it, both from a security as well as a simple resilience model. Every day we see attempts at attacks against protocols, against infrastructure—what we call the protocol stack of the Internet. So anything from physical wiring to how it is carried, all the way through to applications such as email and the Web browsers. This is a stack of protocols designed to be resilient; it can be affected at one point or another and even remedied at one point or another, which gives it a tremendous amount of flexibility. However, in this complexity we do see some risks. In large measure the operational community is able to quantify these and actually remedy them either by working with major vendors like Cisco, Juniper and others, or in forums such as ICASI, or even in some *ad hoc* forums, for example around the recent SSL vulnerability; to be able to investigate fixes and to apply these fixes as quickly as possible for operational and business continuity. Natural disasters have occurred as well as some man made accidents, as well as operator error. A good example of operator error is the incident where a Pakistani ISP attempting to filter YouTube traffic for its domestic users actually affected YouTube traffic for the entire world through a mis-advertised route. The Internet was able to respond within a matter of hours, both detecting it and attempting to address it, again, because of the complexity of the protocol stack and the resiliency within there. Outages such as power outages or cable cuts again can be routed around the Internet and can be accommodated almost immediately by the Internet infrastructure, as well as in the near term adding capacity by simply laying new cable or building new connections. And attacks, for example, against routing servers or key exchange points have all been dealt with and put in hand again partially by the redundancy build in the network that automatically kicks in, as well as the operating community discovering the attacks and filtering them out as quickly as possible by discussing the attacks, sharing data and applying filters as needed. Again, some resilience is built into the community that is there but there are gaps unfortunately because in some cases they do not have the investment that they want to make, that they can make because of, for example, how long-term it might be or how strategic it might be compared to immediate business concerns. So there are some fundamental risks there and there are of course challenges with the number of players and some of the fundamental vulnerabilities such as in DNS or SSL protocols and coordinating all of that to represent themselves provide real challenges ahead for our industry.

Q149 ***Lord Richard:*** I would perhaps make a comment which is that really what you are saying to us is that on the whole the industry is coping but that if certainly additional things were done—not great things—within the compass of the industry that it should be all right and you do not need anything like the EU intervention to improve it.
Dr Nazario: I believe that you used a very apropos word by saying "coping". I think that some assistance would be valuable; I think that some coordination might be valuable to facilitate what many people want to achieve or would wish to achieve. I think that might be valuable to bring to the organisations.
Mr Chantzos: If I may comment? If I look at examples like, for instance, the Conflicker virus. That was a very good example whereby the industry stuck together. The so-called Conflicker working group worked through the possible fixes and came up with a solution very quickly. If we look historically at cases of attacks against the DNS servers, whereas there have been attacks, let us say, in three out of the 14 DNS servers have we been witnessing any significant impact on our Internet experience? None at all. From my perspective I think to turn round and say if we do a few things then everything is going to be fine, I would argue that it is perhaps a somewhat simplistic way of addressing the problem. Why? First of all, the threat landscape is changing all the time; it is evolving. Doing a fix now does not mean that it will work in three months from now. In some ways it is an arms race; it is trying to figure out what the next move

is going to be. So rather than trying to apply just the technological fix or just pump more money into the system, I think it is important that we also try to address some more of the fundamental roots of the problem. On the other hand, I do believe in the value of coordination and cooperation as being an element of the overall mix and I think that this is really, if I see it from an EU standpoint, what the EU would like to try to push forward, and from that point of view, frankly, we would welcome that Communication and we would be supportive of it. To comment on something that Dr Nazario said, that the EU is vague, I take the point that it may be somewhat vague, but I would also like to remind all the people in this room that the EU may be deliberately vague for some very good reasons. In what sense? First of all, when you do your policy statement you do not necessarily want to outline all the bits and pieces, especially if that policy statement is dependent upon the consensus or the cooperation of 27 sovereign governments. In addition to that, let us not forget that when we are talking about information security we are talking about the issues that impinge upon national sovereignty, which impinge upon issues of national security and which put in question how much role and how much legal basis the EU has to act and up to what level. So I would argue that there are very good reasons why the policy needs to be generic because ultimately it needs to be a policy which will not supplement the role of the national governments and the role of the sovereign government in this particular case. It needs to follow the principle of subsidiarity.

Q150 ***Lord Harrison:*** I wanted to drop anchor, my Lord Chairman, on the Mediterranean anecdote. Did anything change? Was the change, for instance, to ensure that there was the concentration of lines for the Internet so that there could be more resilience in the future because there were alternative ways round? Did it make a change in any way, shape or form?

Mr Chantzos: I would need to go back, frankly, and look at how the issue has been addressed since because we are talking about an incident that happened a year, a year and a half ago. I do not represent an ISP so I would not necessarily be privy to all the routing changes that may have happened. Having said that, there were a number of emergency measures taken to re-route the traffic in order to allow for more capacity as well. Obviously there was an issue of outage for some hours when the incident happened, but I think that overall if you look at the bigger picture, let us say, short of literally physically coming and cutting the cable and then trying to find an alternative route and in the end being able to serve that route, I would say that the issue was addressed adequately. The question is how likely is it that in the whole of the Mediterranean Sea a ship is going to come and drop the anchor over the undersea cable? Frankly, when we come to talk about security this is the issue of what I call a risk management approach. So what is the level of risk? What is your risk appetite? What is the level of risk that you are prepared to take? If you are prepared to take a level of risk as to how likely it is that there will be a ship that would aim with its anchor on our cable, then if you are not prepared to take that risk then maybe you need to lay another cable, but that means that you need to be prepared to pay the ticket and the price for that cable. But if you consider that unlikely—let us think about it, how long have we had the Internet now, 20, 30 years—that we have had in 30 years one ship cutting a cable, maybe that is an acceptable risk. There will not be such a thing as 100% security ever on anything, so in the end that is what we need to balance and that is the investment decision for the industry and also for the government.

Q151 ***Lord Hannay of Chiswick:*** A lot of the evidence that we have received indicates that the issue of security tends to be addressed at the national level, as you yourself have just said. It is the realm of the 27 Member States. Or, alternatively, if it is addressed on a multinational level it tends to be so on a wider basis than just the European Union, and the Communication that we are looking at is pretty vague, to put it mildly, about how to bring the United States, Russia, China and other big players in. Could you say a little bit more about what you think the role of a regional organisation like the European Union is? Is there space for it between the national work that is going on, with Britain setting up its own cyber defence and so on, and the global work that needs to go on in order to provide resilience to what is, in fact, a global asset? Is there a space in between or is that space not really there?

Mr Chantzos: To put it in a very simplistic way, I believe that there is space and I believe that there is room and a role to play and I would even go as far as to say that they are not mutually exclusive. In what sense? As I said, there are interesting discussions and there will be even more interesting discussions now that the Lisbon Treaty is coming into effect in Brussels as to what is the role of the European Union in this particular area. Having said that, I think that the legal basis on this issue has evolved over time and the EU has a role to play in terms of taking care of its own Member States, while acknowledging that this is a global problem. As I said before, the Member States have a different level of development. If I can bring in a very good example and if I look at my own country, Greece—I am a Greek national—it does not have, at least right now, a national government CERT, whereas in the UK you have been doing work and you have been advancing the notion of having

CERTs, specialised CERTs within the industry, and having a government CERT, having an MoD CERT and so on and so forth. Greece has been a member of the European Union for 30 years now and within the Euro Zone and within the Schengen Treaty, et cetera. So it is a question of the different levels, if I can use the term, of development, the different levels of advancement; and the different levels of focus that the different Member States have. I would argue that the overall European Union security collectively, including the UK's one, would be benefited if all the Member States would get up to a higher level of security. That does not mean that the UK would have to lower its level of security, but it would suggest at the very least that we can, if I can use the term loosely, drag the rest to a level that would be able to have the rest of the Union talking the same language and have a common understanding about the threat. If I can give you an example that Symantec has done in this area. Symantec was awarded a grant as part of the work—and we had a press release about this, so it is publicly available and I can share this with you—on a programme that would define standards that would facilitate secure messaging about vulnerabilities, threats, incident management and good practices across the European Union and across the different CERTs. That was funded by the European Programme on Critical Infrastructure Protection; so that was EU money that was given to Symantec partly and other partners to co-fund a messaging standard that could be used among the different CERTs, government and private sector or other bodies interested to take up that standard in Europe to exchange information about the attacks that they are seeing, which is not a bad thing. I would argue that is in line also with what Dr Nazario just said in terms of being able to say, "Okay, we understand this is happening; you guys say the same thing, so what are we going to do about it? Are we talking the same language; are we talking about the same threat?" Is there a role for the US? Of course there is; absolutely. The same whether there is a role for the UK from subsidiarity and from a national sovereignty standpoint. The activity of the EU is not replacing a Member State—I certainly hope it will not and I certainly do not think that this is the intention of the Commission, at least at this stage. Do we need to be talking to the Americans; do we need to be talking to the Chinese? Of course we do, but we need to be doing that at national and European level. It is just that right now the EU needs to start from somewhere and it does that by taking care of its own house.

Q152 ***Chairman:*** Dr Nazario?

Dr Nazario: We concur with regard to the fact that the EU has a major role to play; it is a common economic system, with common political goals, and a common social community as well, even though there are of course many distinguished Member States each with their own distinctive voices. There are, of course, shared goals and economies. Engaging with the US is going to be key, I think, for connectivity purposes—no nation is an island on the Internet—and they are all tied together as well from the standpoint of supplying resources, both operational resources as well as software resources. So being able to communicate as a single economic voice or a unified voice to software vendors around the world will have a significant impact at raising, for example, software quality standards and software features. That will be very, very important as well and it is something that I would encourage the Commission to examine as a mechanism to improve security for the Member States through these relationships. There are, of course, challenges in some regards to language issues as well as to shared standards. As an example, many of us have some difficulties reaching effective partners, for example in China or in Russia, to be able to begin to address common problems. Those barriers are coming down by simply meeting people and making introductions. We have very similar goals but those barriers have an historical foundation that is going to be very difficult to overcome in some regards. We all recognise that we have very similar goals and we all want to achieve very similar things. You must work with the rest of the world, including the US, Russia and China to achieve those goals—it cannot be done otherwise.

Q153 ***Lord Mackenzie of Framwellgate:*** Could I move to a more practical case study and could you give us your understanding of what actually happened during the so-called cyber wars in Estonia and Georgia?

Dr Nazario: With regards to Estonia these events occurred in large measure in April and May of 2007. Arbor began receiving enquiries from partners and friends in Europe, including Finland and Germany on behalf of the Estonians. This included private partners, such as F-Secure, as well as FICORA and other folks, ISPs included. We were carrying some of that traffic and seeing some of that traffic and wanted to know what we had been seeing and what we could do to help the Estonians, so we began digging into some of our data. We have a programme called ATLAS, which is a global honey-pot system, which ties together a number of different data sources, including shared data from our Peakflow monitors around the world as to the nature of the attacks, the scale and duration, as well as botnet tracking, where we can understand the origins of some of those attack commands—who may be behind them and what tools they are using for some of those. So we were asked to bring much of this data to bear and to assist and we actually wound up deploying some of our

gear with the Estonians to help to filter out some of the traffic, as did many others including Cisco. We shared equipment to help them as well as resources to help them address that. What we observed in Estonia, as we have written about in the past, were non-state actors, responding to what we anticipate to be non-state actors, or interpret to be non-state actors, acting largely in a sympathetic manner to the political tensions between Moscow and Tallinn over the movement of the statue. This was a very tense issue. We do not have any evidence that we had gathered that would suggest anything much more serious and that is one of the things to keep in mind here, that these attacks, both in Estonia and Georgia and many other places around the world, follow these diplomatic tensions—they do not generally lead them. So by the end of May—in fact after Victory Day, May 9—the attacks began to dwindle and we saw coordination and forms and blogs that they tracked; we saw a number of tools used, including botnets and handwritten tools and custom written tools and scripts designed to watch some of the attacks, coordinated and called for by many different parties largely in the Russian language world. So that is much of the former Soviet Union. We saw significant attacks. The attack scale themselves that we measured was modest by global standards but was in fact significant for Estonia's resources. In Georgia we actually tracked attacks going into Georgia's President Saakashvili's website in mid July during some of the build-up to the groundwork of August 2008. We actually had some difficulty reaching the Georgians to alert them of this fact, which I think highlights some of the challenges across Europe with regard to the unevenness of response capabilities. We worked in large part through the Estonians to help the Georgians actually detect and filter some of the traffic and some of the resources from Georgia were moved to the US as well as to Estonia, where there were better capabilities to filter out the attack traffic. The attacks in Georgia we detected were larger in magnitude but again still modest on a global scale, and lasted a bit longer than the ones in Estonia. So we saw a maturation, if you will, of the process that had begun far before Estonia but really hit the global stage in Estonia in 2007 and 2008 in Georgia.

Mr Chantzos: Being a barrister I would like to choose my words carefully. You referred to cyber war. I would somewhat question that because war and acts of war have a certain meaning within law and have a certain meaning within the Geneva Convention and have a certain meaning as how we understand it. I am saying that because, as Dr Nazario has pointed out, it is very difficult in the Internet environment to do threat or attack attribution, basically to say who is to be blamed for something.

Q154 ***Lord Mackenzie of Framwellgate:*** I did use the term "so-called" cyber warfare.

Mr Chantzos: Indeed, but as this is a public record I will be on record as being cautious about it. We have seen a number of discussions and I have attended conferences like the one organised by the NATO Cooperative Cyber Defence Centre of Excellence in Estonia, whereby what has been debated is things like the nature of if there is such a thing as a nature of cyber war what would cyber war look like? How likely is it that we are going to have military conflicts with cyber elements, et cetera? So have we seen large-scale attacks on IT systems in particular countries, such as in the case of Estonia and Georgia? Absolutely. Our role in those cases could have been much more focused around things like understanding and identifying the nature of the malware that has been used in deploying the appropriate counter measures to be able to basically remove the malware from the infected computers. We have seen an increase of botnet activity targeting specific countries. Most botnet attacks will be spreading all around the world and so, technically speaking, there were European countries, for example, attacking Estonia through the botnets whereas it was not necessarily, let us say, the countries themselves rather the computers had been taken over and were successfully compromised and were used by third parties to launch those attacks. In terms of the history of how the attacks occurred and materialised and their timeframe, I do not disagree with Dr Nazario. In fact what has been in the press is quite well known—political tensions either because of a particular part of Georgia, in the case of Georgia, or the removal of the statue in Estonia and then this climax of reaction also on the Net. What it is important and interesting to highlight is when it comes into a discussion about how these attacks were organised and coordinated and about the power that the Internet has in terms of growing a grassroots campaign. How quickly within the Internet the word of mouth or the different communities can be called upon for that action to materialise and manifest in some kind of a protest—mass emailing in terms of reaching out to constituencies and expressing concern and opposition or, in this particular case, into the activities that we have seen.

Q155 ***Lord Hannay of Chiswick:*** Could you throw any light at all on the allegations that have surfaced in the last two or three weeks about the attacks that were made on the University of East Anglia's material on climate change, on which there have been quite serious allegations that these attacks originated from Russia and were politically motivated. It is, of course, slightly different from the Estonia and Georgia case because it is not an attack designed to take out—it is an attack to gain access to and then make use of material that belonged to somebody else.

Can you cast any light on that? Perhaps at the same time you could also, dealing with Georgia and Estonia in particular, try and throw a little light on this matter? Nobody, I think, has yet suggested that the Russian state was involved in the attacks on Estonia and Georgia because there is no evidence of it. On the other hand, presumably the Russian state has some capacity to interdict actions from its own users, so even if you accept the view that this was a lot of patriotic right-wing Russians sympathising enormously with what Russia's policy was in Estonia and Georgia, is there not still another question behind that which is why has the Russian state not done anything to inhibit people doing that? So even without going into the conspiracy theory that they are manipulating these people for their own purposes, you still surely have a question mark about why they are not doing anything to inhibit it. Could you throw any light on this?

Mr Chantzos: Two thoughts on this. I would like to understand more about the East Anglia attack that you mentioned. But if I look at the way that attacks happen on the Internet a lot of focus has been put on attacks which are examples of, let us say, denial of service because these kinds of attacks are very visible—something does not work. If you realise that you do not have connectivity people can access information that you have. So from that point of view it is immediately realisable. However, a very significant amount of attacks is not about disabling the infrastructure by the denial of service, but rather it is about collecting confidential information. If I look at the latest Internet Security Threat Report, which is the annual report that Symantec produces on the current state of the Internet threat, it is roughly 150 pages long and I believe that in our submission we have shared some of the data and should you want additional data we are more than happy to make that available—and we publish it once a year. If you look at the Internet Security Threat Report I think roughly 87% of the top 50 new malware, new viruses that have been produced aim at stealing confidential information. So in many ways the *modus operandi* of an attacker will very often be information-centre driven. Why? Because the information has value, so it will very often be around stealing information. The same tools that are designed by cyber criminals in order to steal confidential information are the same tools that can be used also for some kind of espionage—economic or otherwise. From that perspective again, as I said, short of literally doing forensics and following the forensic trail on the attack in question, i.e. doing physical and online investigatory and forensic steps, it is really difficult to tell who is behind that or any other attack of this nature. The same tools that can be used to steal your credit card numbers can also be used for stealing business secrets. So I hope that addresses East Anglia.

Q156 ***Lord Hannay of Chiswick:*** On reflection after this session, and because it is now a matter of extreme interest to a lot of people, if you were to come across more material it would I am sure be helpful to us, if you could make that available. We have to grapple with the fact that now there are three possible incidents in which there seems to have been some concerted action taken from a Russian base. Whether that was a Russian state base or a Russian individual private base, so far all the evidence is the latter rather than the former, but that, as I say, does not actually answer all the questions.

Mr Chantzos: My Lord, just to give you an idea of the magnitude, if I can use numbers, we are talking malware, we are talking about a virus stealing information, back in 2002 we had 20,000 new viruses a year, last year we had 1.6 million new viruses. We project, unofficially—and we will have the numbers officially hopefully some time soon—that we will be looking at roughly, possibly—please do not hold me hostage to the number—three million new viruses this year. The way of the writing of the viruses, the way of the writing from malware, to be technically correct, is done is so that it evades detection; it goes through the same software engineering process that business products, technology, commercial software is going through. You can literally go and buy online the malware and use a licence agreement with it, which promises you updates of the malware and which will be null and void should you give the copy of your malware to the security industry—us. In many ways we are getting now to the point whereby every time the malware writers discover a new vulnerability they write a new form of virus and then they take that new form of virus and create hundreds of variables so as to try to avoid detection. The argument that you make that it seems that it is coming from country A or country B, I fully take the point; but if I could point to another statistic and look at the Internet Security Threat Report, global United States is the top attacking country across the world—top attacking country, so number one in malicious code rank, number three in the amount of zombies, and number one in the amount of phishing websites. Number one in terms of attack of origin. That does not suggest, obviously, that the US is attacking the UK rather what it does suggest is that the way the cyber space is designed it allows for people to be able, unfortunately, to take over other people's computers and utilise those to launch attacks remotely and make detection much, much more difficult. If I can use a different regulatory example, of which all of you may be aware, the whole reason why there is an EU data retention legislation and the whole reason why ISPs in the UK and in other countries around Europe are expected to retain data for a period of months to assist law enforcement investigations is to be able to follow the forensic trail. It is to be able to go back and say, "Whoops! We think

something happened and we need to have the data in order to be able to go back and go back and go back." But even that trail is going to go cold the moment that you go to a country which is unwilling to cooperate.

Q157 ***Lord Harrison:*** With all the qualifications about the term "cyber warfare" should we be looking to NATO for help as well as the European Commission about the protection of the Internet?
Mr Chantzos: Each one of them has a role to play, my Lord.

Q158 ***Lord Harrison:*** What would be the balance of that role?
Mr Chantzos: I would submit the EU is having more of a role in the civilian side of things. Clearly the whole work around critical infrastructure is about basically protecting infrastructure which is critical for our society but is actually run by the private sector. I think it is a question of proportionality. In what sense? If you look at countries like the US they have developed a Cyber Command. If you look at NATO we are talking about the Cyber Defence Management Authority, and obviously within the NATO Communications Security Agency (NCSA) NATO has a certain set of capabilities in this area. In the end it is a question of doctrine and proportionality. In what sense? What would you define as a military threat or a military incident that would justify a proportionate and appropriate military response? Would it be an attack on the critical infrastructure that would be so critical that it would disrupt and threaten, as you define it, national security? Would it be the fact that military facilities are being attacked? Would it be a combination of both? There is clearly an element whereby it is for the industry, for civil society, and for law enforcement to work with this, and then perhaps there is an element whereby it is a combination of all of them together, and then an element which goes more to the security services defence part of the overall security operations. There is no quick, simple answer because there is no clear demarcation line.

Q159 ***Lord Harrison:*** Could I ask Dr Nazario for his answer. Is there any evidence of the European Commission or the EU talking to our NATO colleagues about this?
Dr Nazario: I am not aware of any, your Lordship, but I am not privy to all the communications between the EC and NATO. I concur in large part with Mr Chantzos' splitting of the problem with regards to the bulk of it should be borne by the EU on the civilian side and there is certainly a role for NATO to play with potential military threats. There are many questions that are being asked by NATO with regards to whether they should be engaged and whether they should invoke the common defence articles with regard to some of these questions. There are very many unanswered questions there with regards to whether these threats rise to that level—proportionality again. Mr Chantzos correctly alluded earlier to many of the challenges that we face with his remarks around the Geneva Convention and the laws of war. I am not qualified to answer. I am just an interested observer in terms of those debates. I do know that there is a tremendous challenge with any outside party whatsoever, whether it be the EU and EC, or whether it be NATO coming in, for example, and assuming control of a network, only because of the complexity of anybody's network. Network technology is so bespoke in some cases for the very large traffic providers, the configurations are so finely tuned and tailored any outsider who comes in, no matter how qualified, is very liable to do some damage initially through accident. A supporting role however is certainly going to be very, very crucial here, to build bridges and provide expertise and assistance in those areas, to expand capabilities, to expand reach and to expand experience, and there I think the roles of the EC and the EU as a common defence area as well as NATO certainly have a role to play. I also could not hope to address the disjointed nature of NATO membership and EU membership. That is another challenge in this regard.
Mr Chantzos: Two things very briefly on the point that you mentioned. My understanding is that in the press there has been information about senior level contacts between the EU and NATO. For the record I think that is relevant to mention. I would point again to the legal basis of the EU. Issues of national security and national defence are not Community competences. I would also highlight the point that the membership of NATO and the membership of the EU are somewhat different, so that is also something that needs to be considered.
Chairman: Thank you very much. Lord Dear, would you like to maybe combine two questions. I am just watching the clock and we must move on.

Q160 ***Lord Dear:*** Indeed, gentlemen, you have already dealt with resilience and I conclude from that, if I am clear in my own mind—and correct me if I am wrong—that you think the internet structure is certainly vulnerable but you think it is highly unlikely that you could bring it down completely, either by botnets or natural disasters, ships with their anchors and all the rest of it. Would you like to put some sort of percentage on that, by which I mean if the total internet cannot be brought down in its entirety, what do you think is the worst case? Would you see 20%, 30%, 40% as the maximum damage that could be occasioned, or is that an impossible question?

Dr Nazario: It is a challenging question, your Lordship. If you look at the internet background structure there are some interesting features to it, for example in how autonomous networks are connected to each other. Through accidents of market and natural forces there are tremendous amounts of consolidation to a few key players, globally and regionally. If there were, for example, a catastrophic exploitation of vulnerabilities within one of those key players, you might see a reasonable amount of the internet lose connectivity to the rest of the world and even to each other in large measure. We have seen certainly with the case of the FLAG cable cut by the boat anchors parts of the continent of Africa lose connectivity or have greatly diminished capacity which effectively reduces their internet connectivity to zero.

Q161 ***Lord Dear:*** It may be a naive question but would you like to put a figure on that?
Mr Chantzos: I would go further than Mr Nazario and I would say that you are giving me an impossible question to answer. The reason why is because Mr Nazario is seeing it from an ISP perspective and I am seeing it from the security provider perspective, if you like, and from that point of view we would begin an endless discussion as to first of all what kind of attack are we talking about. For example, if I look not from the point of view of bringing down the internet meaning there would be no connectivity but actually hitting and attacking the nodes, ie the different end points, the different computers, your PC, my PC, Joe Bloggs' PC on the street. Is there potential that there would be a major malware, a major virus which would go out and hit all those machines? Well, yes, we have seen those in the past, but it would not mean that the internet would not work. Rather it would mean that the end point of the internet for some, presumably many, could potentially be infected at a very high speed. Have all of us survived those kinds of attacks? Absolutely, but, then again, can there be an attack which for example had a virus infecting the end points and then telling them to shut down or not work or whatever? Yes, that is possible. Then to challenge you in a different way, I would ask you why would an attacker do that? What do I mean by that? If I think about it from his *modus operandi*, hacking now is for fortune, it is not for fame. Attacks are financially motivated. At least the cyber criminal ones are, which is the vast majority of attacks. It is in my interest to have the network up and running so that I can steal information which I can then trade in the on-line black market, so I would rather have it on and running and me acting like a biological virus, like a mosquito that goes underneath your defences and sucks your blood, because if you realise that I am there you are going to swat me and I will not be able to make money any more.

Q162 ***Lord Dear:*** I am grateful, thank you. Perhaps a slightly easier question to answer, although it does touch on the whole global issue, and I am conscious of that when I ask you, how well do you think the UK is doing, bearing in mind the UK is a player in a much more fluid environment? Is it possible to isolate the UK and say they are doing very well, well, could do better? Is that a question that is impossible to answer as well?
Mr Chantzos: I think it is possible. I would answer that the UK is doing quite well. I would answer that the UK is doing quite well because if I look at the statistics historically that we have been gathering over the years, there was a time, four years ago I think roughly, that the UK was top of the amount of attacks that were launched from the UK. I think now the UK—

Q163 ***Lord Dear:*** Which were mounted from the UK or—?
Mr Chantzos: Launched from the UK to other countries, which means that basically there were perhaps too many machines in the UK that were infected. In fact that is normal if you look at the sheer numbers of population and the broadband enablement. This is also why countries like the US or countries like China feature top in the number of attacks. The sheer number of broadband users is such that it is numerically impossible not to be somewhere high on the list, but if you look at the UK, the UK was up and now the UK has gone significantly down that list of top attackers. Considering the amount of broadband penetration this means actually the UK has been doing quite well. If you add on top of that the advances that the UK has made from a public policy stand-point, so if you look at the awareness with activities like Get Safe Online, if you look at the awareness within government and the public sector with activities like the *Digital Britain* report and the Cyber Security Strategy, the creation of the Co-ordination Centre within the Cabinet Office, the security operations part within other government departments, I would say that the UK is doing quite well and is also quite advanced. Then again, as we said, the threat landscape moves so it is an evolving process.

Q164 ***Lord Dear:*** Dr Nazario has been nodding as you said that. Would you agree generally with what has been said?
Dr Nazario: Yes. I am just looking over our third quarter report for the European Union, which includes Great Britain along with a number of its peers in the region. Great Britain is doing very well. This is across a number of different axes including denial of service attacks, inbound and outbound, the number of infected PCs, and the number of malcode hosting sites. This is a handful of metrics that we

collect that we can provide some insight on this. The number of infected PCs within Great Britain appears to be pretty well-managed. On the number of denial of service attacks, inbound and outbound, unfortunately they lead in the European Union, according to our measurements. On a global scale they are at number three for the quarter. The attack size is six gigabits per second peak size and about 40 gigabits per second for the largest for the quarter that we saw globally, so it is pretty substantial in most regards when you think about just denial of service attacks, inbound and outbound. Those are generally well-managed by the providers and the operators here in the UK. The number of infected PCs, so this is the number of consumers for example that are affected by information-stealing viruses as well as proxies for other nefarious activities is relatively small and well-managed. I would attribute this to being well-connected with regards to the security operations community, ISPs and CERTs, so they have well-trained staff, they have adequate resources and they have data flowing continuously in and out to help them discover and manage the problems.

Q165 ***Baroness Billingham:*** Gentlemen, is the internet safe for consumers to use and will this Communication make any difference to that?

Mr Chantzos: The Communication, as I said, is intended to stimulate and promote co-operation within Member States and within Member States and industry, so the Communication in principle is not addressing or dealing with consumer issues. If, let us say, governments work better together and the industry works better together with the government, the theory is—and I would imagine the practice would be—that the consumer would also get benefit. Having said that, is the internet safe for a consumer to use? The on-line world is a reflection of the off-line world, I would argue, so the level of security that we have in the off-line world and the level of security challenges that we are facing in the off-line world are similar also to the level of security challenges that we are facing in the on-line world. In the same way that I would not pick up someone from the street and tell him I trust him and give him my credit card and tell him to go and do something with it, I would not do the same on the internet. In the same way I have locks in my house and I lock the windows in the evening and do not leave the door open, it is pretty much a similar approach. Security is a question of people, process and technology, so whereas you cannot expect the consumer to be 100% responsible for his level of security, you also need to have an expectation that he will do what the *bone patres familias*, the reasonable average man would do to protect himself, as I said, off-line or on-line. It is a question of having the proper technology in place. The most well-known Symantec technology in this area is Norton AntiVirus and Norton Internet Security, but I would also turn it round and say it is also a question of us, the industry, the government, trying to make aware and trying to educate people about the security threat and the security issues that exist especially for the more vulnerable parts of the population, children or older age groups, to try to make sure that they understand that when they are connected on the internet just because they are behind closed doors and in the safety of their home, it does not mean that they should not take some reasonable precautions when they are on-line. A number of security incidents occur because of ignorance. People not understanding the value of their personal information and just putting it up on social networks, or doing things like clicking on email attachments from people they do not know, so a lot needs to be done in that area, and I am pleased to say the UK with activities like Get Safe Online is very far ahead.

Dr Nazario: I would concur with much of that. It is important to remember, though, that our experience has shown that as CERTs become stronger in a country and gain more traction, that consumers benefit directly and indirectly out of that. Even though the policy and recommendations set forth so far by the Commission are focused on a national infrastructure at that level, I think that there is going to be a tremendous benefit that will reach the end consumer. I concur also with Mr Chantzos that consumers of course need to become better educated but they also need to recognise that the security is very reflective of the real world. Part of the challenge we have seen constantly in this area is that technology at this point is still "magic" for many people. That is not unreasonable. It brings out the idea of the reasonable average man. Just as we do not expect all drivers to understand the complexities of mechanical forces or Newtonian physics, they will drive safely for a number of different reasons, including mechanisms built into their car as well as certain aspects of physics. Here it is not necessarily so obvious, and the fact that your credit card information, for example, has been pilfered and sold on-line is not immediately obvious to you until it is too late, so there are some challenges there, but I think in large measure there will be some benefit to the end consumer.

Q166 ***Baroness Billingham:*** Could I ask a short supplementary. We have used the term here "consumers" and there is such a variation. We have already talked about heads of state as consumers. You could look at me as a consumer. If there were a cyber attack on my computer at the moment the only information you might be able to glean from it is the size of the turkey that I have just ordered from Marks & Spencer's. I have to say to you that we do have a responsibility. Within the EU all Member States have a responsibility to all levels of consumer, from the

most basic to the most sophisticated. You have already made this point very clearly, the need for people to be made more aware and to protect themselves to a certain extent. I am just wondering if within this piece of work that we are now looking at there ought to be built in some more awareness-raising features to ensure that everybody becomes more certain and more aware of what they ought to be doing in order to protect themselves at whatever level they are using it.

Mr Chantzos: Frankly, I would not disagree with you about the importance of awareness-raising. I cannot stress enough how important it is to make people aware of what the security threat is. Also because in many ways awareness is a bit like a marketing campaign. In what sense? You need to keep reminding people and you need to keep educating them. Also different threats or different societal aspects of those threats arise all the time. Cyber bullying is a very good example of an attitude that we did not have in the past. Because of the advent of social networks, with the teasing the kids do at school, suddenly an issue between two kids can suddenly become an issue for a whole community of kids. There is very much an issue of education. It is an issue of the education of children themselves as to what is appropriate ethical behaviour. It is also an issue of education of parents, of teachers, of caretakers, so it is wider community issue. On the other hand, if I look at the way, frankly, the division of work within the European institutions is done, I am not that surprised that the issue of awareness-raising is not necessarily contained in this specific Communication. Having said that, if I look at the work that the EU has done in this area, I can point to the specific awareness programmes of the European Network and Information Security Agency. I can point as well to the Internet Safety Action Plan and the Internet Safety Action Plan Plus, which are all about providing even the funding mechanism for call lines, for testing products and basically building helplines and mechanisms which identify the proper content, which test different technologies, and try to raise awareness around these issues.

Baroness Billingham: Thank you very much.

Q167 ***Chairman:*** Dr Nazario?

Dr Nazario: I think there is room for that type of programme within the recommendations when you think about best practices for CERTs which hopefully would include replicating programmes such as Get Safe Online, educating the public and, as I mentioned earlier, pushing for more secure software from vendors that the consumers will eventually use.

Q168 ***Lord Richard:*** In the Communication from the Commission where they talk about CERTs they seem to be moving in the direction of advocating national CERTs rather than sector CERTs or industrial CERTs or indeed company CERTs. We had some evidence from two people who run CERTs, if that is the right word for CERTs, or who are involved with their running. Do you think CERTs are useful and helpful?

Mr Chantzos: Yes.

Dr Nazario: Yes.

Q169 ***Lord Richard:*** We can all read that, we got that. Do you have any view as to what sort of CERTs would be most useful? Do you think that the Commission idea that you have national CERTs would be easier for you to work with than the present structures that you have got in the UK where it is sectoral?

Mr Chantzos: I am not a Commission official so I cannot interpret what they say authoritatively and say why the Commission is doing what it is doing. Having said that, I think the reason why the Commission is approaching this issue this way is because, seeing it from their perspective, they would like to raise, allegedly, the level of security within Europe, and they need to start from somewhere, so rather than going and saying, "Banking sectors across the European Union need to have their own CERTs," they are probably better off saying Member States need to have their own CERTs because, as I mentioned, some of them do not even have that. It is necessary to begin your awareness campaigning from that point of view. Having said that, personally I can see the value of the sectoral system and I would argue that at the stage of maturity that the UK is, the sectoral system is the way to go. Why? Because different communities have different risk appetites and have different security requirements and, as a result of that, different security profiles, which different sectoral CERTs aim to serve. That was very brief from my end!

Dr Nazario: I would concur that CERTs are very valuable. My interpretation, again not being a member of the Commission, was that it was the most tractable and the most beneficial place to start. I do like sector-specific CERTs. I believe that inter-CERT communication within a country is going to be key so we have an international touchstone and a national point of contact that can then be pushed out and each of these teams can of course, as Mr Chantzos said, address their own needs in a very sector-specific way.

Mr Chantzos: The co-ordination and information exchange when it comes to the CERTs is the key point when you have several.

Q170 ***Chairman:*** We have been given a certain amount of information about ENISA with its responsibilities for delivering European Union policies and programmes. Could you tell us what you think about ENISA? We have had criticism about them being based in Crete but it would be helpful if you could give us a frank assessment of what they do and who benefits.

Mr Chantzos: My Lord Chairman, for reasons of transparency I should first and foremost mention that I am a member of the ENISA Permanent Stakeholders' Group, so I am member, if you like, of their advisory committee which sits within the three institutional aspects of ENISA. ENISA has three different bodies, their Executive Director, appointed by the Member States, the Management Board, whereby the Member States' representatives meet and set the direction for the agency, but then its institutional stakeholders, if you like, the Permanent Stakeholders' Group, so I am one of those members of the Permanent Stakeholders' Group. From that point of view I could say that I have some intimate knowledge about the work that ENISA has been doing and even had a role in providing advice in what I believe ENISA should be doing. I participate there in my personal capacity, meaning I participate there as Ilias Chantzos and not as Ilias Chantzos, representative of Symantec. I think that is also important to mention, to be clear with the institutional point. Having said that, ENISA has been designed to be a centre of excellence and has been designed to be a platform for exchange of information, exchange of best practice, of brokerage, of co-operation and exchange of views. It has not been designed to be an operational agency. I think this was very clear from the very beginning, so from that point of view, with the limitations that its mandate is setting, I think that ENISA has been doing a fairly good job. If you look at what ENISA was expected to do in its first years of establishment, first of all it was expected to establish itself, which within the European Union context is in itself a challenge, bearing in mind that we are talking about relatively small agency numbers but with considerable bureaucracy. That is the nature of the rules and that is what we all have to live with, so on one hand we need to be mindful of that and on the other hand we need to be mindful of the fact that their main tasks were issues like awareness-raising, CERT co-operation and the promotion of the idea of building CERTs. They have been focusing a lot on critical infrastructure protection. They have not been busy mainly with policy. The policy is not defined by ENISA. The policy is defined by the Commission. Rather what they have been busy with is executing the different requests or the different, let us say, activities of implementing the policy that they have been getting from the different Member States. The primary client of ENISA is not the citizens of the European Union; it is the European institutions and the Member States. From these points of view I would argue that they have delivered some quite solid work. Having said that, we need to be mindful that the mandate of ENISA is under discussion and review right now and there is discussion as to what they want ENISA to be doing next, so frankly, once we have gone through the democratic process, we will see what additional challenges they will be called upon to execute. My assessment, and I think this would be also Symantec's assessment, is that they have done quite well so far. It is also relevant to mention that they recently had a management change as well as part of the end of the five-year mandate of the previous executive director. They have brought in now a new Executive Director who also has considerable experience in this area, so I think overall we are all hopeful of additional good work.

Q171 ***Chairman:*** Dr Nazario, do you want to add to that?
Dr Nazario: We are somewhat familiar at Arbor Networks with ENISA. We know some of their participants. We are not ourselves participants in the projects at all. We have been invited on a couple of occasions to participate in the WOMBAT early warning system that they have developed.
Mr Chantzos: WOMBAT is FP7 research.
Dr Nazario: Within the context of ENISA we have been asked to contribute data to some of the programmes and we have not. We have elected not to for commercial reasons within Arbor. We have seen them around a little bit. I think that they have built a decent foundation in their first years since their launch. They have had some success clearly. They have turned out some interesting research that is very relevant. My concerns, coming from my perspective and my community, are that they have not necessarily reached out as widely as they could and they have not gotten as much involvement with the members as they could. That is the perspective I have come to at this point with them. I think that is their biggest challenge in the years ahead.

Q172 ***Lord Hannay of Chiswick:*** So is what the two of you are saying on this ENISA point that ENISA needs to do what it is currently being asked to do better than it is doing it now, or is it that you think that ENISA's mandate should be expanded in order to undertake tasks which hitherto it has not been asked to do?
Mr Chantzos: I do not think I am saying the same thing as Mr Nazario on this so maybe you should not couple us together. I am saying that ENISA has done a good enough job so far. To use another expression, ENISA has been a force for good so far. ENISA has had challenges because of its mandate and I think that is generally recognised. That mandate is going to be reviewed and we need to see what that mandate will look like when that review is completed. I cannot prejudge what 27 Member States of the European Parliament or what the Commission will propose. Mr Nazario feels, if I understood him correctly, that ENISA could be reaching out more. My view is that if you look around the table at who ENISA has been talking to, it has been talking to a number of key industry players. Can we reach out to more people?

You can always reach out to more people but you cannot—

Q173 ***Lord Hannay of Chiswick:*** Can I press you a little bit on the possible extension of the mandate. Of course nobody is asking you to predict what the 27 Member States or the Commission may propose but you are in this industry, and what I am really asking you is where do you see an expansion of ENISA's mandate being useful for the collectivity of European Member States?
Mr Chantzos: Where do I see ENISA expanding the mandate?

Q174 ***Lord Richard:*** Where are the gaps in the present mandate?
Mr Chantzos: If you look at the way the ENISA mandate is drafted, it gives a list of objectives and then it gives a detailed list of tasks by which these objectives can be achieved, so I think to start with, frankly, it is fairly unique if you look at the way other agencies' roles have been drafted. In many ways that is the result of the compromise within the different discussions that happened some years ago. I think what one should be looking to is a more clear-cut and succinct mandate as to the areas that ENISA should be busy with. Right now for instance we have ENISA being busy with aspects of the telecoms package now that it has been agreed on the implementation side, but that is because the telecoms package as secondary legislation is actually calling for ENISA to do things. It is not because it is within the ENISA mandate. For instance, there is a general provision of ENISA providing more advice or providing advice in the area of EU legislation. Maybe that should be done more clearly. Maybe that should be done more solidly within the mandate rather than having to give a specific legal base every time, to give you a very concrete example. Frankly, this may be something worth us coming back to you with specific proposals as to what they need to be doing because you are asking me a point which involves legislation.
Lord Hannay of Chiswick: I think that would be useful.

Q175 ***Chairman:*** Thank you both very much for coming. If you feel you would like to send us a memorandum on that very last point, we have the new Director coming here from Crete to give evidence before us a week today and therefore it would be very helpful if you could give us your thoughts on this in the next 48 hours if you possibly could. I know that is asking rather a lot but it would give members of the Committee important background thoughts in order to have a discussion with the new Director next week.
Mr Chantzos: Another point that may be worth considering, my Lords, is that we have actually been called from the European Commission to submit our comments on the public consultation about the future of ENISA, so that is already available in public and we could certainly make that available to you immediately because that is already our stated opinion, and we could additionally see what can be done from our end in the admittedly short time.

Q176 ***Chairman:*** That would be very helpful. We have enormously enjoyed your kindness in coming here. You have been very full and I think you have been very frank too. We appreciate that very much. We shall pay the greatest possible attention to what you have said in writing our report which we hope to publish before too long next year and hopefully before the general election, whenever that is. Thank you; we appreciate it.
Mr Chantzos: It is the second time I have addressed the House of Lords, my Lord, so I am honoured to be here and thank you very much again for taking the time.

WEDNESDAY 16 DECEMBER 2009

Present	Billingham, B	Hodgson of Astley Abbotts, L
	Dear, L	Jopling, L (Chairman)
	Garden of Frognal, B	Mackenzie of Framwellgate, L
	Hannay of Chiswick, L	Richard, L
	Harrison, L	

Memorandum by European Network and Information Security Agency (ENISA)

The European Network and Information Security Agency (ENISA) very much welcomes this inquiry. Critical Information Infrastructures are nowadays an essential component underpinning economic and social life and development. Computing and communications networks are now becoming as ubiquitous as those for electricity supply—and the functioning of the electricity and computing and communications infrastructures have nowadays to be inter-twined in order to operate successfully! The security of communication networks and information systems is therefore of the highest concern to society.

In this regard, ENISA warmly welcomes the EU Commission's Communication on Critical Information Infrastructure Protection (CIIP) in providing the clearest framework yet for enabling Europe to act in case of major disruptions. Attacks in Estonia and elsewhere underline the importance of increasing Europe's capacity to protect information infrastructure. And increased resilience is required even against prosaic accidents and natural disasters if these infrastructures are to fully support the demands for ever-higher levels of service quality and sustainability put on them by contemporary commercial and social activity. But we realise that many of the decisive details for the practical implementation of this framework have still to be identified and refined. This area of good practice is where ENISA fits in and plays an active role.

In our contributions below, we will endeavour to provide answers to the questions that are as informative and useful as possible. It will be appreciated that the specifics of ENISA's mandate means that it would be inappropriate for us to address all the questions and that we have to be circumscribed in answering others. But we hope that it is equally appreciated that we need to address more than the two specific ones concerning ENISA directly in order to provide the necessary context.

1. Threat Analysis

1(a) *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disaster?*

The Internet is a complex system of interconnected networks and services (hence inter-net). There is no security-by-design to it. The functioning and security of this system is dependent upon the contributions of a range of actors that are at the moment largely un-coordinated, and with many reluctant and/or unable to take responsibility for ensuring the security of the system as a whole. This makes the Internet vulnerable to the growth in threats and their inter-connected nature.

Due to a high level of redundancy, the Internet should be able to withstand many disruptive events better than traditional communication technologies, which have an architecture that are often highly robust but only to critical break-points. Internet communications, by contrast, while more sustainable than traditional ones in acute situations, degrade quickly in quality such that only the most basic data services (eg excluding speech and even more so video) are viable. In addition, it is worth noting that the Internet is implemented using a standard set of communications protocols—any failure within this "protocol stack" could have devastating consequences.

1(b) *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

The short answer is no. The "Internet industry" is actually a composite of many sets of commercial activity, from basic access provision, through service provision of many kinds to applications development. In addition, provision of these activities for Internet communications by commercial entities overlap with provision of the same, similar or related ones in other markets. It is thus hard to say who should be doing what "to ensure the resilience of the Internet" in a singular sense.

A consequence of this is that businesses often see network and information security as a cost, rather than something positive. This is particularly true for SMEs, who have fewer resources than large corporate to both spend on assessing the risks they might face online, or to implement ongoing improvements and security updates.

Simple regulatory intervention to significantly address this situation would be difficult, however, because of the plethora of different entities and the markets that they might actually be properly designated as relevant to (eg telecommunications, media, software). Partly as a result of this, but also because of the how the un-regulated nature of the Internet has enabled innovation (including in security and threat technological development!) to flourish, improving resilience is primarily being addressed by focusing on the identification and development of best practices and appropriate technologies, and on cooperative frameworks for disseminating these amongst relevant entities.

Having said this, no one would claim that the current generation of Internet technologies are the best possible for ensuring sustainable, high-quality communications. The current Internet has grown faster and more widely than its original designers had any conception of.

But the various sectors that make up the "Internet industry" have been cooperating intensively on developing a range of more robust and secure next-generation technologies such as DNSSEC, […]. The main hold-up in the deployment of these has to do with factors not of a regulatory kind, but of market incentives and leadership.

1(c) *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

ENISA believes that this concern is justified. Cyber-attacks are part of a wide range of factors that can impact the resilience of communications networks and undermine the economic activities that rely upon them. We share the Commission's concern; we would also note that cyber-attacks are of particular concern for three reasons.

First, they are structured. As mentioned above, while the Internet is able to withstand a certain degree of disruption to infrastructure communications; with structured attacks this disruption can be modulated and directed to thwart responses to disruption in any one part of the infrastructure. For instance, internet routers of traffic will identify when another router is overloaded or made inactive by an attack or natural disaster and will then search for other routers that are still available through sending requests of availability. Attacks can be designed to do exactly the same thing (perhaps through hijacking the routers software that performs this function) and then use this information to overload or otherwise disable those routers that had indicated they were available.

Second, as attacks become more sophisticated in their technological design (able to be more targeted) they become potentially capable of bringing down ever more specific services according to the agenda of the attacker. To take an analogy, large, unsophisticated nuclear weapons were not of much use other than in catastrophic survival scenarios; more sophisticated, targeted and varied capacity nuclear weapons are far more capable of being deployed to achieve a menu of objectives.

Third, we do not know the magnitude, extent or intent of the "botnets" that are often used to launch such attacks. As a result, it is harder to build calculated models of resilience and response than with natural disasters (other than of a cataclysmic kind, of course).

Fourth, the probability of cyber attacks is increasingly high in comparison with natural disasters. Indeed, small attacks occur on a daily basis.

1(d) *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

The Internet plays a critical role in supporting the internal market. It therefore seems appropriate that the internal market should be capable of providing the the leading role in developing mechanisms for enabling the Internet to continue to function adequately almost of the time. ENISA can play a significant role here by working together with member States to identify weaknesses and recommending appropriate solutions.

The military should only be involved in protecting the Internet under certain well-defined conditions. If attacks are assessed as of a military nature aimed at the security of European states or pan-European security, the military should obviously become involved. When military intervention is required, there should be a framework in place to ensure that military and commercial actors act in a coherent manner and collaborate

towards a common goal. The delineation of ENISA's mandate to economic issues means, however, that we are unable to assess or comment on when such situations would be the case, nor how responses should be organised.

1(e) *How concerned should be we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

Because ENISA's existing mandate confines our work to economic issues, we have not attempted to collect law enforcement data. However, criminally operated "botnets" can have significant impact on commercial entities and their economic performance. Though attacks are at the moment often one-off events, as indicated above, it is hard to get a good idea of what might be "out there" waiting to occur. Botnets are a consequence of poorly protected end-user equipment and thus must be taken as a serious challenge.

2. International Responses

2(a) *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

In the modern global economy, supply chains (or "webs") for the production and delivery of most goods and many services often stretch across different national boundaries and between companies of varying capabilities size and geographical structure. While the final delivery of goods and services may be regulated on a national basis, functional operations may be geographically dispersed and outsourced in quite a complex layering of contractual relations. In a digital and online environment, this can be extreme,

This aspect of modern economic activity can make identification of critical assets and infrastructures challenging. Organisations need to identify precisely the assets they have, asses their criticality to their performance as well as their vulnerability to threats, and what an attack would mean for the organisation in terms of financial, operational or reputational damage. This makes the question of governance for the protection of even traditional "critical infrastructures" such as telecommunications or finance difficult. For example, would the data processing operations of say, a UK telecoms operator or bank that have been outsourced to a country in, say, central Europe a critical asset and therefore part of the UK's critical national infrastructure? The answer would largely depend upon the function outsourced to the central European country to the operational performance of the telco or bank.

A national regulator, however, might not be able to assess that the necessary risk profiling had been done without a European-wide view of the market and of companies' operations within it. Such analysis is needed to ensure the protection of European-wide critical information infrastructures.

Within this scenario, the question of whether multinational companies or others ones are more interested in European Critical Information Protection is not particularly germane. It might be that multi-national companies have the resources to be able to risk profile their extended international supply chains than purely national or local ones. But in a high value online environment, the multi-national might be a company of fewer than 50 people—traditionally an SME—that is perhaps too small to have the resources to make such an analysis. So the question is really of who is best placed to do this—individual market entities, national regulator, or someone at an EU level? The answer is most probably some combination of all three.

2(b) *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

ENISA believes that PPPs are a useful instrument but should not be seen as a "silver bullet".Modern communications markets are quite de-centralised, with a mix of different entities providing networks and services. A simple command-and-control system of regulation in network and information security is probably as hard as in other issues to do with these markets. So getting active and positive cooperation of key players is the most constructive approach: this consideration is the basis of the public-private partnership, and clearly has to be a central feature of public-private cooperation in one form or another.

But a one-size-fits-all approach is probably not viable in any way. A mix of regulation and various cooperative/partnership developed frameworks and tools will probably be most effective in addressing threats that are becoming ever more sophisticated in their technological and physical structures.

2(c) *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

The concept of market failure might be inappropriate to describe the adequacy of market responses to what is a fast changing and complex social and technological phenomenon. Or it might be that the concept is appropriate in some markets—such as for certain social groups and micro-enterprises—but not more generally. ENISA is committed to consider this question in its 2010 Work Programme.

2(d) *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

Yes. Early warning and incident response capabilities will—if organised and operated effectively—be of immense benefit to Europe's ability to assess and respond to cyber-attacks. As already suggested, the most appropriate overall response to the growing sophistication and targeting of attacks will consist of a variety of information sharing and incident response mechanisms. EISAS—along with WARPs in the UK—are designed to facilitate the development of information sharing and incident response arrangements amongst less close-knit communities than CERTs at a national level. They are actually established by national authorities, so the question of "appropriateness" should refer to a relative allocation of resources rather than of regulation. As EISAS are designed for citizens and SMEs—one of the most vulnerable groups in terms of risk assessment and awareness—a relative emphasis on the development of these would seem highly justifiable if combined with awareness raising campaigns. ENISA is working on identifying good practices in both.

2(e) *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

They are one of the mechanisms. National and governmental CERTS are a critical part of Europe's necessary security architecture. It is essential that these do not work in isolation but maintain close working relationships with other organisations that deal with cyber incidents such in the private sector and with law enforcement agencies. Apart from their inherent value in protecting governmental or key national systems, in some of the newer EU Member States, national and governmental CERTS can also play a key leadership role in establishing organisational disciplines and professional development that can then be adopted by other organisations.

It should be noted however that there is currently no centralised body that has a mandate for comprehensively coordinating the efforts of Member States to recover from a large scale Cyber Attack. Within the current framework, such a recovery would depend on the ability of member States to quickly establish and manage the appropriate bi-lateral contacts.

2(f) *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

No. The UK, along with a limited number of other Member States, is considered a leader in this area with developed practices that set benchmarks for others to adopt. So there is little chance that the UK will be adversely affected by developments elsewhere; on the contrary, as other countries develop information sharing and incident response capabilities for dealing with ever-changing threats they will be able to share experiences that will give the UK prior warning of what it may face but may well find useful in enhancing its capabilities. In other words, though the UK currently has highly developed governance infrastructures, in a rapidly evolving threat environment, the UK can only benefit from the development of greater European capabilities in information sharing and incident response.

2(g) Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

As the UK Government has emphasised in its evidence, the internet is a global phenomenon and does not recognise borders; this is something which should be reflected in any work which takes place to ensure availability of internet services. Having said that, it is important to recognise the reality that the United States is probably the leader in network and information security capabilities, the development of security capabilities and information sharing and incident response mechanisms.

However, Europe is able to offer little by way of partnership to the US unless and until it has got its own act sorted out. An overly prescriptive European approach would be problematic; but, given the extensive commercial, technological and law enforcement cooperation that exists in organisations in this area, a Europe-

alone approach is unlikely to develop and would almost certainly prove non-viable. As it is, Europe and the US cooperate closely within existing international organisations and initiatives, and ENISA is involved in many of these. ENISA also has extensive representation of leading US companies and professional representatives on the Permanent Stakeholders Group which advises the Executive Director on our Work Programme and strategic orientation; we also include such companies and professional representatives in the work of our expert groups.

3. European Network and Information Security Agency (ENISA)

3(a) *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

ENISA has focused its efforts on supporting the development of CERTs in European Member States that are not as well-developed in this field as countries such as the UK through brokering relations between potential partners. For instance, we worked with Hungary to provide expertise in the establishment of a national CERT in Bulgaria. It should be emphasised that these brokerage activities are always done at the request of Member States and is not something imposed on them.

As suggested above, ENISA's CERT work benefits directly from the leadership and experience of the UK, and the UK's WARP concept forms the fundamental basis of the EISAS model. UK plays a leading role on our Management Board (BIS), and has a large number of business and academic experts on our Permanent Stakeholder Group (PSG). The voluntaristic, partnership model of cooperation between public and private sector actors that lies at the heart of the UK approach is reflected, in fact, in ENISA's remit explicitly establishing the PSG as a formal part of our decision making apparatus and focus on identifying and disseminating good practices. It would therefore be surprising if the UK did not see ENISA as an appropriate body for work on the development of CERTs and EISAS in Europe. The more telling question is what role ENISA should play in this developmental work.

3(b) *Is ENISA being effective in its role, or does it need reform?*

The Agency has faced challenges in establishing itself and identifying how to optimise the positive impact of its limited resources. But we have benefited greatly from the generous support provided by the Greek government and our hosts at the FORTH institute in Heraklion.

It would have been inappropriate for the Agency to pretend to take a leadership role at an early stage of development. We have now become well established and mature enough as an organisation to assist in organising the discussions around the implementation of the Commission's programme and Member States' needs.

4. Timescales

4(a) *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

Different parts of the Commission have various responsibilities for implementing their overall plans. ENISA is working extremely hard to meet the requirements necessary to fulfil the responsibilities it has in supporting the Commission. But we are unable to comment on this question overall.

December 2009

Examination of Witnesses

Witnesses: Dr Udo Helmbrecht, Executive Director and Dr Jeremy Beale, Head of Stakeholders Relations, ENISA, examined.

Q177 ***Chairman:*** Good morning Dr Helmbrecht and Dr Beale. Thank you very much for coming. You have come almost as far as any other witness that this Committee has had for a very long time and we are most obliged to you for coming all this way to help us with our inquiry. Could I begin by just explaining some of the background housekeeping situations. You realise that this session is open to the public and the webcast of the session goes out live on the audio transmission and will subsequently be accessible via the parliamentary network. A verbatim transcript will be taken of your evidence and this also will go on the parliamentary website. We shall be sending you a copy of the transcript for you to check for accuracy, and if you need to make corrections we would be most obliged if you could make them as soon as possible; that would be very helpful. Also, if after this session is over you feel you would like to amplify or explain in greater detail some of the things you have told us, again we would much welcome to have

supplementary evidence from you. A final thing which I always say is that the acoustics in this room are very bad; I am rather deaf, so will you please speak up. Perhaps now you would each like to introduce yourselves and if you would wish to make some opening remarks we would be glad to hear them.

Dr Helmbrecht: Thank you very much for this warm welcome. We very much appreciate this opportunity to talk about IT security topics in this round. My name is Udo Helmbrecht and I have been the Executive Director of ENISA since October of this year. My former position was in Germany, President of the Federal Office for Information Security, so we were involved from the management point of view during the set-up of ENISA in the last five years. So I am well aware of the topics we are discussing here. At the beginning the only remark I want to make is that if we talk about IT security today it is really a new challenge in the area of e-commerce of how we work together, how we communicate together, and therefore I think it is very important that we have this open discussion on this topic.

Dr Beale: My name is Jeremy Beale; I am the Head of Unit for Stakeholder Relations at ENISA. I have been there since April of this year so I am also relatively new. Prior to that I worked as Head of the e-Business Group at the Confederation of British Industry here in London; and prior to that I worked for a number of years at the OECD in Paris on these issues, as well as a brief bit in between at the Cabinet Office.

Q178 ***Chairman:*** Thank you very much. Perhaps I can ask the first question, which is one of those basic questions: tell us who works for ENISA; what do they do; and, most important of all, who benefits?

Dr Helmbrecht: ENISA has a staff of around 65 people currently. We have permanent posts and contract agents and we cover a whole range of skills in our Agency. This is because—if you talk about IT security in *society*—we think that we need different skills; so we have people with a technical and computer science background; we have lawyers and economists so that we can address the different perspectives of IT security. We have recruited staff from the private sector, for example, from the Commission or seconded international experts from the Member States. A lot of people coming from the private sector have experience as a Chief Security Officer—for example, our head of the technical department—so this means that we can cover the experience from the public sector, the private sector and different skills for the work packages and work programmes we are running. The benefits: what we try to do is to provide added value for the Member States and for the Commission. So that there are two directions. One is that we provide guidance to the European Commission in the process, for example, of their legislation via European projects or research areas. On the other hand, we work together with the Member States, for example in building up CERTs and having reports which they can use in their own Member States. We try to do those things on a European level with cross-border activities or cross-border needs in this area.

Chairman: I did not say to you both that if either one of you wants to come in and supplement what the other is saying we would be delighted to hear from you. Lord Richard?

Q179 ***Lord Richard:*** Can I be fairly practical and ask you a few background details? What is the governance structure of ENISA? How does it actually work?

Dr Helmbrecht: If you look into our regulation we have some formal bodies: one is the Management Board. The Management Board is representative of each of the 27 Member States.

Q180 ***Lord Richard:*** You have 27 Member States.

Dr Helmbrecht: And three representatives from the Commission, so the Management Board has 30 members and the Management Board is responsible for approving appointment of the Executive Director.

Q181 ***Lord Richard:*** How often does it meet?

Dr Helmbrecht: It meets two times a year as a whole body. The other formal structure is the Permanent Stakeholder Group, which is appointed by the Executive Director and has members from academia and universities, and from industry; and from the citizen point of view from the, let us say, associations or businesses from the Member States representing users. So these are the formal bodies; and in addition to these we have so-called National Liaison Officers. These are representatives of national governments who act as a single point-of-contact. In addition when we are running our work programmes, we typically have experts for technical expertise; this is the basic structure. If you look at, for example, financial regulations, we have work package processes where ENISA makes proposals, which we discuss with the Permanent Stakeholder Group and the Management Board, and these proposals are then presented to the Management Board to discuss and approve; so this is the basis of our work. This means it is influenced by industry, private sector users, by governments, by the Member States, and by the Commission—and the results are also in the end presented to them; and for the annual account for the financial area I have to go to the European Parliament for them to "discharge" to use an accounting term.

Q182 ***Lord Richard:*** You have national representatives in ENISA?
Dr Helmbrecht: Yes.

Q183 ***Lord Richard:*** Do you have ENISA representatives in the individual countries?
Dr Helmbrecht: We do not have representatives of our own in countries; so this means that we with our Agency are located on Crete. For projects, for meetings we often go abroad; so this is something where the interaction is done on a project and working in them.

Q184 ***Lord Richard:*** What I do not quite understand—and I would be grateful to hear the explanation—is who decides what you actually do?
Dr Helmbrecht: It is a process. On the one hand it is the expertise of ENISA. The second step is that we discuss it with the community. This is on the one hand the Permanent Stakeholder Group, which has expertise of sectors of the private sector—such as the banking sector, the IT sector; the universities—so the representatives who say where the technology is going, for example. So this is a discussion when in the end topics and priorities are set and then because this is also discussed with the Management Board, it is then discussed with the Member States and with the Commission. So there is a picture where this whole group then says, "These are the topics we should address for the next years." Currently we have a three-year plan, so at the beginning of the year we discuss it for the next year and by this process we try to cover all interests, all aspects from the political level to the technical level.
Dr Beale: If I may, there is a final formal written approval of the work programme and the budget by the Management Board. So there is a formal process of approval there.

Q185 ***Lord Richard:*** That is only twice a year, is it not?
Dr Helmbrecht: At the beginning of the year we start with the process; in March we have the first Management Board meeting and this is the first discussion. Then we have in the mostly in the middle of the year a discussion between the Management Board and the Permanent Stakeholder Group; then in October it is the final approval of the work package and the annual budget and by this you have the process involving other people and the formal decision by the Management Board.

Q186 ***Lord Richard:*** I am sure it is my fault and I am trying to not get entangled in bureaucratic spaghetti, if you follow me, because there are an awful lot of strands in this, but really what I would like to know is who takes the actual decision as to what the work is going to be? If something is happening rather more quickly than others you cannot let it emerge from a 12-month process?
Dr Helmbrecht: Of course, as something which is my responsibility, I will say that there are certain topics I believe are important, from my experience and from my discussion with the Member States and with the industry. Of course I will try to put these issues on the table and then to discuss them and push them forward. On the other hand, if something comes up like a threat or something where we have to act in the short term, I am able in these circumstances to decide to remove resources and say that this project is done on a longer timescale and we have to do this; this is management through shifting resources. And if it affects something in detail I can always discuss it with the Chair of the Management Board and the whole Management Board. So, if it is; in the short term, it is a direct communication with the Chairman and an ongoing discussion, it is a usual management way to set varying priorities.

Q187 ***Lord Hannay of Chiswick:*** That is very helpful. So if I am right the stakeholder forum is purely advisory and has no decision-making or executive function. The Management Board, which has one representative from each Member State and three from the Commission, takes decisions but within the mandate that has been set for ENISA. How would you change that mandate? If you wished to make some really radical changes what would be the body that would change it? Secondly—and this is probably a bit more difficult really and it is not a question only to ENISA—are we not reaching a point where the management structures that involve representatives of 27 Member States and three representatives of the Commission are becoming hopelessly unwieldy? No university in this country is now allowed to have a council which is as big as that on the grounds that it is utterly ineffective when you get as big as that. I understand how the European Union has got where it has got to, but at some stage it is surely going to have to re-think these structures because they are going to become unworkable?
Dr Helmbrecht: I will first answer the question about the mandate. It is not the task of ENISA to talk about the mandate; this is a political process and a political decision. This starts in the Commission, then as a Communication of the Commission you have the co-decision process between Council and Parliament, so this is the way the mandate can change. ENISA has a limited mandate until March 2012 and this discussion starts now and this will be starting officially in the next half year probably. So this is where there can be some informal discussion, of course, but the basic procedure is the way I have just told you.

Q188 ***Lord Hannay of Chiswick:*** The Council of Ministers—which Council would it be that would take the decision?
Dr Helmbrecht: Within the telecommunication working group?

Q189 ***Lord Hannay of Chiswick:*** Yes.
Dr Helmbrecht: If you talk about the Management Board of course it is a challenge if you have 30 people, but it is a question of how you do it in daily work. One way is that there is a close connection between the Executive Director and the Chairman; so this means that if something has to be discussed in the short term, it is no problem today to pick up the phone or to have an email or to have a discussion. Then what happens is that usually you have Member States who are interested in different topics—because the IT security level is very different in Europe—and you have other Member States who do not put so much effort into it, so in the end it usually turns out that there are some active groups and some who are just following what is the mainstream. My approach is to have discussions with the board members, get the interest of the Member States and if you do this over time you get an impression of where there is a compromise to be found or where there are some challenges to face. Then if you prepare—and I think this is important—a Management Board meeting with a tough agenda with information beforehand you can challenge this.

Q190 ***Lord Hodgson of Astley Abbotts:*** I think you said that in October of each year you came to a conclusion of what will be next year's work programme. I do not have a record—I apologise if I missed it—of what is on your programme for 2010. What are your key tasks for 2010? Perhaps at the same time what are you looking at for 2011 and 2012 since you take a three years view?
Dr Helmbrecht: If we look at 2010 we have in our work programme some tasks which I will mention in a second, which we started and will then finish, and we have some new work packages—we call it preparatory actions—which start next year. So, we have done a lot of work on the topic of network resilience. Due to the Commission Communication on Critical Infrastructure Protection—CIIP—we are also concentrating on the resilience framework within the CIIP. Then we have our support of the Member States building up CERTs; then we have our risk assessment in this area. So these are some main programmes we are running, which we will continue. And we start a new activity on identity and trust and this is to start in the next year. So these are the main topics.

Q191 ***Baroness Billingham:*** I just wondered if you have any direct links at all with the Member States of the European Parliament or do you always work through other agencies?
Dr Helmbrecht: If you talk about the European Parliament there is the so-called ITRE Committee. This is a Committee which on one hand has to approve the election of the Executive Director and on the other hand it is a committee where ENISA has a chance to present itself. I am accountable for the financial aspects to the European Parliament. On the other hand, it is on an ad hoc basis if there are any other engagements with the European Parliament.

Q192 ***Chairman:*** How often does the Chairman of the Management Committee change?
Dr Helmbrecht: I do not know this off the top of my head but currently it is Professor Posch from Austria and I think he has been doing it now for one and a half, two years and will do it until next year.

Q193 ***Chairman:*** This Committee has had problems in the past with various European organisations where the chairmanship of the management committees changes much too quickly and the person doing it hardly gets a chance to get their feet under the table. Do you find that the Chairman of the Management Committee has enough time to really get to understand the problems?
Dr Helmbrecht: I think in this case for ENISA currently we are very lucky because on the one hand the Chairman, Professor Posch, has done it for some time and does it also in this, let us say, transition phase with a new Director. Secondly, he is the Chief Information Officer of the Austrian Government so he knows his topic and this means that not only on a political level but also on a technical level there is an information exchange and because he is involved in a lot of other European topics I think for ENISA it provides for good communication with the Chairman.

Q194 ***Baroness Garden of Frognal:*** You mentioned in a reply to an earlier question that you were looking to resilience and to critical national infrastructure and we understand from previous witnesses that those used to be off limits for ENISA. So has that change been successful, incorporating those into your work, or is it too early to tell?
Dr Helmbrecht: The answer is basically yes. I think that the challenge for ENISA in the starting phase was that it was being built up in 2004; you had to recruit people and it takes some time to get familiar with the organisation before you can really work. I think this was a challenge also for the former Director. Then the question always is, if you look at the European level have you understood the interests of the Member States and also the limits of the

Member States? Then if you look at the regulation it is something where you then have to look at what are the tasks and to put the tasks in to deliver. So if you look to the general discussion about critical infrastructure over the last years in Europe there have been some discussions in the past but on the European level it took some time really to be aware of how to put this into a co-operational level in the European Union. So when the European Commission then made this communication of CIIP ENISA was prepared to take up this task and we are lucky that it fits into our skills, our work packages that we can address, and that if we do something in this area we can be successful.

Q195 ***Baroness Garden of Frognal:*** So it was not a policy decision as such; you are saying that it was a timing and administrative decision that you did not take it on initially but you then broadened your remit?

Dr Helmbrecht: Yes. I would say that sometimes when you look at this discussion it is always a question of what is in the interests of the Member States and when do you pick this up on a European level.

Dr Beale: If I may, I also think that it is a trust issue; that ENISA had reached the point where trust had been built with the member countries and the Commission. If I could just say from my past experience at the CBI when the discussions about setting up ENISA were going on we were concerned and we did not want a European agency getting involved in national security issues. That was appropriate for Member States; we did not think it was appropriate that at the European level the competence existed there. ENISA did not do that; it did not try getting into areas where it would not be helpful. So I think the fact that it was asked to take on this work in resilience was actually a compliment and showed that there was that trust, and I think that the results since then have shown that that trust was well-deserved. I hope I am not breaking a confidentiality issue but we were just at CPNI before we came here and they said that some of those materials generated by that work they were finding very useful. So, so far so good.

Q196 ***Lord Harrison:*** I thought I would ask my own question first and go back, if I may, because I think we are touching on areas in this way. Good morning, gentlemen. I have read the written evidence that you have presented where you say that the clearest framework yet for enabling Europe to act in the case of major disruptions has been clarified, but you realise that the practical implementation of this framework has still to be identified and refined and that this area of good practice is where ENISA fits in and plays an active role. I am wondering whether you would like—and I know that you have already said, Dr Helmbrecht, that you resist commenting on the mandate that you presently have—to see ENISA tackling a wider range of issues and would you like to see a change of role perhaps involving more operational issues. It seems to me from both what you and Dr Beale have been saying that you are straining at the bit here; that there are opportunities and opportunities that whilst they may well be a matter of trust that you do not trespass into that area, nevertheless seem to be an open goal, as it were, for ENISA to become more involved, more active and to help the ultimate aims of yourselves and of what the European Union would want.

Dr Helmbrecht: When we look at the current mandate of ENISA it was written and decided in 2003. So from this time on we have two basic developments; one is that we had the enlargement, so we now have the chance to involve new Member States and help them to improve IT security in general. The other thing that we have is the Lisbon Treaty since December now, which also gives some opportunity for the future. The basic point I want to make is that when we from the ENISA side look at IT security, it is first prevention—IT security is something that is needed in society today—and how can we put IT security into e-commerce, e-government and all that we are doing here. On the other hand, this is tied to the smooth working of the European market. So what I want to say is that when I look at this from ENISA's perspective, even with the current mandate there is enough to do. And to look at how can we improve IT security on the internet if we have electronic communication? We need a lot of awareness and education of how to be competitive in Europe with our IT industry or industry in general, looking to other areas like Asia or the United States. If you look from this industry, from the private/public sector, which affects our everyday life, this is something where we have—if we do it in the right way in the interpretation of the mandate—a lot of possibilities. It means that where we can have our priorities, that we need to be sure they really add value for us before we start the discussion of how much to extend the mandate of ENISA, which in my view should be a long term discussion. Because, if you talk about operational things, it is sometimes a little bit of interpretation. For example, the department where we do most of our formal Work Programme activity is carried out now, we call an operational department, in contrast to where we do our administrative tasks. But if you talk about operational things like doing 24 hours, seven days a week, 365 days a year, running a CERT, then you will need some other resources, for example. So, what I mean by this is IT security is so big that I want to concentrate with our limited resources on the priority, on the European Common Market.

Q197 ***Lord Harrison:*** There could come a time where you outgrow that original mandate and it could be useful by expanding that mandate, but at the moment you are curbed by resources. This area of good practice is where ENISA fits in and plays an active role—active in the sense of promoting what can be done—in promoting good practice, and then already you are beginning to change the mandate, are you not?
Dr Helmbrecht: Yes. I see it currently as a situation where for me as a Director I wear two hats. One is that I am responsible for running this Agency and with these resources for the next year, doing the best for you all. On the other hand, of course, I am someone who wants to stimulate the discussion about the future of IT security in Europe with different aspects. To give you one example, a concrete example: currently we do not have a connection with law enforcement and I would not talk about ENISA being involved in law enforcement currently, so there is a clear red line. You had another question about NATO and it is also clear that ENISA is not involved in any NATO topics—there is a clear border. But if you, for example, look today at threats on the internet, you have different laws in different Member States and it is difficult if you have a botnet if somebody is abroad attacking some country in Europe, so we need in the future some improvement in international law and IT security. This is something where I would stimulate the discussion but for the moment I would keep ENISA out of this role to have a strict reduction to the mandate.

Q198 ***Lord Harrison:*** Before I come to the NATO question perhaps I could ask Dr Beale, who laid great emphasis on his CBI perspective when he was there that trust was of the essence that ENISA did not outgrow its role. Are you at one with Dr Helmbrecht on this, that there may have to be change to reflect changing circumstances?
Dr Beale: Yes, I think there will be and there are changes. One of the reasons why I certainly went to ENISA was because I felt that I had been working on these issues here in the UK but that a lot of the areas that needed to be addressed increasingly were at the European level; so that generated my interest and I felt that ENISA had an important role to play there. I should just say, though, that one of the things that I learned at the CBI—it is a similar thing that we are debating at ENISA—is just because there is a problem that needs to be addressed you should not try to be the ones to address all the aspects of it. It is a matter of learning to identify who the key partners are and to working with them. We had to do that at the CBI—there were many problems our members had and we had to identify who in our membership could make the difference and help them to work with others. In many cases that is what we are doing at ENISA. Dr Helmbrecht referred earlier to the way that there are certain leading Member countries. Part of my responsibility as Head of Stakeholder Relations is to identify who in the private sector—and which countries—have the lead, have the ideas, can help set the agenda and to work with them so that they can, rather than ENISA, try to do more of what is needed than we can be ourselves. The question about the mandate comes in where, in that architecture of all actors being active, should ENISA play a role—and I think that Dr Helmbrecht outlined the key issues of concern in terms of what that debate should be about.

Q199 ***Lord Harrison:*** Dr Helmbrecht, you have partly answered the next question: do you liaise with NATO or indeed other military groups? Under the main question, do your plans involve the engagement and encouragement of defences against cyber warfare?
Dr Helmbrecht: As I said, ENISA will not be involved in NATO topics. On the other hand I want to stress that with the problem or challenge of the internet you have the same technology and the same tools that you use in the private area and in the military area. This means that from my perspective there should be approaches in the Member States and if the Member States look from their national security at how they deal with things then they have to find solutions. Then of course there must be, for example, from a NATO level also some solution for this; but, as I said before, for ENISA we can deliver best practice and we can deliver information and if you read our reports where we discuss technology evolution, impact of technology and threat analysis, these things of course can be used by other stakeholders in other areas.

Q200 ***Lord Hannay of Chiswick:*** Could I just follow that up. I understand and respect what you say about the red line and NATO but it is of course a self-imposed red line by the European Union and it does sound to me from your reply that it is a bit of an inhibition to have two organisations—the EU through ENISA and NATO—with a very big overlap in membership, and given that there is a similarity between cyber warfare manifestations originating from States and those originating from criminals or the private sector, that this red line in the longer term is a bit of an inhibition to the sort of co-operation that there ought to be between a European institution and NATO. Is that not something that Lisbon will help to address that can be reduced as a red line, or is it absolutely un-crossable and something that is going to govern your work for the foreseeable future?
Dr Helmbrecht: I think we should look from the responsibility point of view. For example, if you talk about military threats you have national structures.

Also, if you look for IT security you have a lot of Member States—let us just say the old Member States or big Member States—who have experience with this, which have agencies, and so you have established structures there. Also in other sectors you have found ways of how to work together with different sectors and government, private sector, military and so on. So if you put this on the European level the question is: what responsibility do you want to put into a European agency like ENISA? Of course I agree that if we now have the Lisbon Treaty that it must be a political question—what do you want with such an agency—and we can also participate in this discussion from the technical input. But in the end it is a question of what do you want to have here and I think that if you look at other cases, for example at telecommunication, at internet service providers, if you talk about vendors producing IT products you are talking about a huge amount of area where as a daily business what we are doing is faced with, let us say, the classical threats of the internet like botnets, Trojan horses, phishing, getting money off other people—so a lot of things which in this area are not connected to what are NATO topics. Of course, on the other hand we have to have some kind of information exchange but this can be on another level which must not be something that you put in a mandate with responsibility. If you talk about responsibility and you talk about how to run the European Market, how to have things involved also as they do it with other sectors, then it is an approach where you can keep this line and say that this is national responsibility, this is European responsibility and this we put to ENISA.

Q201 ***Chairman:*** Can I pursue the NATO side of this. I am sure you are aware that NATO is an organisation which is prepared to come to the aid of a stricken nation if they request it in the event of a major terrorist attack or a major natural disaster. Each year they have an exercise. I attended one some years ago in Croatia where they had a simulated hijack, a simulated biological attack, a simulated earthquake, a simulated major oil spill and a major transportation breakdown. They are having another one in September in Armenia. They have them each year and they are very well attended—not just military—particularly with civilian aid organisations and emergency services coming from countries right across the NATO alliance. I ought to know but I do not know whether they have ever had a simulated cyber attack, but I would be very surprised if they have not. For instance, they have had a simulated dirty bomb. I feel sure at some time they will have had or will have in the future a simulated cyber attack. Have you ever been approached or involved in taking part, even as observers, in those exercises; and, if not, do you think that it would be worthwhile if you were involved, even as observers, because there are quite a lot of observers, as I know very well.

Dr Helmbrecht: The answer is we have not been invited or involved in NATO exercises and I think what you are discussing is different when you talk about something that is part of a mandate. If NATO invited ENISA to put their experience on the table, of course this would be no problem. If we discuss this topic we are also talking about exercises in the IT security community; so from the European Commission Communication it is intended, and it is now our work programme, that there should be an exercise in 2010, so what we are preparing is how to do this. But if you talk about exercises I know that the military community has a lot of expertise in how to do exercises, so we do not have to invent the wheel again. This means that of course you can have discussion, exchange information, exchange best practice and experience, but, on the other hand—and I think this is the question that you raised—if you talk about crisis management, if something happens, how to react, this is not something different from what we have to discuss for the future, and how do we want to deal with a civil crisis and military crisis in the future if a significant IT threat was involved. What I want to say is that there are a lot of topics which must be addressed. One is the ENISA mandate, one is our work, one is how to work together. You can use the connections in participating in conferences and exercises but we have to carefully distinguish what we are talking about at this level.

Q202 ***Lord Dear:*** Gentlemen, last week when we were taking evidence a witness suggested that in his opinion you had failed to engage with the global security groups that are operated by the internet industry. I wonder whether you would agree with what he said and whether he was right in talking about the organisation way back in the past or even currently and whether you have any plans to extend your activity and your interface with the industry?

Dr Helmbrecht: I can understand this remark because, as I said, ENISA was building up connections and, like Jeremy said, building up trust and building up this community, so what we want to improve in the future is the following. On the one hand we have the so-called Permanent Stakeholder Group; we have members coming out of Europe, so this means that we have on an expert level built up in this community. You have other organisations like the OECD or ICANN for the internet. So this means that we are starting to have a dialogue with them and this means that step by step we will improve this global network. What is also something positive for us is that we get invitations or questions from organisations from abroad, for example from Asia or even other countries, asking us if we could give a presentation of this or that, so we get invitations. This is something

that will evolve in the future as ENISA works on these topics and extends its network. Does that answer your question?

Q203 ***Lord Dear:*** I am grateful to you for that but in my experience the internet itself is a very fast expanding entity and the industry that supports it has to be very fast as well—one drives the other. So we are talking about something which is changing almost on a daily basis and I wonder whether you are able to work up to a speed where you can interface at the same sort of speed or whether you are constantly, as I understand from your last answer, trying to catch up to something which is disappearing further and further into the distance?

Dr Helmbrecht: My aim is to overtake them. My approach is if you look at the current situation, for example let us take the CERT community, we had to face, as Jeremy said, building up trust so that we are accepted by European organisations like the Trans-European Research and Educational Network Association's CERT Task Force (a part of the FIRST global association) and others, so by being part of this community; and then immediately you have contacts to Asia, the United States and so on, so this is something which spreads out. Of course, on the other hand—and this is what is important for us—to be in contact with the research community and the industry community, so that, for example, I am now able to select a new PSG because it is just in a phase of changing and I am looking for people and I have a lot of applicants who are coming from industry—let us say, for example, companies like Nokia and France Telecom or British companies. So, other companies are participating here and we also have American IT companies with subsidiaries in Europe and this means that my aim is to have a close connection to them so that you can have by this an immediate response—what other technologies are taking place and what threats are coming up. This is something that starts working and so if you have these connections you are aware of their company strategies and what they are doing and thinking and what is changing.

Q204 ***Lord Dear:*** You have talked a lot about trust in your evidence so far and I appreciate that because it is the bedrock to most human relationships and organisational relationships, but as I understood you before—and you must correct me if I have got hold of the wrong end of that stick—the trust I thought you were describing was between Member States within the EU. But I think what you are now talking about is building up trust with the security industry itself and I am surprised to hear you say that because I would have thought that they would have welcomed involvement by an organisation such as your own, representing the whole of Europe, to help them to deal with something which is a burgeoning problem. Am I not seeing the same scenario as you?

Dr Helmbrecht: Yes, but there are maybe two different approaches to what is happening and on two different levels. One is, which Jeremy addressed, that if you talk with Member States about critical infrastructure the question is what is in the interests of a Member State to have under its own responsibility and what to put on a European level? So in this discussion if you have ENISA then you have two levels: one is you have the organisational trust and do you trust that ENISA keeps information confidential and how do you share it? And the other is personal trust. If you talk about CERT topics it is a lot about personal trust, you know each other and to share information. On the other hand, if you then go to industry we did not really until now establish a public/private partnership model. So what we do currently is have projects and have experts and discuss it with them. But the question is, for example, what I want to do—I start it next year—that if we talk about the internet we have to have close co-operation with the telecom providers, with ISPs, to have also some kind of early warning system, technology and other things. So it is not that the industry comes and say, "Hi, there; it is ENISA," it is something where you have to talk to them because the question is what is the added value from a European perspective for a global acting company. This is something where we are having some discussion and also to have this trust by the industry that they have an added value if we work together with them.

Dr Beale: If I could just add to that and, again, if I can draw from my experience at the CBI? There are a lot of agendas out there in the industry side and there is a difference between suppliers and users and between the different communities of suppliers and what they are supplying, and I think the value added that ENISA would bring will be to be smart about its agenda and to identify which interests again can work best together and this is particularly pertinent in those public/private partnerships—or models of co-operation is maybe a better term because sometimes PPPs can be a specific legal form. The task is about identifying what the agendas are that are going to bring the actors in so that ENISA is not seen, for instance, as just representing the interests of network operators or software suppliers or business users but a forward-looking agenda which helps each of those entities or those sectors and others move forward on an information security agenda for Europe. That is where we are still, as Dr Helmbrecht has said, engaged in defining the terms in that debate and that is a maturity aspect of our development. We are still a young Agency but I think that the new Permanent Stakeholders Group will be very, very helpful to us in refining that agenda along with the advice from the Member States because the Member States will of course get that lobbying from the industry too.

Q205 ***Lord Dear:*** In about a year or two years' time do you think that your organisation will be able to work at the same speed as the internet industry?
Dr Beale: My personal experience from the two months that Dr Helmbrecht has been with ENISA is that we might have overtaken aspects of them too. He is working us very hard!
Dr Helmbrecht: I did not tell him to say that!
Lord Hannay of Chiswick: Could we look at the issue of CERTs now?
Chairman: Just for the record, Computer Emergency Response Teams.

Q206 ***Lord Hannay of Chiswick:*** It is like the *Today* programme! The Commission's Communication puts a lot of emphasis on the desirability of setting up national CERTs which would cover more than simply public sector infrastructure. That in a way is slightly different from the approach that is being followed in this country, as you know, where we have industry-specific, sector-specific and company-specific CERTs. You are presumably doing a lot of work on this; do you regard those two approaches as being mutually inconsistent or do you think that in some countries, perhaps smaller Member States or Member States with a less mature internet industry, a national CERT makes more sense but that in others the sort of approach in the UK makes more sense? Could you perhaps give us some thoughts on that?
Dr Helmbrecht: I think both approaches in the end match together because, as you said, you have small Member States who do not have any CERTs and the question then is how to build it up, and because you have from ENISA's side this connection to the Member States, to the Management Board and other people, you can then build up governmental and national CERTs. But I would also appreciate in support if such Member States would then have academic CERTs and so on. I think it has been shown in the past that sector-specific CERTs work very well because they understand the business. It is different if you have an academic part where you have a lot of students and teachers or if you have an insurance company or a stock brokerage where you need seconds of reactions and you need other procedures of CERT interaction. So if you have sector-specific CERTs and if they interact, as I said, on this trusted communication you can improve it. So it is my approach, wherever we have a structure like a well defined and working structure in the UK, is to take this as best practice and to use it and interconnect it and support the interconnection and support smaller or new Member States to go this way; and in the end if we have CERTs—and this would be my vision—in every sector or every Member State in a trusted communication then we have really improved something.

Q207 ***Lord Hannay of Chiswick:*** If I were to take that a little further, setting up a national CERT in a small Member State that does not have a very mature internet industry might be the obvious first step but it would not preclude them subsequently having sector-specific or company-specific CERTs as they became more sophisticated and as their involvement built up?
Dr Helmbrecht: Yes.

Q208 ***Lord Mackenzie of Framwellgate:*** Good morning, gentlemen. Lord Jopling mentioned earlier about simulated cyber attacks and of course a lot of your tasks emanate from EU Communications and large-scale cyber attacks. On the question of resources, do you think you have sufficient resources to do this work and do you expect to deliver on time?
Dr Helmbrecht: For every agency there are never enough resources. The question is if you take the topics and you take the resources how to set priorities. So it is very important to discuss these things, in our case with the Management Board and the responsible stakeholders, as to what priorities we want to put into our work programme. I can say that for 2009 we delivered all on time. Of course, we have a tough work programme for 2010 and, as was mentioned before, if something comes up it is always a management challenge then to move resources. I think if you connect it to our current situation for 2010 and 2011 this is what we can foresee, by setting the priorities and discussing this. From the Member State perspective you know what we can do and this is where we can also say that with our resources we can reach these goals. What I currently do is to optimise the processes within the Agency and to get resources from the administrative area module and operational area, but in the end it will be discussion. As I mentioned before, if you talk about this new process of the mandate it is then your decision of how much resources you give ENISA because I am well aware that in the end it is the citizens who pay taxes.

Q209 ***Lord Mackenzie of Framwellgate:*** Just to follow that up, you mentioned that it was a management challenge to move resources around but if there was a surge of demand, for whatever reason, do you have the mechanism for actually increasing resources, even on the short term?
Dr Helmbrecht: It is limited of course but we have a part of our budget which we have for projects and which we can use for contract agents.

Q210 ***Lord Mackenzie of Framwellgate:*** Like a contingency fund of some kind.
Dr Helmbrecht: It is not in this way that there is some reserve in the Agency but it would depend on the stage of the year. If it is in the early stage of the year I can always decide and say that if there is something really urgent we can do this in this way. On the other

hand, if it is at a later stage of the year I would go another way and say is there some support of some Member State or some company with resources, because also in this community sometimes it may be an advantage for somebody in the private sector where you can say, "Could you also help us on this topic?" So there may be ways out if it really gets very critical.

Q211 ***Lord Hodgson of Astley Abbotts:*** You are looking at the challenges of a virtual industry—a virtual and fast moving industry, as Lord Dear reminds us. I note that in your evidence you said some very nice words about the Greek Government's generosity in the facilities in Heraklion. Could you say something about the challenges that you have in recruiting people (a) who can be at the leading edge of the developments which were the subject of Lord Dear's question; and (b) whether the fact that it is based in Crete assists or detracts from that ability to recruit?

Dr Helmbrecht: It is not a black and white question, of course. If you decide that European agencies are spread around Europe then it is the responsibility of the Member States to define the seat and I appreciate all that the Greek authorities do in this regard. But, of course, there are some challenges. Most of the burden is taken by the employees because it means travelling for them and travelling always means for a mission here because you can never do it on one day. On the other hand it is currently a difficult situation for families with children because you do not have a well established European School in Heraklion, so if you have parents with children from the ages of, say, 12 to 18 it is nearly impossible currently. This means for some employees the family situation is difficult, but this does not mean that it is difficult in general because we get a lot of applications for vacancy notices—although it is not really spread around Europe on the whole. We get a lot of skills from the public and private sector, so it is not a problem if we have a vacancy notice to get somebody there. But in the end you get, as I said before, a limited social mix in such an agency.

Q212 ***Lord Hannay of Chiswick:*** Could you elaborate slightly on this? When you advertise your vacant posts are you getting the same sort of uptake that you would expect if you were, let us say, in Frankfurt or London or somewhere like that? Or are you really being inhibited by the fact of the geographical situation of the Agency? Are you achieving the retention period that you need if you are to have professional people who understand their jobs really well, or is the fact that the Agency is situated in a place where it is quite difficult to get to and from and that there is not a European School, and so on, is causing problems both of retention and of recruitment? It would be helpful to have an idea as to that. What we were struck by when we looked at the origins of ENISA was that it was rather odd that Greece was allocated ENISA but was then left to choose whereabouts in Greece it should put ENISA. The normal practice, from my own experience, is that the bid of a country for an agency like this should be accompanied by a proper analysis of the place that they were offering to put it and its ability to help on these things like recruitment and retention.

Dr Helmbrecht: If you discuss this topic there are always some points of advantages and disadvantages and in a second I can give you an advantage of the location. The basic point I want to make is that this is not only a question that challenges ENISA, it challenges also some other European agencies, but in the end if you put this Agency somewhere else in Europe you would always have travelling and you would have this discussion. So if you go deeper into this discussion it becomes difficult because in the end you would say that every agency should be in Brussels and maybe this solution could also be questioned. So from the principal approach it has some different aspects. You have an advantage if you look at Heraklion that you have a big university campus; you have a research institute called FORTH, which is working on computer science and intelligence and other things, so this is something, from a technology point of view when you are looking where is the technology going, something which is an advantage for ENISA. The other thing is of course that if you look in the end—and this has to be discussed honestly—at somebody who has worked in London and then goes to Heraklion and he is in the situation that he has two children and a wife then it becomes a problem if the wife does not get a job there immediately because of the situation. The point I want to make is that we get staff—that is not a problem; we get enough applicants for vacancy notices that we can choose high quality; we get it from government and we get it from industry, so this is not the problem. But, in the end, if somebody says, "I want to have this one in this family situation" then it is not possible because they will not come.

Dr Beale: If I may add something here? It is also in many senses the agenda that an organisation has that attracts people. They will put up with lots of things if it is an exciting, dynamic, important place to work. I think it is over the last 18 months that three British people have joined ENISA to work there where previously there were none; and there is a reason for that. As I mentioned for myself, it was because I felt that a lot of the issues were becoming important and—and he is too modest to say—that Dr Helmbrecht, who was President of the German BSI before, has also come to work there. There is no inherent barrier where ENISA is to attracting high-calibre candidates, if I could be so bold as to put

myself under that umbrella. The key thing becomes about how you work and what you do—and that is really the focus of our efforts: it is now on improving our interaction with our stakeholders and being more at the centre of the debate. We have also opened a branch office in Athens with the support of the Greek Government so that we can hold meetings there that will make it easier for the people we interact with to come and participate and, as Dr Helmbrecht mentioned earlier I do believe, we also hold meetings in Brussels, in Vienna, in Madrid, in Paris and we have held one in London too. So we can be flexible and I think that is the more important thing—not getting trapped as a result of where we are.

Q213 ***Lord Hodgson of Astley Abbotts:*** I heard you say that of course it is people with young families where the major problem is. In my experience this is a young person's industry and it is young people, people who will have families who are going to be leading the charge on taking the industry forward; they are the people who have the mental agility and the intellect. So it does seem to me that there is quite a disadvantage if young people with families do not want to go to Heraklion for the reasons that you have identified. Could you just confirm that all the 65 of your staff are based in Heraklion? And it would really help me greatly if you could tell me how many nights the two of you spend in Crete each year?
Dr Helmbrecht: I can give you the figures, of course, but not in detail. I can give you an approximation. I can say that for young families, if it is kindergarten and the first years at school it is possible; so now it is an evaluation to say that if you have parents aged up to 35/40 years it is not a problem if the wife does not work. But then it becomes a problem if the parents are between 40 and 50 years old because then you have this family situation which makes it difficult. On the other hand, all staff live on Crete because it is a condition, if you sign your contract, that you move there. Of course you can fly back and forth when you want. What happens in some cases is that the man or the wife who works for the Agency lives on Crete and the family does not live on Crete—we have some examples of this—because of the situation, and this then makes it difficult for those parents who are let us say 45 years old. But if you want to have the figures I can give them to you in detail.

Q214 ***Lord Dear:*** Gentlemen, this is more of a statement I suppose rather than a question. I remain uncertain of the validity of what you have told us, from my perspective. Let me tell you where I am coming from. I think if we were looking into some deep-rooted problem in the motor industry we would be surprised to find if any EU Commission set up to deal with that was not located in the Ruhr or in Turin or some other centre of motor manufacturing. Similarly, this is a global problem and if it is being approached in a global way I think we would be surprised not to find the international organisation located in Silicon Valley in California or in Cambridge, UK. I speak as the Chairman of a high-tech company, which is located in Guildford, and much as it would cost us money to relocate we are seriously thinking of relocating to Cambridge because that is where the centre of excellence is for high-tech in this country, and that is quite a short move. I am surprised—and this is what I want to put on record—that we are talking about something which is as fast moving and internationalised as the cyber problem and the location that you have has been chosen in the way that it has. I would have thought that there must be a great difficulty—although you tell us that there is not—in attracting and relating on a daily basis face-to-face with the sort of people who are up to speed with the problems, and how that can be done from the fringes of the EU with no huge tradition of dealing with these sorts of problems still defeats me. That is more of a statement than anything but I wonder if you would like to respond to it.
Dr Helmbrecht: One remark to this is what we can improve in the future using the technology really in a daily way in which we are dealing with internet security. For example, if you have a video conference system, if you have some kind of tailored working this may reduce some of the difficulties in the future. On the other hand, if you are looking to the industry it is an industry where you have, at least in Europe, too much dependency on plant locations. Of course, I follow your argument that if you look around Europe where do you have the IT industry but this means in the end that it is more of a community that we are dealing with, to say "Where do we meet?" So for us it is more an issue of saying we have this community of experts, of working programmes and we come together with the Management Board, with the PSG and we are doing our projects and we are running our exercises and we are doing this, as Jeremy said, in different countries of Europe—wherever is most appropriate for that body or project. So we meet this challenge today by saying that we look to have the right place for where we are working together at any one time or on any one issue in the Community. The other thing is what we have talked about before—the location for the staff. So it is more a challenge for the staff and not for the everyday working for the future.

Q215 ***Chairman:*** I want to move a shift on this question, from those who work for the Agency to those who have to visit it. From which European hubs can you fly to Crete, apart from Athens? I am

asking where are the direct flights to Crete from European hubs, capitals if you like, besides Athens.
Dr Helmbrecht: From most European main cities you have direct flights to Greece, to Thessaloniki and Athens. In the summer you have flights to Heraklion. This is during the tourist season from about March/April to October, so you can have direct flights by the different companies which bring tourists to the island.

Q216 ***Chairman:*** Most of those will be charter flights, will they not?
Dr Helmbrecht: Yes, most of them are of course charter flights.

Q217 ***Chairman:*** Do I take it from your answer that it is only really from Athens that there are regular direct flights?
Dr Helmbrecht: Yes.

Q218 ***Chairman:*** How many flights a day are there into Crete to and from Athens?
Dr Helmbrecht: I do not know but I can give you a typical example. When we go back to Heraklion in a typical way we leave London in late evening, have a flight to Athens and stay overnight at Athens Airport and take the first flight on Thursday morning. So that is the typical way that you go from Brussels, Frankfurt, Paris or whatever in the evening and have an overnight stay. On the other hand if it is a question that you have a meeting early in the morning then it is the same the other way round; or if you have a late morning meeting sometimes you can take the first flight from Heraklion and then be here another time. So it depends a little bit on the time schedule but let us say for a one-day meeting you need to spend two nights.

Q219 ***Chairman:*** My question was how many flights a day are there regularly between Athens and Crete?
Dr Beale: I do not know the exact number but there are numerous flights during the day from which one can select to go either to or from Heraklion to Athens or back.
Dr Helmbrecht: For this afternoon there are three flights to Athens from London, for example.

Q220 ***Chairman:*** I am not interested in London to Athens—that is the normal thing. What I am concerned about is Athens to Crete.
Dr Helmbrecht: Athens to Crete, in the summer it is nearly an hourly basis; in winter time it is Olympic and Aegean so you have some flights in the morning, some flights in the afternoon and late evening, so there are a number of flights.

Q221 ***Chairman:*** Let me take this a little further. I think the Committee was not aware that you had an arrangement in Athens where you could have meetings there, but if you cannot tell us straight out could you give us supplementary evidence of, say, over the last year how many visits have you had for meetings from outside visitors who are not employed by the Agency? It is this matter of the inconvenience of getting to Crete that we are not clear about and it would be helpful if we knew how many people a year come to visit you. Could you give us that information?
Dr Helmbrecht: I can give it—I apologise not now. The basic information is that the Athens office, which is paid for by the Greek Government, we have had since the autumn of this year. We did not have it before; so the last five years it has really meant meetings in Heraklion or meetings at other places in Europe.
Dr Beale: What you are getting at, I think—and I can point out another aspect of it—when I go to get a flight from Heraklion to Athens in the winter I only need to leave the office about half an hour to get to the airport and through to the departure gate. If I need to go to Heathrow from many places in London I need to give it an hour, and at Heathrow I may need to give a good hour to get through check in and security. There are certainly drawbacks but there are benefits of being in a quiet airport during the winter.

Q222 ***Chairman:*** What I am thinking about is the inconvenience of people visiting you for meetings and business, who have to spend probably an extra night getting to Crete and an extra night getting back. It sounds like two nights in Athens, which is highly inconvenient and expensive, and what I am trying to get at is how big is this problem? And one can only assess how big the problem is if we get some sort of an idea how many people are affected by this, because it seems that the most highly inconvenient way of setting up an agency is if people have to spend a night on the way back. But if you could give us some idea of your experience since you set up the Athens office—was that July?
Dr Beale: That was this autumn. In fact, literally about a month ago, two months ago it was first opened. We have not had any major meetings since then in there; we have had meetings of various expert groups in the Athens office—two so far since it opened—but next year we will be holding the Management Board meeting there, and possibly the Permanent Stakeholders Group meeting there, twice-yearly for both of those.
Chairman: That sounds a good start.
Lord Hannay of Chiswick: Presumably—it is perhaps a little unfair to say this—the actual decision to open the Athens office simply validates all the questions that the Chairman has been putting to you.

Chairman: Exactly.

Q223 ***Lord Hannay of Chiswick:*** Because under normal circumstances it would not be a very useful application of resources to have an office in Athens which is simply there in order to provide meeting rooms. But clearly the pressure from people who do not particularly like spending the two nights that going to Heraklion necessitates has led to this decision. So it is a kind of sticking plaster decision to what I can only suggest was a somewhat hasty decision in the first place as to the siting of the Agency.
Dr Helmbrecht: If I can make a remark. We tried to avoid this problem in the past by having meetings somewhere else in Europe.

Q224 ***Lord Hannay of Chiswick:*** But then that is inconvenient for the staff of the Agency because they have to be absent for substantial amounts of time.
Dr Helmbrecht: Then it is some kind of customer orientation to say that we take the burden.

Q225 ***Lord Hodgson of Astley Abbotts:*** I think this point has been largely covered but it is not only the time wasted of visitors, it is the time wasted of valuable senior staff going to Athens or going somewhere else. When you give the additional evidence could you tell us what time would you would have to leave your office in Heraklion to attend the meeting at 10 o'clock this morning, if you had flown straight from Heraklion? You would obviously have to overnight somewhere but what was the latest time you could have left your office?
Dr Helmbrecht: I have to think because I came from Paris last night. As Jeremy said, it is a very short way to the airport; it is very easy to board; it is a 50-minute flight. So sometimes if you take the time to go there, if you have a big city and you have to go through the traffic, it can take longer in the end. I can tell you the other way around because I know that when I leave this evening I will be in the office tomorrow at about 10 o'clock.

Q226 ***Chairman:*** I think we have covered the ground and made the point. Thank you very much for coming; you have come a very long way.
Dr Beale: It was no problem!
Chairman: We very much appreciate the evidence you have given us and, as I said at the beginning, if you wish to expand upon it we would be most obliged if you would let us know as soon as possible. Thank you very much, that concludes the meeting.

WEDNESDAY 6 JANUARY 2010

Present	Avebury, L	Jopling, L (Chairman)
	Garden of Frognal, B	Mackenzie of Framwellgate, L
	Hannay of Chiswick, L	Mawson, L
	Harrison, L	Richard, L
	Hodgson of Astley Abbotts, L	

Examination of Witness

Witness: Professor Ross Anderson, Professor of Security Engineering, Cambridge University, examined.

Q227 ***Chairman:*** Good morning. Thank you very much indeed for coming to give evidence in front of us. We really appreciate that. We appreciate all those who are kind enough to do this. Perhaps you would like to introduce yourself for the record, Professor, and if you would like to make some introductory comments, we would be delighted to hear them.

Professor Anderson: Thank you, my Lord Chairman. I am Ross Anderson. I am Professor of Security Engineering at Cambridge. I also chair the Foundation for Information Policy Research, which tries to be the UK's leading internet policy think-tank that brings together people interested in security: engineers, economists, lawyers, and others involved in technology policy.

Q228 ***Chairman:*** Thank you. Let us begin. You will agree, I think, that most security issues either affect everyone or they are very localised. Could you tell us whether you see value in regional initiatives, as envisaged by the Commission Communication, or whether you would rather wait for action to be taken at a global level?

Professor Anderson: Internet security is a global public good, like scientific research. As we know from elementary economics, global public goods are underprovided: there are many free-riders. But that does not mean that they are not provided at all. In the field of scientific research, for example, an awful lot of the heavy lifting is done by the USA for the simple reason that their industry can capture much of the spin-off, much of the profit, from scientific research. Does this mean that Europe does nothing? Not at all. We have European scientific programmes, the various framework programmes, because it makes more sense to invest in some kinds of science at a European level, because if an idea that I have is not captured by a UK firm, it may be captured by a German one or a Spanish one or whatever. We find exactly the same mechanisms when it comes to internet security. At present, if a bad thing happens, say a bad man in Moscow sends out a million phish, if you are the Commissioner of the Metropolitan Police you are tempted to say, "Only 1% of these will end up in my manor, within the M25"—because London is, roughly speaking, 1% of what goes on online—but America is 25%, "so, rather than my spending my budget on this, let us let the FBI do the heavy lifting." At present we see that it is difficult for even forces like the Met to sustain interest in electronic crime: their initiatives come and go over the years and are forever being squeezed. As a practical matter, much of the work is left to the FBI and other US organisations. However, that would change if we could get a European initiative together, backed by a plurality of Member States, because all of a sudden Europe would become a larger part of the internet than the US is, and so there would be economic logic in investing in protection.

Q229 ***Chairman:*** But would not a European organisation of that sort be a poor relation of the FBI even then?

Professor Anderson: There is obviously a problem here and it is tied up with how the European Union develops over the next generation or so. Will it remain a loose confederation or will it become, as some prefer, an ever-closer Union? I do not want to get involved in that particular argument, but if you do see a future with an ever-closer Union, then you would naturally see a future in which an organisation such as ENISA played an ever more significant role. If you prefer the confederate type of approach, then an organisation which majored on co-operation between Europe's police forces and, perhaps, as the European Union suggests, between Europe's CERTs might be the way to go. In the meantime, as we cannot make up our minds, perhaps both paths are worth pursuing.

Chairman: Before turning to Lord Hodgson, I should say that we will be coming to ENISA later on in this session.

Q230 ***Lord Hodgson of Astley Abbotts:*** If the UK has 1% and the US has 25% of the world's internet traffic, what percentage does the EU cover?

Professor Anderson: I think it is roughly the same as the USA, perhaps slightly more. I do not have the figures to hand, but in terms of population, GNP and so on, you would expect that.

Q231 ***Lord Avebury:*** When Mr Andrea Servida from the Commission gave evidence to the Committee on 2 December he drew attention to an agreement between the European Union and the US on strengthening their co-operation on resilience and security in the internet. Through which agency is that being done? Is it through police agencies or in some other manner?
Professor Anderson: I am not sure I am aware of which agreement you are referring to.

Q232 ***Lord Avebury:*** He was not more specific than that. He just said that there had been an agreement reached between the European Union and the United States to strengthen co-operation on resilience and security.
Professor Anderson: I am afraid I am not aware of any details. There are many such discussions that have been ongoing for many years, but I do not know that particular recent history.

Q233 ***Lord Avebury:*** You do not think there is an agency for doing that, or if there was one you would be aware of it.
Professor Anderson: The problem is that this is a multi-stakeholder business. It involves not just governments and governmental bodies—some CERTs are governmental bodies, some are private—but it also involves, of course, the big internet service providers, the big software companies and many other players. It is complex and messy.

Q234 ***Chairman:*** Maybe we could draw your attention to that piece of evidence, and if you want to send us a supplementary note you could do that.
Professor Anderson: Sure.

Q235 ***Lord Mackenzie of Framwellgate:*** Good morning. I have a point of clarification. You compared the FBI dealing with the American problem with the Metropolitan Police Commissioner. Does the Metropolitan Police Commissioner represent the whole of the country when it comes to these issues, or would he just be representing the Met? It is not a like-with-like comparison, because obviously the FBI is a federal bureau whereas the Met looks after the London area.
Professor Anderson: That is a fair point. The Met has historically tended to lead on computer crime for about 20 years or so, but, as I mentioned, it is something that has come and gone according to the interests of particular officers and the funding that was available. However, the Met does not by any means have a monopoly of action on online crime. When online crime involves banking, for example, then that tends to fall within the bailiwick of the City of London Police, and this creates a bit of a split because how a bad thing on the internet typically affects a user is that you end up getting a debit on your credit card statement that you do not agree with and the fact that there is not a single police body dealing with all the aspects of bad things on the internet is one of the problems.

Q236 ***Lord Mackenzie of Framwellgate:*** To add to that, would it be worthwhile to consider creating a national body—perhaps the Met could take it over, I do not know—to deal with it on a national basis as opposed to each force dealing with its own problems?
Professor Anderson: It would certainly be useful to have a single body that dealt with online crime, including malware and other things that affect the infrastructure, and things like bank fraud that affect the end-users. The current arrangements are not satisfactory. Whether that would be part of some eventual British FBI or whatever is, of course, one of these policy issues that comes round again and again.

Q237 ***Lord Mackenzie of Framwellgate:*** I was just thinking that we did it with child pornography, for example. The organisation that oversees that seems to be a national body looking after the whole of the UK.
Professor Anderson: Yes. CEOP is part of the Serious and Organised Crime Agency. Again, it perhaps does not make much sense to have that particular aspect of online crime set aside into a small body of half a dozen or a dozen people who do not really have serious technical expertise. That has led to problems in the past when prosecutors have perhaps been a little bit too credulous about credit card data. It would have been better had we had a larger body dealing with all the aspects of online crime which had in-house technical expertise and which could have done a better job.

Q238 ***Chairman:*** Following up on what you have just said about the City of London Police, which of course is a very much smaller organisation than the Metropolitan Police, if the City of London Police had responsibility for cyber-crime in the city, do you think they have adequate resources to deal with that problem?
Professor Anderson: I think the main problem with the City of London Police's unit is that it is largely financed by the banks. This obviously gives them a certain perspective on things. There has been much criticism over the years, including by the Science and Technology Committee of this House a couple of years ago, of the fact that people who are victims of online fraud were supposed to report that to their banks rather than to the police. As a result, the online fraud figures went down but reporting online fraud became more difficult, and there is always a concern that there may be bias in dealing with those kinds of

online fraud that involve insiders. The banks may be less willing to take to the police complaints which involve some suspicion of internal malfeasance. This always casts a question mark over the effectiveness and integrity of the police in online crime and that would be better cleared up.

Q239 ***Lord Hannay of Chiswick:*** Are you suggesting that the FBI does have a 50-State responsibility for this particular area, despite the extreme jealousy with which individual State police forces and city police forces in the United States defend their patches, and that would show us the way in which we might do it, or is it, in fact, just as subdivided as we are? Second, I was fascinated to hear that the great ideological debate about the direction in which the European Union will move has managed to flow over into the cyber area, but, given my own views that that ideological discussion will never be resolved in the direction of either of the two very clear-cut alternatives you put, on which side does work on a regional basis come in Europe on cyber if we are going to be muddling along in the future somewhere between those two extremes?
Professor Anderson: In terms of making progress in Europe, what is most needed is that we adopt, for the time being, a multi-stakeholder approach. The European Union document itself is somewhat equivocal on this. It says at one point that progress in cyber-security will require a multi-stakeholder approach and then in its recommendations it implies that the thing should be driven by national CERTs. The problem is that national CERTs only have a fraction of the necessary expertise, and if you limit effective action to government bodies then you are in effect cutting out the communication service providers, the electric power companies, and the various other private utilities which, like it or not, control most of Europe's critical national infrastructure. You are also cutting out various NGOs and academics and others who have good expertise, and are also, for example in the case of the UK, probably marginalising other government bodies that have or are building relevant expertise, such as the National Physical Laboratory. What is needed to drive this forward is a big tent, rather than saying, "Let's have an initiative which will try to put the CERTs at the centre of things." The Government CERTs are basically a later add on. CERTs started off, in effect, as volunteer organisations: people rolled their sleeves up and started dealing with the problems that arose. Some years ago, various CERTs acquired a government imprimatur that was set up by government, but they are by no means the whole game. For the meantime we should avoid actions which result in responsibility being given to some subset of all the effective players and stakeholders.

Q240 ***Lord Hannay of Chiswick:*** There is a later question which will deal with this issue of national CERTs. You might like to look at the evidence that we took, but both the Commission, I think I am right in saying, and ENISA made it very clear that they did not think that the whole matter should be handled by 27 national CERTs; they merely thought that some of the smaller Member States that had no organisation at all would benefit well by having national CERTs but they thought that the continued existence in countries like the UK of a multiplicity of stakeholders was the right approach, so they basically blurred the line you have drawn there. That evidence is there. That seems to me to be slightly different from what the Communication appears to say.
Professor Anderson: In that case, I would agree with that. We certainly want to keep the broad spectrum of players in the UK engaged in this task.

Q241 ***Lord Hannay of Chiswick:*** And on the FBI?
Professor Anderson: This gets us into another piece of territory. One thing I have observed over the past 20 or so years is that there is a very different approach in America from here to dealing with law enforcement problems that can cross more than one jurisdiction. In America, agencies will compete to get convictions; whereas in Britain, all too often agencies compete to pass the buck. For example, we have been involved in a number of fora and at a number of times in looking at disputed online transactions of various kinds, and when we try to get various people interested (the FSA, the Ombudsman, the Metropolitan Police, the Bank of England, the Treasury or whatever) there is always a good excuse why this is somebody else's problem. In America, because the institutional culture is different, because law enforcement bodies compete to get scalps, they compete to put bad people behind bars—and also that the Sheriff can be re-elected or whatever—you get a different approach. The FBI is rather active with operations such as recent Operation Bot Roast for example, where they specifically tasked some people to go out to catch and put in jail the people who were running botnets. We do not see that kind of action in the UK and I do not know what sort of institutional changes would be needed to shift agencies' attitudes towards the American attitude.

Q242 ***Lord Mawson:*** Is it not the point that the whole discussion about the internet is an entrepreneurial environment, and a lot of the discussion about big tents and all of that stuff is about a world that operates up here somewhere and all the real stuff is happening down here? Is not the American example an illustration that if we really want to get hold of this environment seriously, an environment that is growing at quite a rate, we do

fundamentally have to change the way in which we engage with this? Is that not the thing the Americans have discovered? In many ways, discussion of this feels like old men in new clothes: we are trying to apply to it a set of processes and systems and ways of thinking that fundamentally do not apply to this world that is emerging around the internet. It is like two worlds passing in the night. It often feels like this discussion. Those of us who have spent a bit of time working with this environment know what a different kind of world it is. We write reports and do policies and have the same sorts of old discussions about it, but, fundamentally, they are worlds passing in the night and the only way to get hold of this new emerging environment is to create the kind of competitive entrepreneurial cultures that can really stimulate entrepreneurs and others to engage with the problem. Is that not the dilemma we face?

Professor Anderson: Indeed, one of my FIPR colleagues, Nicholas Bohm, once remarked that the arguments of lawyers and engineers "pass through each other like angry ghosts." This is exactly one of the problems that FIPR has been trying to deal with over the past 10 years. There are a number of other aspects to the problem. The first is the technology aspect: whether people are aware of technology or are technophobic or are simply not interested. In order to make technology policy, one has to be aware of the boundaries, and yet the policy establishment in the UK tends to be drawn from people with degrees in history and subjects like that. This is something on which many have remarked. Why doesn't the Civil Service recruit more engineers, scientists, mathematicians, economists, people who did a bit of programming at university? It is not enough that the Cabinet Secretary is an economist: we have to have more at all levels in the structure. The second thing is that trying to regulate all online things as internet policy might have been viable 15 years ago but it no longer is, because as one industry after another moves online you cannot just talk about the resilience of the internet infrastructure, you have to think about the resilience of communications, of electric power supply, of healthcare, of finance and so on, and so you need to start bringing in some more subject expertise. The issue between industry and government is a huge one. Government's time constant tends to be something like 15 years: when a new problem arises, it takes two or three elections for the questions and the possible answers to percolate through into the political system, and yet the software industry tends to have a time constant of something like 15 months. Regulating is really, really hard. You have to look for regulatory tools and mechanisms that are as technology neutral as possible, otherwise you will find that you are solving problems of three generations ago or five generations ago, technologically speaking. It is difficult and business does have a role to play. There are also fractures in business. One of the big dramas in my trade over the past 30 years has been the big fight between computer companies and phone companies. Phone companies have a 15-year time constant and computer companies a 15-month time constant. The result of that clash was that the old phone company technology and technology base got wiped out. Companies like Marconi were just destroyed and they were replaced by companies like Cisco and Juniper. This is not going to happen elsewhere—you cannot simply destroy the Government and replace it by Microsoft—but the tensions that led to that kind of tussle are real and we do not yet have good means of dealing with them.

Chairman: Thank you. You talked about the internet. Let us talk about that further.

Q243 ***Lord Richard:*** This inquiry is into the EU policy on protecting Europe from large-scale cyber-attacks. To do that we need to know something about the threats. What sort of threats does it face? Whence cometh they? What can we do about it? Can you help us on the threat? What sort of threats do you think the internet faces?

Professor Anderson: The Internet has historically faced a number of different threats. Back in 1989 there was the Morris worm which shut it down for a day or so—rapidly spreading malware. We have not seen any worms for about four or five years now because the threat environment there has changed somewhat. Another concern until a few years ago was monoculture because most of the systems that form the backbone of the internet were sold by Cisco. If somebody wrote some malware that turned all Cisco boxes into bricks, that was it. It was over. That is no longer such a concern because there are companies such as Juniper and Huawei hooked into that market and now at least the serious players have equipment diversity and we are no longer so exposed. As for what will go wrong, I am sure there will be large-scale failures in the future but they will tend to be those things that we have not thought of. That is in the nature of things, that as one networks systems, the failures tend to become fewer but larger. One just has to make sure that there is the resilience there to deal with them. As for threats that we know about and that will persist, botnets will no doubt continue to be a threat for a while. We cannot see any obvious technical or policy way of dealing with that. There will also be a problem from strategic play on the internet: not everybody's incentives are aligned and we do not have effective global regulation, so there may always be selfish behaviour that leads to failures of various kinds. There will be natural disasters and accidents which cause various parts of the internet to go down for a while. Hurricane Katrina, for example, knocked out a chunk of the internet for a while. We

have had various incidents where ships—dredgers, for example—have broken undersea cables. We had the Buncefield fire in the UK, and no doubt we will have more of that. But these I reckon will be local or at the most regional and dealt with within a few days and weeks.

Q244 ***Lord Richard:*** Really the issue this Committee is trying to grapple with is to what extent we need to modify international reaction towards the possibility of large-scale cyber attacks. I have to say the impression I got listening to the evidence, not yours particularly but the evidence of lots of other people, is that there are dangers and there are possible accidents but really it is not as desperate perhaps as some people say it is.

Professor Anderson: I would tend to agree with that. Criticality will increase all the time as more and more things come to depend on the internet. Large-scale cyber attacks, there are private individuals out there who control botnets with hundreds of thousands or even millions of machines. If you have to an attack resource of that scale then you can close down all but the very largest of websites on a whim. There is considerable nuisance value there if someone were to deploy it creatively. Of course if someone did make a confounded nuisance of himself then he might find that a lot of the world's policemen were trying to knock on his door. How that will work out, we do not know. Perhaps there will be new, innovative attacks whereby people combine scare techniques online with physical terrorist attacks in the real world, who knows? That is up to what people innovate in the future. All told, I do not think we are too badly off but there are some things that we have to think about and plan for as we become ever more dependent on online.

Q245 ***Lord Hodgson of Astley Abbotts:*** One has the impression that there are a small number of people or groups who carry out attacks with malice aforethought, but the much larger group are lonely anoraks sitting in their bedrooms and like taking on the system as a challenge, as a purely intellectual challenge as opposed to something with an objective in mind. Has any analysis been done of the threats and the nature of them, where they come from and what the response should be?

Professor Anderson: As far as malicious threats are concerned, particularly private sector malicious threats as opposed to state sector or natural disasters or whatever, there was a big change about five years ago when the bad guys got themselves organised. Up until then, we did see that the majority of the threats were teenagers showing off, people writing worms to impress their girlfriends or whatever, but since then we have seen the emergence of black markets, in which bad guys can trade. "My malware for your stolen credit card" perhaps, and where they can offer their services, "I will cash out stolen credit cards from ATMs for only 70%" or whatever. There are all sorts of people offering these goods and services for sale. That has really changed the nature of the game, because it means that the bad guys are getting the same benefits of specialisation that we started getting in the real economy around about the 1750s and which Adam Smith wrote about. This has meant, for example, that antivirus software no longer works particularly well. Why? Because it is written by professionals rather than by teenagers in their bedrooms. It is written, in effect, by companies. They may not be incorporated and they may be located in St Petersburg rather than Silicon Valley, but they do have R&D departments and they do have test departments and they do have customers—you know, with big watches and leather anoraks—and so they do take care to see to it that their malware is not detectable by the antivirus software before they sell it. As a result, antivirus software nowadays is catching perhaps 20 to 30% of new threats, rather than the 70 to 80% that it caught five years ago. The whole thing is becoming more focused, and it is becoming more focused on commercial exploitation: on sending spam; on phishing; on hosting bad stuff, providing so-called bullet-proof hosting; and, increasingly, on keyloggers (that is, software that sits in affected machines and tries to steal banking passwords). From the point of view of the police, this is bad news because the criminals are getting better at their job of stealing stuff. From the point of view of the national security establishment it is perhaps good news because it means that the bad guys are more focused on things that are not fundamentally a national security concern. That said, there is a caveat, because when you do have botnets under the control of bad people then it is possible for bad states to rent these botnets or to make use of malware that has been professionally written for criminal purposes, to use that malware for purposes, say, of espionage. It is a complex equation, but the big thing is that the bad guys are now organised. They are specialised in trade and becoming good at their jobs.

Q246 ***Lord Hannay of Chiswick:*** You covered a very wide range of risks and threats following Lord Richard's question, but you did not approach, as far as I could tell, the possibility that in a situation of international tension a government might wish to make life difficult for the other state with which it is in contention, but not to do so directly and attributably itself but by some indirect method for which the internet provides a plethora of possibilities. Do you think this is a risk we should be concerned about? We have had evidence produced on Estonia, Georgia and so on. There is the latest example people have talked

about, hacking into the evidence from East Anglia University about climate change. Do you think there is a risk out there of governments acting by proxy to cause damage to an adversary, or do you think that is all quite fanciful?

Professor Anderson: You might care to have a look at a paper we wrote last year called *The Snooping Dragon*. The story behind this was that in September 2008, round about the time of the Peking Olympics, we got a call for help from the Dalai Lama's private office: they believed that their machines had been compromised. One of my research students happened to be waiting in Delhi for his British visa to be renewed, so I told him to get on a train and go up to Dharamsala and see whether we could help them with it. It turned out that some 30-odd of their 50 machines had been compromised. They had had a rootkit installed on them and confidential information was being sucked away to China. We knew that this was an action, in effect, of the Chinese State, because the intelligence product was used by Chinese diplomats on more than one occasion when the Dalai Lama's staff were arranging for him to meet foreign dignitaries. The dignitaries were contacted by Chinese diplomats and warned off. Had it not been for that, then perhaps there might have been some difficulty in attribution. There was in fact a long debate about this, and after we wrote our paper there were some quite angry noises from China, saying, "We didn't do that," and they were trying to let on that this was being done by sub-state groups. When one reads the available literature on Chinese information warfare doctrine, it is apparently quite clear that they rely on using hacker groups/civilian auxiliaries as part of their overall strategy. I do not personally read Chinese; this is second-hand, but you can chase up the references in our paper. Apparently the Maoist doctrine of revolutionary warfare presupposes that if, say, the Americans drive their tanks to Peking then the Chinese people will rise up and surround them and do them much injury, so it is a very, very small step from here to saying that if we are in a state of information warfare with a foreign power then patriotic groups can be given a task and they can take it home and get on with it in their drawing room. There is apparently significant literature in Chinese archives. That is entirely consistent with what happened in the Dharamsala incident, that perhaps a hacker group was engaged in the initial penetration and once the rootkit was installed on the Tibetan computers then the Chinese police, military intelligence or whatever harvested and used the product. We may assume that is how a number of states will operate. It provides at least some cover of deniability if things go wrong.

Chairman: Thank you. We will obtain that paper and we shall include it as part of our written evidence in our original report.

Q247 ***Baroness Garden of Frognal:*** Professor Anderson, taking on the discussion of problems with the internet and possible disruptions, could you say whether it is possible that the internet could disrupt other parts of the critical national infrastructure and, for instance, cause power cuts or disrupt the water supply or be used in other ways either accidentally or deliberately to disrupt personal and business life?

Professor Anderson: At present, that could be done a bit. I fear that in the future it could be done an awful lot more. Take, for example, electric power. The typical electric power distribution network has, in effect, private communications. There are dedicated links used for safety and for control communication (that is, if you are going to switch particular circuit breakers or whatever). However, there is increasingly an extra layer of monitoring which uses the Internet, because it is simply cheaper, easier and more effective to use Internet technology for a power company to get an overall picture of its network configuration, of where faults are or may be, about the state of equipment and so on and so forth, and so, in addition to, if you like, the critical control network, there is ever greater reliance on stuff that is Internet-based. When I speak to people at power companies about whether the loss of the Internet would result in harm to their operations, they say, "No, no, no, we will just put more people in power stations and we will get by and put more people in substations," and in many substations they already have people because they use these as repair depots to go out and fix line faults. It is easy to anticipate that five years or 10 years down the line they will become more and more dependent on Internet-based systems. They will have cut back the reserve staffing levels they have more and more, and then if the Internet were to go away for three days or a week, we might see power failures resulting from that.

Q248 ***Baroness Garden of Frognal:*** And presumably the skills of the people operating that would begin to disappear as well, would they not? There would be a different set of skills required for the internet operations than from the people in the substations.

Professor Anderson: That is another problem altogether for the control systems community, in that they have an ageing workforce. This workforce is being allowed to shrink as people retire and as things that were previously manual operations become automated. It is very, very credible that Internet failures in 10 years time might cause power failures, and it may be prudent for regulators to start nudging power companies towards making appropriate contingency plans and reserve arrangements. This is something with which regulators such as Ofgem and its counterparts overseas are relatively familiar, because maintaining a dependable electricity supply means ensuring that there is adequate reserve—

reserve generation capacity in particular, so that if you have a sudden cold snap or a sudden spike in demand then you can meet it, and various market mechanisms are used by putting extra taxes on the price of electricity at normal times in order to fund the existence of required reserves, so regulators have experience of the generic sort of mechanisms that are probably required. Over time they probably have to think more about dependability and more about security of supply.

Q249 ***Lord Mawson:*** Do you think regulators can improve resilience, or should these matters be left to industry?
Professor Anderson: Ultimately it is industry that has to do the work: it is industry that has the engineers and it is industry that has the routers and the fibre and all the rest of it. The role of regulators in the case of the Internet will be similar to the role of the regulators in electricity supply, seeing to it that there is sufficient resilience in the system, whatever form that resilience might take. In the case of the Internet, for example, it is making sure that there is sufficient alternative routing and that you do not have single points of failure, such as national internet exchanges, which would cause widespread havoc if they failed.

Q250 ***Lord Avebury:*** I wonder if we could return to the threat of cyber-warfare and ask you what you think about the role of NATO in helping to keep the internet secure. Do you think it has a specific role? How do you think that should be co-ordinated with that of the European Commission?
Professor Anderson: I have some reservations about giving NATO a role here. First, on the technical side, NATO tried for many, many years and failed, for example, to get agreement between NATO Member States on technical standards for identifying friend and foe in the military, and if they cannot co-ordinate what is in effect a computer security problem in a closed and constrained military environment, then what chance would they have in a much more open and complex and freewheeling and multi-stakeholder open systems environment? The second reservation that I have about that is that, if you make NATO lead agency rather than the European Union or ENISA, you intrinsically make co-operation with the Russians much harder. An awful lot of internet bad stuff comes out of Russia and the Russians often have mixed feelings towards it. Some Russians are proud that their criminals are great at stealing money from Western banks and that their malware industry is profitable and so on and so forth. Parts of the Russian State may think that it is convenient that they have people on their territory who control large botnets. Other parts of the Russian State are affronted by this. We had a Russian police captain come to a conference here in London a couple of years ago who boasted how he had personally busted and closed down a gang that was blackmailing British casinos with denial-of-service attacks. Given the complexity of the political situation there, it might perhaps be an unnecessary provocation to put NATO in charge of cyber-security. I am also rather leery about equating cyber-security too much with cyber-warfare. There was an awful lot of talk about cyber-warfare starting about 10 years ago. It kind of died down after 9/11 because the agencies had other arguments with which to get money from the Treasury, but it has never been 100% convincing to me. Of course, using cyber-techniques you can do some of the things that agencies like GCHQ and the NSA have always done: you can try and blind someone's air defences in the first night on which you send your bombers into a foreign country and then use kinetic means to physically destroy the exchanges or switches or so on in which the air defence rests, but doing things on a sustained basis is difficult and doing things on a controlled basis is difficult. Cyber-warfare suffers from many of the problems of chemical warfare, in that the stuff may be blown back in your own face or it may not work or it may not work in predictable ways or, once you have used it once, the other side will put their gas masks on and then it is ineffective. Cyber-warfare just is not, at present, particularly dependable, except for specific one-off missions. I would therefore rather see cyber-security as an essentially civilian security thing but with some national security backstop and interest as far as critical infrastructure is concerned.

Q251 ***Lord Avebury:*** You would agree with the evidence that ENISA gave us that the military should become involved in protecting the internet only when the attacks are either assessed as being of a military nature or directed against the security of the European State. If you do agree with that and, according to an article in the *New York Times* on 13 December, *In Shift, US Talks to Russia on Internet Security,* since the technological response to the cyber-attacks on government computers is likely to be the same whether the target is civilian or military, do you not think there is an argument for close collaboration between the European Union and NATO agencies? What are we doing to identify the sources of these attacks on government computers in order to classify them as of a military nature, or of a security nature, or of a civilian nature and therefore to be left to the Commission to deal with?
Professor Anderson: That is a hard one, especially if the other side is going to be using freelancers (hackers, students or whatever). There are very regular reports of Chinese-targeted malware attacks, for example, which may be of a military nature against List X companies or maybe of an economic intelligence nature against companies whose ideas they are trying

to pinch. These could both be the same company. How do you classify such an attack? I suppose you can adopt the kind of strategy where, if you detect an attack coming from a country such as Russia or China, you first ask for the miscreants to be extradited, and if the country refuses you then perhaps take a somewhat harder line, but what do you do where there is a background noise, as is reported from China, of attacks on companies? It is a hard policy problem. It is not the sort of thing that we have come across before. By way of analogy, the difficult problem with cyber-crime is that all of a sudden it is a globalised version of petty crime, and our means of dealing with crime internationally are basically designed for Dr Crippen. If you have one identifiable or high-profile villainous person who has done something wicked like murdering his wife, which every government agrees is wicked, and you know that he is arriving on a boat at New York in two days' time and you have just invented the telegraph, well then, great, you fetch that guy and send him back. But with cyber-crime you may be having millions of attempts being made per hour, and perhaps hundreds of attempts per day succeeding, where a gang is trying to steal a few hundred pounds from people's bank accounts. Normally, a theft of a few hundred pounds is considered to be petty crime. If it is done on an industrial scale, it obviously is not, but if it is done internationally, how do you get the mechanisms to deal with it? Similarly, we do not have the concepts, let alone the mechanisms, of how to deal with a constant background noise of hacking attacks being made against Western companies from a foreign country, or, for that matter, for dealing with a constant background noise of attempted frauds by gangs in Russia against small and medium-sized businesses in the USA (which has been one of the news stories over the past six months).

Q252 ***Lord Avebury:*** Do you not think that at the very least there ought to be some mechanism for technological collaboration between the European Union and NATO so that the ways in which you first of all analyse and decide on the response to these multiple threats are well co-ordinated between the two agencies?
Professor Anderson: There may be room for some agency co-ordination, but I think there may also be room for new mechanisms of enforcement and new philosophies of enforcement. One idea that I have toyed with from time to time is the idea of randomised enforcement. At present, the police will try very, very hard to catch a murderer and they will probably ignore somebody who steals £300 from somebody's bank account. I would suggest that, instead, if someone reports a theft of £300 from their bank account, the police should with some probability—perhaps 1:10,000—investigate that with just the vigour that they would allocate to a murder. That way, if somebody committed many tens of thousands of times a theft of £300 from people's bank accounts, then eventually sooner or later they would find the Feds coming after them with vigour and with determination. Perhaps an approach like that might also give you a way of dealing with a constant background noise of hacking attacks from China.

Q253 ***Lord Richard:*** Perhaps I could try to sum this up as far as your own attitude is concerned, because if you are saying what I think you are saying then I find myself in considerable agreement with you so I need to make sure that you are saying what I think you are saying. As I understand it, you do not put very much credence to the idea of cyber-warfare and large-scale cyber-attacks, but you do put quite a lot of emphasis upon individual attempts to try to use the internet for criminal purposes. Is that about the distinction that you would draw, you do not think there is much danger of major cyber-attacks, of government attacking government or that sort of thing, but you do think the criminal possibilities are of course great?
Professor Anderson: At present there is a significant and growing amount of crime on the internet. There is also, apparently, a small but still significant amount of espionage-type activity going on. As for whether a government might use a big botnet to shut down some part of, say, Britain's infrastructure: suppose, for example, we were in a trade dispute with China or suppose the row at Copenhagen had been even more fierce and a Chinese botnet were used to shut down the websites of all Britain's major clearing banks. If that got to the stage that it was clearly going on and it could not be denied any more, then what sort of retaliation might be in order? The Chinese might have to take into account the possibility that the European Union would snap a punitive tariff on their exports or some other completely nontrivial diplomatic action would be taken. We might, for example, decide as the European Union that we were going to blackball communications with China, so that their exporting firms would have to use phones and faxes to communicate with customers in Europe. There are many, many possibilities on the menu for retaliation before you even start thinking about military means. To my way of thinking very few of these retaliatory measures are cyber-measures.

Q254 ***Lord Richard:*** Diplomatic responses or economic responses to a problem which has been created by, say, the Chinese.
Professor Anderson: If the Chinese created an economic problem for Britain by closing down bank websites, then the obvious response, given that we do

not have America's military power, would be some kind of economic response. This is an example I used 10 years ago when people were first talking about cyber-war: suppose that the West were to close down Iran's electricity grid and kill a few dozen people thereby. The Iranians would treat that exactly as if we had sent some planes into Isfahan or wherever and dropped some bombs and killed a few thousand people and retaliate. There is no special "Get out of jail" card for cyber, and so seeing cyber-warfare as something in a category of its own is perhaps a mistake. It may be at its most effective when it is combined with the with traditional kinetic military mechanisms. We hear, for example, that cyber-techniques were used to silence Iraq's air defences in the first days of Gulf War I. That seems a sensible use for the technology if you can find the exploits, but relying on cyber for prolonged, large-scale, strategic offensive against another country just does not seem to make sense, given the nature of the technology at the moment.

Q255 ***Lord Hodgson of Astley Abbotts:*** You have talked about worldwide petty crime which goes unrecorded, either because the sums in each case are trivial or because the institution that is involved with it, a perfectly reputable one, does not wish to admit malfeasance is going on inside their organisation and, therefore, their wish is to keep it quiet and not report it. Our previous inquiry was on money laundering. In those circumstances, you cannot keep offences of that sort quiet or you would be committing an offence because you are required to report money laundering. Where you believe money laundering may be taking place, you have to make a report to SOCA. Would it help improve our knowledge and, as a result, also improve the state of our defences either in the UK or Europe-wide if we had a similar requirement to report cases where you believed or had reason to believe a cyber-crime was taking place?

Professor Anderson: Absolutely. In America there are now laws in 30-odd states which require companies which have suffered a security compromise which has affected the privacy of individuals to notify all the individuals who could possibly have been affected. This has had a salutary effect in bringing things out into the open. Colleagues and I have recommended on a number of occasions that we get similar reporting rules in Europe, and it is interesting to see that the European Commission is moving towards doing this for telecommunication systems. In my view, it should be done more widely. It should be mandatory, for example, to report online and electronic frauds. Out of all the European Member States, at present only Britain and France publish figures. If you do not know what is going on, then you have difficulty in making appropriate policy responses to it. Another thing that would be good would be to have information by ISP on the numbers of infected machines, because at present we notice that some ISPs tend to have very many more infected machines than others. Broadly speaking, the bigger ISPs have more infected machines because smaller ISPs may come under pressure in respect of their peering arrangements if they send disproportionate quantities of spam, and so there is a bit of a market failure there which we could hope to fix if we had more information. The information per se would not be a complete fix but it would be a good step along the road. There are all sorts of reasons why we want more information and better reporting.

Q256 ***Chairman:*** Just have a guess as to how many reports that might amount to within a year. Lord Hodgson was talking about our previous inquiry on money laundering. We have expressed concern about the huge number of reports which were necessary with regard to money laundering. Just have a broad guess over a wide range of error as to how many reports we would be talking about if we moved in that way.

Professor Anderson: In Britain, current fraud and online fraud together is about half a billion pounds. Let us guesstimate that that is one million incidents of £500 each: it is more than 1% of the population but less than 10% of the population suffering every year. Scale that up to Europe and that would give you the size of the financial reporting operation. Of course this has to be automated. People have to build systems to collect the statistics and file the appropriate reports. It is not something that you could require on 30 days' notice, but certainly regulators should be taking a view that within some reasonable time period, two or three years, the banks should have built the systems to report that. In many cases they may have internal reporting mechanisms anyway for their own monitoring purposes. Similarly, when it comes to reporting things like infected machines, guesses hover around the 1%/2%/5% mark with infected machines, so a bit more than 1% per annum but perhaps not hugely more than that. If you have mechanisms for doing the reporting, then you first have the beginnings of the mechanisms that you need to provide incentives (for example, statutory penalties for ISPs which do not do something about infected machines within a particular period of time) and, second, you have to have the mechanisms to detect the infected machines themselves by observing that they are sending spam or whatever. There are a number of advantages for having decent reporting systems, in that the kind of reporting systems that you build overlap with the kinds of systems that you need for enforcement.

Q257 ***Chairman:*** It would be talking about a massive new burden on both private and public sectors.
Professor Anderson: I do not think the burdens there would be enormous. The banks should be monitoring fraud in any case. When I worked in the banking sector, as I did in the 1980s, I saw to it that the fraud reports came across my desk every Friday. You need computers to deal with the volumes nowadays, but, nonetheless, that is good management practice. It is something that we do in Britain and they do in France; there is no harm, it seems to me, in asking banks elsewhere in Europe to do the same. When it comes to monitoring bad stuff going on in ISPs, many small to medium-sized ISPs do that already. I do not see there is much harm in asking people like BT and Virgin to do it as well. Because of the economies of scale, they would probably be able to do it more cheaply.

Q258 ***Lord Mackenzie of Framwellgate:*** In the light of the evidence that you have given this morning and given the growing importance of the internet in commerce, in your judgment is the internet still safe for consumers to use? Does the Commission Communication make any difference to that?
Professor Anderson: There is an interesting question here because safety of the internet or security of the internet can mean two entirely different things: whether the bits get through (in other words, whether the infrastructure keeps working) and whether bad stuff happens to you as a result of doing transactions. To use a transport analogy: what are the security issues on the M6? Security issue one is that the IRA might blow up a bridge. That is a threat to the infrastructure. Security issue two is that a burglar from Birmingham who is not known to the police in London might come down and burgle your house and be back in Birmingham by breakfast time. These are two completely different things. The Commission is mostly about security of the infrastructure and ensuring that bits get from place A to place B, but the things which harm individuals are mostly about applications that run on the internet. In Britain the highest priority for action, in my view, is to do with banking regulation because we do not have anything like as strong consumer protection for people who do banking online and who use credit cards and so on as they have in America or even in the Netherlands, but that, I suppose, is not this particular Committee's subject. From the point of view of the consumers, what is really needed is for somebody to take the FSA by the scruff of the neck and give it a shake.

Q259 ***Lord Mackenzie of Framwellgate:*** Is it safe to use, in your judgment?
Professor Anderson: The internet would be safer to use if people who were defrauded online were guaranteed that they would get their money back. Then, the incentives, the proper incentives, would lie on the banks and on the service providers and the big commercial websites to crack down on fraud. That is not really to do with the kinds of security issues that the European Commission is considering in this document. That is a matter for another day, I suppose.

Q260 ***Lord Mackenzie of Framwellgate:*** Indeed, but of course confidence can be shaken in the whole system if fraud is allowed to succeed. People stop using it, presumably, to shop.
Professor Anderson: This is one of those things that I suppose could be described as a market failure, because merchants are not sufficiently motivated by the non-arriving online customers to go and lobby Members of the other place for tougher regulation of the banks.
Chairman: Let us turn to CERTs, which, for the record, are Computer Emergency Response Teams. Lord Hannay.

Q261 ***Lord Hannay of Chiswick:*** We had a brief discussion about it in an earlier exchange, but the EU's Communication sets out the idea of national CERTs which would cover more than just public sector infrastructure. As it has been explained to us in the evidence, the Commission and ENISA are not looking at that in an exclusive way, but they are saying that for a quite large number of Member States which have no CERTs at all this is the best place to start. They have explained, as I said before, that they do not believe the more complex sort of situation that we have here, with lots of industry CERTs as well as public sector CERTs, is in any sense a bad thing. They think it is a very good thing. It is a sort of higher form of CERT really. Does that make sense? Do you think that for small countries without any such thing it is valuable to start with a national CERT?
Professor Anderson: It would be valuable to have a national CERT, sure, but that should by no means be the only player. You would expect CERTs to arise in big user organisations. The University of Cambridge has a CERT, for example. It is just part of the infrastructure which has grown up naturally over the past 25 years or so that there will be one or more individuals in many large organisations that take on the responsibility, who know each other, who know each other's mobile phone numbers, who have cryptographic keys so that they can send encrypted messages to each other. By all means let there be government CERTs where there are not any, but let us not let them crowd out private sector activity, because it is usually the private sector activity that will provide the rapid response.

Q262 ***Chairman:*** You have mentioned, I think twice already, ENISA, which, again for the record, is the European Network and Information Security Agency.

Q263 ***Lord Harrison:*** Professor Anderson, we have had the occasional witness who is perhaps sceptical of activity in this sphere at the European level, who suggests it should be done globally or suggests it should be funnelled through NATO. From the evidence you have given us this morning, you have a clear idea that there is a role at the European level. You touched on it earlier in some of the answer to the earliest questions. I wonder if I could I invite you to expand on that, on the form that response could and ought to take, and whether the fledgling ENISA is the proper vehicle for that. If ENISA is such a vehicle, could you say whether it is sufficiently resourced? I do apologise for asking this last question. The Committee has been much exercised about the location of ENISA and I wondered whether you had anything sensible, on this very cold frozen day outside, to say about the attractions of where ENISA is currently located and whether it is an appropriate place to bring together the players that are needed within the European Union to further the cause that we meet in common about.

Professor Anderson: I do believe that the European Union has a significant role to play in internet policy, broadly defined, and that it is going to have an even larger role in the future. Over the past 10 years, since FIPR has been involved in lobbying on various issues, we have observed—and we observed it even before FIPR was founded—that more and more national parliaments like this one are not dealing with the important technology policy issues. Whether it is telecoms regulation or IP enforcement, it always ends up being a matter for Brussels. In the other place, in particular, honourable Members seem mostly concerned with "red top" issues that will get a headline: dodgy auctions or child pornography or whatever. The serious action is being done in Brussels and that is where the serious players go and lobby and where the serious decisions are taken. Of course the European Union is going to have a role to play in this. Of course it should have a centre of technical expertise. There are a number of very able individuals within the European Commission who are technology literate and aware of the issues, but there is a benefit in having a place which has a clear mission which provides institutional continuity, a permanent seat at all the relevant tables at all the relevant Committees. Yes, the European Union needs an organisation. Whether it is an organisation like GCHQ or an organisation like the BSI in Germany or an organisation like the National Physical Laboratory in the UK is of course a separate question. If you are going to have a body (which we might as well call ENISA), there is then a question on what specific roles it should play in Europe, and this is obviously constrained by Member State sensitivities. We hear, for example, that British and French agencies lobbied hard to prevent ENISA, when it was founded, being too central, too powerful or too technically competent. I spoke to various officials from the Netherlands who were most upset about this but were not, given the pre-Lisbon power structures within Brussels, able to do very much about it. How can we improve ENISA (or whatever that body might be named in the future)? Location does matter. Ideally, I would think ENISA should be located in Brussels so that the expertise is there available on tap, so that people are having coffee and having lunch and having tea and having dinner with the movers and shakers within the European Commission, within the Parliament and elsewhere. That would be ideal. If policy dictates that it be in Greece, then for goodness' sake it should be within a 20-minute taxi ride of Athens airport. There is not just an issue of convenience in terms of being able to lobby people, in terms of being able to make a trip to Brussels a day trip; there is also an issue of recruitment and retention of high grade technical staff. Good software people like to be in places where there are other good software people. Brussels' neighbourhood is survivable because there is KU Leuven, there is Université Catholique de Louvain, there are various start-ups, there are various things going on. Another good place to have it would be, say, near Stansted Airport, because then people could be part of the wider Cambridge community. Another possibility might be near Munich. If it has to be in Greece, then put it in Athens. Putting it out in the wilds, in the back of beyond, has the effect that they go and recruit some bright young computer science PhD from Germany, who goes there for six months, gets a great tan and lies around on the beach, then gets bored out of his mind and realises that his career is not going to go anywhere because he is not doing anything useful. He has nobody interesting to talk to and he is not getting any publications that would look good on his CV; he is getting out of touch with all the people in the swim of his trade, and, because he is a technical person, he cannot expect to rise to the top of the European bureaucracy. So he then thinks to himself, "Right, it's been a nice six months' holiday, but that is it. I'm out of it." That is fundamentally the problem: if you cannot attract and retain top class technical people, you cannot run an agency like that.

Q264 ***Lord Harrison:*** What about the resources side? Is ENISA properly resourced at the moment? I take all that you have said about the resource of people, experts, but just in terms of money and support?

Professor Anderson: I cannot say I have ever sat down and studied their budgets. They do seem a rather small agency for the kinds of tasks that they are setting themselves, but maybe these things just take time to build. If they were at Stansted, I think, realistically, GCHQ would be trying to stomp on them as hard as they could. If they were in Munich, for example, or in Frankfurt or in Brussels, then they would be better placed to fight their corner, to get more manpower, to get more budget, because they would have more contact, they would have more influence.

Q265 ***Lord Mawson:*** I am interested in your comment about the technical person not being able to rise to the top of the European Union. Is that not part of the problem? This environment we are talking about is dominating and increasingly will dominate the globe and the European Union in many, many forms, and yet those people who understand it are not capable, in your words, of "getting to the top of this organisation". Is that not a major problem?

Professor Anderson: It is a major problem everywhere, but in other organisations people have done something about it. When I was working for Barclays Bank in the mid-1980s there was a rule passed that nobody would get promoted to senior manager level (grade 3 in the Civil Service) until they had some IT on their CV. A suggestion a couple of years ago to this effect within the Civil Service was stomped on with great disdain, but, nonetheless, it remains the case that if you think of a government department nowadays, what is a government department but a website? It is a website to which you go, you put in some information, and it tells you to put in some money or it pays some money out to you. Whether you are talking about tax or pensions or agriculture or whatever, that is fundamentally what administration is about: it is about running complex socio-technical systems, which have often got complex outsourcing contracts, where you have to manage the evolution of a platform, where you have to keep on replacing applications on it in response to policy initiatives. That is fundamentally an administrative skill that our civil services—and I use the plural because it is not just Britain's problem, it is a wider problem—do not have. How do you fix that? We wrote a report in March last year for the Rowntree Reform Trust entitled *Database State*. In the first part of the report we criticised some existing government databases for being too intrusive on privacy grounds. That got much airtime in the press. In the second part of the report we made a number of suggestions for how Civil Service reforms and other structural changes could make government better at doing IT in the future. That got almost no press coverage. But when the Government responded to our report in December it was these constructive, helpful suggestions which drew forth the angriest response from the people who had written the Government's reply. This is a really, really big issue. How do you make the Civil Service competent, how do you make the European Commission competent at designing, procuring, maintaining, evolving and operating complex systems? Hey, the country that can first solve that problem will, I think, acquire significant competitive advantage.

Chairman: Professor, you have given us an outstanding morning and one which ideally will lead us up to our final evidence session a week today when the Minister, Lord West, is coming to give evidence. You have given us a broad approach, a thoughtful and a clear view on these matters. It has been most revealing. The Committee is massively grateful to you. We have had a first-class morning. Thank you very much indeed.

WEDNESDAY 13 JANUARY 2010

Present	Avebury, L	Hodgson of Astley Abbotts, L
	Dear, L	Jopling, L (Chairman)
	Garden of Frognal, B	Mackenzie of Framwellgate, L
	Hannay of Chiswick, L	Mawson, L
	Harrison, L	Richard, L

Examination of Witnesses

Witnesses: Lord West of Spithead, a Member of the House, Parliamentary Under-Secretary of State, Minister for Security and Counter-Terrorism, Home Office and Dr Steve Marsh, Deputy Director, Office of Cyber Security, examined.

Q266 ***Chairman:*** Minister, welcome. You have braved the snow—I gather you were a bit held up but you are in very good time indeed, and we are starting, I think, a little earlier than we might have anticipated—and straight from the rigours of replying to the Committee's debate last night, which was an interesting experience. Thank you for coming. You are aware that this is a public session, it is being broadcast live internally and it will later appear on *BBC Parliament*, I understand. If you feel afterwards you want to clarify or amplify any points please do not hesitate to let us have them. Obviously, we shall not ask you, as we do with most witnesses, to introduce yourself, because you are well-known to all of us, but would you like to make any opening remarks, or do you want to go straight into it?
Lord West of Spithead: All I would say is I think this is very timely by your Committee. This area of cyberspace is something that is very relevant. I think one only needed to listen to the media this morning and Google talking about what is happening in China. This is a very real issue and so it is timely. I think that is probably all I would say to kick off with, and then we will maybe move into the questioning and see where we go from there.

Q267 ***Chairman:*** Very good. Let me begin then: Minister, do you think that the problems on the internet could affect other parts of the critical national infrastructure and could they, for example, cause power cuts or the water to go off, or all those facilities which are so vital to the life and economy of the country?
Lord West of Spithead: Again, this is an important question. It is something we have looked at and, indeed, it is looked at continually. CPNI, really, are the people who look at this most closely; they are effectively based within the security service but I have a certain amount of oversight in ministerial terms of what they actually do. I think it might be worth saying that last year we produced the first ever Cyber Security Strategy for the United Kingdom. We set up, as part of that, an Office of Cyber Security and a Cyber Security Operations Centre. The Office of Cyber Security is based within the Cabinet Office, and that is the sort of head of all the policy and all the structure side of things, and the Cyber Security Operations Centre is down in the West Country, in Cheltenham, in what is known as the Doughnut—the big building there—in GCHQ. They are the ones who are the practitioners and know all the practical aspects of it and are able to focus on that sort of work, and they have just started producing their first set of reports. As part of the work being done by the Office of Cyber Security heading this up, critical national infrastructure is one of the many strands being looked at. As I say, a lot of work has already been done by CPNI. These areas are not as vulnerable as some other areas of the global internet. Very often they do not have direct connections to the internet itself, and of course if you have an air gap then that is the only time you can be absolutely sure that no one can actually get into your computer and mess around with it, or your systems and mess around there. There are, however, some connections; we are aware of those and they are monitored and looked at. I think we probably need to do more still and there is more going on, because as people get cleverer and cleverer there are other opportunities for them to do things. Of course, one can do all sorts of things either with a disk or with one of your little plug-ins, or something, if you can get someone on the inside to do something. In all of these things we have to look at how we can make sure it is safe. However, on the whole, our water distribution, in particular, is, I believe, at the moment, secure. In terms of the safety of it from people putting poisons in it, we have done a lot of work on that as well. That is a side issue but a huge amount of work in the last two years, and we are a lot safer there. In terms of power and the Grid, that probably is easier to affect than the water, but is still secure, and I am content with where we are at the moment. That does not mean we can be complacent, and we have to keep looking at this.

Q268 ***Lord Mawson:*** Good morning. It would be helpful if you could share a bit with the Committee about what work has been done in this whole area

around the Olympics question, and the possibilities of what may or may not happen around that time?
Lord West of Spithead: Are we talking in terms of the critical national infrastructure aspect, or other aspects of Olympic security?

Q269 ***Lord Mawson:*** Obviously, there are infrastructure aspects—there is Telephone House there, which is an important cable facility globally—and there is also the whole question of the effect of cyber warfare. Obviously, IT is going to be pretty crucial in terms of the running of the whole of that operation.
Lord West of Spithead: I think in terms of the Olympics the first thing I would say is there has been a lot of physical work to ensure that, for example, overhead power lines and everything all now go, as you are probably aware, underground; things like the sewage systems and things, some of that has been adjusted and we have protection in place for that, because all of North London's sewage suddenly shooting on to the Olympic site, which travels at about 40 miles an hour down three pipes (each of which is 12-inch bore) would be quite exciting, I think. Those aspects are being looked at as well. We have set in place very strict rules for how the voids are locked—these are the voids where cabling, water and things like this are carried, and telecommunications. Those voids are checked as well and then locked again; they are monitored, and their mechanisms, so that we know if anyone has gone into them. There, of course, could be attacks on the ticketing system and things like that. That is being worked on at the moment, to look at what can be done to protect that. I think what one needs to bear in mind all the time is that almost every single government, industrial and other site is under attack, probably quite regularly; there are always people trying to get into these things. So on the Olympic system, for example, we found there had been some attacks on that and we are aware of those and we are dealing with those, but it is something we have to constantly monitor. Going back to critical national infrastructure, I went for water and power, but the telecommunications infrastructure, clearly, has vulnerabilities because that, by definition, is connected. I think it is very interesting, if one thinks about it: we actually are better placed, say, than in the United States only because they went into the computer world so much before us and they were talking to each other on computer systems when we were still with quill pens (not quite but almost). We have come into the computer age, and things like our GSI.com, the government communications things, is actually very good and very well controlled. The Americans do not have an equivalent, and that is why Obama, when speaking about this, said he wants to have a major effort. They have just produced their new (I do not like the word "Tsar" because they were not particularly pleasant people but that is what they call them) cyber tsar, a man called Schmidt who we know well in this country. It is an area of great focus. They were talking in terms of, maybe, having to spend up to 17 billion to sort their systems out because the access to them is so easy; it is so easy to get in. There are so many entry points into it—several thousand. Indeed, we have actually worked very closely with them and we have helped them in looking at numbers of access points and things like this. They have a lot to do. We are much tighter. It is a bit of a digression but I thought it might be interesting to the Committee. So the telecommunications bit—I go back to that—by definition it has to be connected and, if one thinks of Digital Britain, the whole point is to utilise and use these things. To make it work well you have to be connected to people, and trying to do that and be absolutely secure is very difficult. A computer wants to tell you things—it is designed to tell you and pass information—and so what we are having to do is stop it doing that when we are putting these checks in. The same with communication systems; they are designed for you to link and talk, and the same thing applies. In the context of the Olympics, we have looked on site and we are doing things there; in the context nationally we are doing work to make sure our telecommunications sites are protected as well as they can be, and we work very closely with companies on this. BT (I think, Steve, you know the figure) have attacks of about 1,000 or more a week, do they not?
Dr Marsh: Yes.
Lord West of Spithead: It is thousands, to try and get into the BT systems, and that is the same with any of these companies. As I see it, we are toe-to-toe with these people today. I am very glad we have had our first Cyber Security Strategy. When I came into post two-and-a-half years ago one of the first things I was surprised by was that we did not, and I pushed from that moment on to get it. It took time to put it all together, we have now got it and we are now moving downtrack fast on this, but this is a battle that is raging today. Using words like "battle" is wrong, but it is a constant struggle; these people—and it ranges from state actors through serious organised crime through individual criminals through hackers, who might only do it because they just think it is fun—can cause unbelievable damage. One incident probably costs a small firm about £20,000; for a big firm it probably costs them £1–2 million, and this is just someone fiddling about. So it is still serious. I am sorry, I am probably rambling on a little bit too much. Another figure I would give is malware, the things like Trojans and things that come into your systems; they can go into your hard drive, sit there and when you talk about a certain thing they will say: "Right, we'll send that out" and you do not know it

is there. In the last 10 years, up until 2009, there were about 15 million types of malware around. Last year, 2009, there were 25 million. So you add 25 million and about 15 million and that shows the rate at which this is happening.

Q270 ***Lord Richard:*** My question follows on very much from what you have just been saying. I think some of us who have listened to the evidence in this Committee (speaking at least for myself) have some doubts as to how serious the threat is. What I think I would very much like from you is, really, an assessment of the seriousness of the threat; where you see it coming from and what do you see the threat to; what sort of actions it is we should be guarding ourselves against, and how much intergovernmental threat is there. Really, it is the analysis of how important this is and how threatening it is, which is bound to influence the proposition this Committee might make on what one should do about it.

Lord West of Spithead: What I would say is (and I hope what I was saying before indicates this) I believe the threat is very, very serious. I mentioned all those various actors, state actors—we know state actors have got into major industrial concerns and taken every bit of data, let us say, about an aeroplane engine. So they do not have to do any of the design work or anything; they have got it.

Q271 ***Lord Richard:*** State?

Lord West of Spithead: State actors—countries. There are instances of that, and countries doing other things; countries trying to get into other systems (as I say, we are quite well placed in this) but trying to get into them and certainly getting into companies' systems and trying to get into other systems. Serious organised crime, where we know this is costing, globally, several billion pounds already, is a really big issue. Smaller level crime, where people steal identities, get into a bank account and take a bit of money—those are at the lower level. I have mentioned hackers, and then, of course, one that I am particularly nervous about is terrorism. At the moment, terrorists have not really done this on a great scale but, of course, you can learn very quickly. As soon as you have got people who are good at this you can do that, so that clearly worries me—that they might move into this space. It is a different issue from use of the internet and all the webs for radicalisation, which they do already, of course, and there is a mass of those sites, and we are engaged in a struggle there where we take sites down and where we do all sorts of other things which I would not want to talk about, but there is a struggle going on there because that has a real impact. When you put all that together that is a very real and very serious threat. It is a very serious threat. As I say, two-and-a-half years ago, when I came, I said: "My goodness, we have got to do something" and we now have this strategy. People like Steve and the team in the Office of Cyber Security know very clearly I have been pushing them really hard to actually get things going before Christmas; I would not let them wait till after Christmas. We are really moving on these things. Now the Americans have got their Cyber Tsar we will work very closely with them and I think they will start to be able move because there are some areas where, as I say, they have real difficulty, but we work absolutely closely with them on these things. However, this is a very real and very serious threat. There are issues such as if you go into a system somewhere, let us say, and you destroy a power station (and one could do that in certain parts of the world because of their connectivity and how it is done—you can stop it functioning as a power station), well, is that an act of war? If you bombed it, it would be. The other thing is attribution. It is very, very difficult to find who has done this. I say there are state actors but this is not straightforward. When this happens it takes real skill and real time to find out. Can you then be 100% sure? Let us say you want to consider something as an act of war, can you take action? Is the attribution good enough? There are some really big issues. So one of the great chunks of work I have got the OCS doing is to do with legal and ethical stuff. I am expanding a bit beyond the question but these are all serious issues that we are addressing and have got to look at. I suppose my simple answer to you is: this is a major and serious threat which I do not believe a large number of people have taken as seriously as they should do. I think now we are doing that and I think we have got to get that message across to the public. I am in the process, with the OCS, of making sure we can get this across. At the lower level, when it is personal security, there are certain things people can do that make their laptop or whatever a lot safer. I have been talking about this grand scale of the state, and if the state decides to get into your laptop you are stuffed, basically, but normally that is not going to be happening. However, you can do simple things, if people are aware, that make you much safer and make your systems much safer. We are going to be educating people in that way, and it is across the whole range.

Chairman: Just before Lord Richard comes back, the Minister has to leave in 48 minutes. We have eight more questions after this and I have got three people coming in. Can we all bear this in mind because I would like to get through all the questions, as they are all very important?

Q272 ***Lord Richard:*** All I was going to say was (and perhaps it is a comment rather than a question) the impression I get firmly from what you have been

saying is that really you are running very hard in order to stay almost level with these possible threats.
Lord West of Spithead: I think in some areas that is true, but I am always a "glass-half-full" sort of person. I would say that we have done a huge amount now since last summer and we are moving forward fast. It is not as if nothing was done before. CESG down in Cheltenham did a lot of work on these sorts of areas; CPNI has been doing this work; BT and other companies are doing a lot of work. What the OCS is doing now is pulling all this together, making sure this is all properly co-ordinated, setting some new tasks and new things we have to do, and I am very positive about this. However, this is a huge, huge area of risk and danger—there is absolutely no doubt about it—and we do need to be very clear what we do about it. The Americans, who we deal with very closely, have the same issue. They, for example, are saying: "Well, is this the same as an attack, a kinetic attack? If it is, clearly, we can attack backwards." What should the authority be to do this? These things are happening like this. Is your automatic response to go back down there and destroy the thing that is doing it to you? We could do that but, actually, that is quite a high-scale thing, and do Ministers need to make a decision on it? There are some really big issues and we are wrestling with those sorts of things. In some of those areas there needs to be a proper debate—in some of the areas. One of the dangers I always have before these Committees is I could talk instantly at a level which would be very damaging to us and would give away all sorts of things, but I believe within the context of this global area of cyber security there are bits that need to have certain public debate and discussion, certainly Parliamentary. This ethical side and legal side absolutely needs to. We need to develop what action needs to be done there, and that is what we are doing at the moment.

Q273 ***Lord Hannay of Chiswick:*** Could I pick up, Minister, on something you have said, which chimes exactly with what I was going to ask you, which is the factor of attribution? We have, obviously, had evidence on the Estonian incident and we have had evidence on the Georgian incidents at the time of the hostilities there, and we have all woken up this morning to hear about how there are heroic Chinese people hacking into Chinese human rights activists. In all of these cases the states in question have been careful enough to keep the state fingerprints off, but it defies the imagination of most people, I think, to think that the states—Russia in one case and China in another—are not involved with something that is so obviously part of the state's interest. Having identified that as a problem, which I think you did too, what are the possible solutions to this which have not yet occurred to anyone? Is it conceivable that one could try to get the main countries which have capacity to do these things to agree that they would not allow people within their jurisdiction to do them—i.e. to try to find some kind of international instrument which would be a sort of non-aggression pact on it? As you say, if it gets to tit-for-tat it could be very damaging indeed. On the other hand, nobody is going to just sit back and allow it to be done to them all the time.
Lord West of Spithead: The answer to that is that there is work going on to look and see if we can come to some instruments on agreement amongst nations. I think the Russians have been working on one and come up with some proposals. The proposals they made are not really satisfactory to us because it constrains us but does not constrain them (I suppose that is the best way to put it). I think there is some merit in continuing to pursue this. There is no easy answer because, you are absolutely right, we can generally find, at a level that one cannot discuss, that it has come from a country. What we have now got to debate and we are debating is how do we actually approach this? If you go to the country, and I have done this personally to a specific country some years ago when I was Chief of Defence Intelligence, because they were doing it even then, and I went there and said, they immediately, of course, said: "We are very sorry. We didn't know this was going on. Thank you for letting us know and we will stop this instantly", and that day it stopped, and about four days later it started from a different set of computers in the same country, but not the same ones. It is extremely difficult to pin them down. When we go up to very high levels of classification one can find out all sorts of things and one could, I suppose, exhibit all sorts of information, but you do not want to give away your capabilities. Even then, if you are able to show that to these people I do not think necessarily they would stop. So it is very, very difficult. So does one do some damage back? I think this is where we need this debate. There is no easy answer. What we have got to do, of course, and we are doing a lot on, is make sure you are thoroughly protected and you know when someone is trying to get into your system; that you stop that happening; that you make your systems highly protective. Clearly, the most important ones you have to make them impossible to get into. There are concerns about what sorts of equipment are fitted into systems; is there something about that equipment that lets someone have access? There is a whole raft of areas like this which we are on top of, dealing with and looking at but, as I say, this is a real problem area. It is very, very difficult and there is not an easy answer.

Q274 ***Lord Avebury:*** You said a couple of times that we were working very closely with the Americans on these issues, particularly on the range of threats that

you have tried to identify. Does that mean that our priority is to work with the Americans rather than Europeans?

Lord West of Spithead: No. It stems, really, from the fact that, in terms of intelligence, we and the Americans have always been very, very close. If you think back to the '48 agreement where NSA and GCHQ were absolutely joined at the hip, in terms of the exchange of data, stemming from Bletchley Park and the War and all the data we gave to the Americans to enable them to do certain things, that has been a very longstanding thing. So we are very, very close to them. In terms of Europe, there are countries there that we deal more closely with than other ones. Really, in intelligence terms, you tend to try and deal bilaterally. We need to try to expand that within the European context, but probably one of the most difficult things is to get a whole range of nations all to exchange exactly the same data on very high intelligence levels, because they just will not do it. It is something we have had to work at now for some years within Europe, to try to do as best we can. When there has been a specific conflict, really, like in the Balkans, one can actually achieve more in terms of releasing high-grade material to do with people's lives. We have just got to keep working at this. However, there is no doubt that we are closest to the Americans because we have been doing it with them for so many years; we are absolutely closely linked in and alongside them. I have to say I think it is very fortunate for us, and, I believe, for a lot of the things I believe in, because they have an immense capability. One of the issues in terms of cyber is how many people are involved at certain times. We leverage a huge amount out of our structures like GCHQ and everything on this. The Americans have vast numbers. When you go to China there is an army of people who are involved in this area of work. When you have that number of people then this is a real issue. Indeed, I gave a little bit of a wake-up call, I believe, to the EU last year because I was trying to get them to be aware of how great this threat is. I said: "If I wished to actually find out about an EU directive, how to think about it and which way it is going, the best place to go is China because they have got more people working on it than you have". I said that specifically to give them a wake-up call. I think it has. That is absolutely right; we do have to work very closely with Europe. When I say how close we are that does not mean we do not work very closely with Europe, and it is absolutely right we should do it.

Chairman: We are down to less than five minutes for the eight remaining questions, but that leads straight on to Lady Garden.

Q275 ***Baroness Garden of Frognal:*** Minister, my question leads on from the previous discussion in military terms in some of your answers there. Should we be looking more to NATO to protect the internet than the EU Commission? What would you see as possible benefits, or indeed damage, if there was military oversight of the internet?

Lord West of Spithead: I do not think NATO is the appropriate body to do this. They are very much part of that military structure and, of course, they have done a certain amount of work in this area, and our OCS is linked into them. They have a set-up in Estonia that is doing some work. I do not think they would be the right one. As these things are very connected, if an individual member's security was threatened then I think they could be involved. As regards the EU, its role as the EU is not to protect the internet. I found this last year, because I find it quite difficult sometimes to deal with them when I am talking to them; I am not quite sure how much authority they have got to do certain things. Their job, really, is to co-ordinate and pull together to make sure the nations within Europe all realise this importance and work together, I believe; not for an EU structure to actually legislate and do things. I think that would be too difficult for them. So I think that is probably how I would see it. I would not see NATO being responsible for that. Yes, if the security of one nation was involved we could draw on some of their abilities. The EU needs to co-ordinate this response, and that is what I was trying to get when I went to the Commission; I was prodding them because, again, I do not believe they realised how serious this is. I think that is a general problem.

Chairman: That leads on to Lord Dear now.

Q276 ***Lord Dear:*** Minister, thank you. You have been particularly full in your answers. In fact, I think you have touched on my question already, which is specifically that the EU Commission envisages that European initiatives will lead on almost naturally to global activity. I wonder if you would like to tell us whether you are doing anything to ensure that that particularly will happen.

Lord West of Spithead: I think we need a bit of clarification—I am not sure exactly what they want to do.

Q277 ***Lord Dear:*** I may be wrong, but, as I understand it, it is taking the good practice which is evolving very rapidly in Europe out into countries which are, perhaps, not so well advanced as we are.

Lord West of Spithead: We are engaging with the critical information infrastructure protection (CIIP) and the various fora involved to try and help with this road map because it is so complex. I know we are talking with people like the Telecommunications Council, ENISA and those sorts of areas as well. I think the fact that we are a very close ally of the US gives us a very key role, actually, in this because lots of people forget (a Committee like this would not but a lot of people forget) that the whole of this cyber area is global—cyberspace is global more than almost

anything else; it has no borders at all. It is there and, therefore, you have absolutely got to get all nations involved. The fact we are very close with the US, that we have certain particular very, very good skills—we have some absolutely amazing people—means that we can influence things within Europe. I think it is fair to say that within this arena and within ENISA and all those arenas we are ahead of pretty well every country in Europe (they have little niches), but when it comes to the broad tapestry of this, therefore, we do need to work very closely and give assistance in getting this road map. I think we need to encourage the EU possibly in taking this thinking forward through the Internet Governance Forum or somewhere like that. We can do a lot, but we do need to make sure we have real clarity of what this roadmap intends to achieve and I do not think we have quite got that yet.

Q278 ***Lord Harrison:*** Minister, my question is to ask you how the Government is involved with the internet industry. It sounds to me from what you have already said that we have already made overtures to the internet industry. If that is so, can you say what the nature of such involvement was and what the Government hopes to get out of that?
Lord West of Spithead: This is a crucially important area. Obviously historically we have been involved with the industry; indeed in my two and a half years I have spoken to various groups where we pull in the telecommunications industry with things like TISAC and things like that; CESG has been closely involved with them and, of course, we have had very close Government links with BT and other providers. What was very clear to me was this had to be one of our top strands of the work. I have asked Steve particularly to focus on getting these links with industry, pulling them in so they are aware of what we are doing, making sure that BIS, ourselves, Defence and all the various departments are linked in to them as well so they are getting the same message from us all. I think there are very real opportunities for British industry to become leaders in this area. This area is so important globally that anything which can be done to enhance security has to be of value, whether it is procedural, and techniques and procedures to do it, or whether it is technical. The aim of the work we are doing is to leverage and accelerate and make better those links.

Q279 ***Lord Harrison:*** Has the industry been helpful?
Lord West of Spithead: Yes, industry has been helpful and we are in constant dialogue. I rather beat the drum about this; Steve is probably feeling bruised because I even said I need an industry person within CSOC down in Cheltenham. Has that now happened?
Dr Marsh: We are pursuing it, yes.
Lord West of Spithead: Pursuing means they have not done it yet! We need an industry person there and I have said we need that because we must have those very close links. It is a global issue and they are the people who run all of this. The bulk of the issues are commercial, they are not government controlled. We can look at a really crucial link and say, "That is so important to Government, nothing is going to be done to affect that in terms of what kit is used on it, how it is connected and things" and we do that. The bulk of the stuff is stuff where industry is responsible for it and therefore we have got to link and work with them.

Q280 ***Lord Mawson:*** Thank you for your last comment, I found that helpful. I have gone on a bit like a broken record at this Committee about the different cultures between government and the internet industry because the internet industry is an entrepreneurial industry. I am an entrepreneur and I have spent a lot of time trying to engage with government as an entrepreneur and what I have found is sometimes the words are all there, but when you dig below the surface of the words and the engagement of Civil Service and government, a lot of these relationships and understanding about this culture is not there. We have listened to quite a number of presentations at this Committee but I think there is still quite a gap. The talk is there but the reality of really understanding what this culture is about, creating an entrepreneurial response to these problems which you are describing as very serious problems, my sense of it is we are a very long way from doing it. When we have listened to some of these presentations, while civil servants turn up at meetings and hear reports and write policies, it is a great worry that there are not people from the internet industry—you were just making the point—right in the middle of all of that because these are two cultures passing in the night. My sense of it is they are still very much like that, they are not like that. I wonder what practical steps—you made your decision earlier—you are going to take to make sure that starts to happen. It has very profound implications for government itself and how we operate in practice and the future of the Civil Service, et cetera. There are very big things in these issues and I wonder what those practical steps are going to be.
Lord West of Spithead: It is very difficult for me to identify those at the moment because, as I say, Steve here is pushing this issue and I want to get someone from industry in. I think it is important to harness what is a wonderful entrepreneurial spirit we have in this country because that is the way we come up with innovation and ideas across the security area. I have been pressing this very hard. The SMEs and these other organisations, we will be having our first big event early this year which has the Home Office science and development branch, plus UKTI, DSO where this will be a thing where we invite people from countries all around the world looking specifically at security things, and I hope to tie in energy security on top of

that the following year. This is to give these opportunities you are talking about. There is always a clash clearly being entrepreneurial. It is quite difficult with government money. I know that; I bought a small ship on the telephone and gave my credit card as the authority for it and almost got court martialled many years ago. I am glad to say the ship was very useful and valuable for 10 years, but I learnt a lesson that one does not do that with government money. My legs were chopped off but I learnt a good lesson. You cannot play games with government money, it is a different sort of money, but we do need to harness the entrepreneurial aspect and business aspect and that is what we intend to do. That is exactly the pressure I have been putting on Steve, but I cannot give you the practical steps that are there. It would be wrong to pretend we have not had very good links before. CESG have very good links and very often these are youngsters and they all talk the same language, which I have to say is very difficult for me to understand half the time. We have got good links and they do talk, but we have got to make it better and we have got to open up and harness that ability.

Dr Marsh: I think that is the point. One of the key elements we need to pursue in this area and in some of the previous conversations we have had is the exchange of information, information about the threats, the vulnerabilities and so on, and that has to be both ways. A lot of that has to be developed within trusted environments. CPNI have also done a lot of work, as has CESG, to establish those trusted fora where this information can be exchanged both ways between government and the private sector. The problem we are struggling with is those mechanisms are quite hard to scale up. You tend to end up talking to large companies, big players and so on just because of the resource implications of that. You are quite right, we need to develop mechanisms where we are talking to a much broader range of the innovative entrepreneurial businesses in the UK, but it is difficult to see quite how we can do that and still maintain this trusted environment and that is the challenge we have.

Q281 ***Lord Mawson:*** Can I come back to you on that. My experience, having built an internet network around this country, was we did not talk, we brought some practitioners together in a room with some computers and we gathered bit by bit, piece by piece to build this network and work out how you build an IT network online for the social sector which works. It was not about policy papers, it was not about talk, it was about doing and it was out of the doing that relationships, trust and understanding, et cetera, came. There is an army of young people out there who have great expertise in the whole of this area. As an entrepreneur, if it was me, I would be trying to create an environment where some of those people are on the inside of this because these issues, it seems to me, are happening at quite a speed and you need to be able to respond very quickly and you need to have the mindset and the culture which can do that. My problem, because I can hear the words, is whenever I touch the culture that is meant to deal with some of these things in the area I am in, it is such a distance from the reality. I worry that in this area what you are telling us is really, really important, and I can believe that, we are very ill-prepared for what that means.

Lord West of Spithead: As I say, I have put a lot of pressure on this area; I have put a lot of pressure on Steve. I think the fact that he has suddenly started speaking shows the pressure he is under and we see it as very important and we will have to keep moving. It would be wrong for us—I think that was what Steve was trying to say—to say this is easy, it is not, it is like all the areas in this, but it is important and it is something I have pushed very hard. This issue of SMEs and small groups and small entrepreneurs is very important. We have been quite good with CPNI, for example, at talking at very highly classified levels with big companies because you can identify a person, get him properly cleared and do it. It is extremely difficult when you get a couple of people come walking through the door who are very, very good, but are you going to tell them exactly what the threats are and how they are coming in, these are the issues which have to be dealt with.

Q282 ***Lord Mawson:*** Is it not this point that bureaucracies talk to bureaucracies; where this stuff is not about bureaucracies, it is often about the small and individual groupings?

Lord West of Spithead: Absolutely. That is why, as I say, I am pushing so hard for SMEs and things like that but it is not easy.

Q283 ***Lord Avebury:*** Minister, you sent us a very helpful supplementary note on the Exercise White Noise, which dealt with the widespread failure of the telecommunication industry. Can I ask you about a concluding remark in that note where you said: "Some key areas where the response could be improved were identified by the exercise. These are being reviewed and action through the coming year will be taken to address the issues identified". Can you please elaborate on this and tell us what those issues were?

Lord West of Spithead: Yes. As you know, this was the first exercise of this type ever held and being a military man, as you can imagine, I am a great believer in exercising things because it bowls things out. The more you do them, when it happens for real then people know what they are doing. It does not mean you are absolutely prepared for the event that happens, but you are much better prepared to do the right sorts of things. If I can give a few examples because some of the lessons are things I would not want to have out in the open domain. For example, the

training to much better prepare BIS staff for their specific roles, it was quite clear they were not trained as well as they should be for specific roles which were required in an emergency. We need better training for some of the crisis leadership skills. Some of the people found themselves in crisis leadership positions and they were not really prepared for that, so we need to do better in that area. When you do an exercise, part of the value of it is preparing it, working out what you are doing and that makes you think hard about it. We need to be even better prepared and I think we could have more background material. We need to have improved communications management SOPs for during the exercise. Basically we need to have it set out better in a template to do it so we can draw even more from it and then get proper lessons. With any exercise you always need to make sure the lessons learnt are actually learnt. I have constantly been horrified over 43 years how I end up doing an exercise I have done before and it is the same bloody lessons again and they still have not been learnt. Then sometimes you go into war and you find they have not learnt the bloody lessons. You have got to make sure lessons are implemented and that is clearly an important thing. We have identified specific improvements in terms of practical handling of the emergency by the BIS team in relation to management shift changes and things like that, co-ordination with the centre and with other Government departments, which was not as good as it should be. There are certain aspects to do with improvements and information management, better technological solutions to some of these problems. As you know, they took down the basic landline system and took down the mobile system and we really need some better technological solutions. This comes back to the things we are asking of industry. We produced again the first ever science and innovation strategy for security last summer, with the first of the brochures looking at areas we need to look at and this is one of the areas we need to get industry and entrepreneurs to look at. Academe, industry, we have gone out and said, "Look, if you look at this, there is money in this". I want to finally try and tie money to the sort of money which is likely to be around in this country and globally if you can get an answer to things because it helps entrepreneurs and industry to do development, pay for development and do certain things. I would not want to say any more than that, but that is a package of the sorts of things we have learnt from it and we need to do another one. This is something one wants to exercise and very often one can do these things with a chunk and a lower level to do a bit, before you do the big grand one, because there are costs involved in that, to make sure you have learnt all these little lessons and then put it together. You have got to move ahead like that.

Q284 ***Lord Avebury:*** I am wondering how you disseminate the results of this exercise because when I put Exercise White Noise into Google, I came up with only two pages and some of the entries in the two pages were repetition. The only public authority which seemed to have made any comment on the outcome was the Government Office of the North East. There is a myriad of organisations which were said to have taken part; how are they learning the lessons you have identified this morning?
Lord West of Spithead: I have to say, I do not know the specific answer to that and I would have to come back on that because I am not quite sure how it was disseminated. I can give a spot answer to that. Clearly some of the things, I think you know, are things one would not want to put on the web, but there will be some which I am sure could have been. I would need to come back with an answer to the Committee on that. I do not know exactly how it was disseminated, how that was done and how those lessons learnt will be pushed out.

Q285 ***Chairman:*** Can you let us have a note on that as soon as you can, that would be helpful.
Lord West of Spithead: Absolutely.

Q286 ***Lord Hannay of Chiswick:*** In the EU Communication we are looking at it was suggested there should be a European-wide exercise on large-scale network security incidents and this should be held by the end of 2010. The Explanatory Memorandum which your Department gave us described that as highly aspirational, which I take it to be *Yes Minister* speak for off the wall. Although the word 'aspirational' has become slightly more fashionable within Government circles in the last few days, can you perhaps tell us what your view about the proposal for a pan-European exercise is and a realistic idea of when it might usefully be set up?
Lord West of Spithead: I have to say, I think the thought of a pan-European exercise on the scale they are talking about is really not a starter. If they tried to do it, and it would be them probably without proper preparation, you would not learn anything from it, it would just be a bit of a mess. That is my own personal view and I think the team, on looking at it, are very concerned about being able to achieve that. That does not mean we are not very closely linked in with them because we are because we believe an exercise programme is important. What they need to do is set their sights lower and do a rather smaller-scale exercise first of all, learn the lessons from that and see what the sorts of problems and issues are and then move to something bigger. What they are proposing at the moment is such a large-scale thing, just getting all the preparations in place, if it is going to be meaningful, is going to be pretty damn near impossible. As a Minister I should not say it is off the wall, but I think it is probably a bit hopeful. It is the sort of thing where a midshipman, if you told him to go away and organise something, he would come

back with this great plan and you would think, right, boy, try and implement that and it would be a shambles, it is that sort of thing.

Q287 ***Lord Mackenzie of Framwellgate:*** You have almost answered the question, Lord West. Obviously you are a very strong supporter of the old adage that failing to plan is planning to fail. Of course, Lord Hannay has touched on the exercise point. As you know from your experience, we have a very poor record of involvement in civil exercises with NATO and my question is a specific one. As the UK, would we participate in an EU exercise—you can give a personal view, presumably you cannot give a Government view—and what would you expect to get out of such a multinational exercise?

Lord West of Spithead: The answer is I would expect to be fully involved in an EU exercise of this type. I would hope that we will play a significant part in planning it. As I alluded to earlier, I think we have got a lot of real skills in this area; we have got some amazingly competent people. Some of the youngsters that are used down in CESG and GCHQ and places like that have incredible skills. As an aside, it is quite interesting, we have some of the best mathematicians in the world and the Americans still value them so immensely, but what is gorgeous in this doughnut in GCHQ—everything is connected, everything inside there is so highly classified they do not even have compartments, apart from a couple of them, because they have all got that classification, everything is done by flash and internet, the mathematicians have insisted on having blackboards, which I think is rather fun, they have a blackboard and chalk; you cannot stop the world's best mathematicians having a blackboard—their ability to get into what I call 'lower grade codes', to crack things like this, to come up with ideas for things; and on the internet side, the ability of some of these youngsters, some of whom have been naughty boys in the past who now are on our side means we can add considerably to the planning of this. I would hope we would be very heavily involved in that and it would certainly be our intention of being very firmly locked in. On the NATO side of exercises, that has not taken off yet but, again, I would hope we would be more involved. The MoD tends to lead that sort of area and I know they intend doing that. There is no doubt, and I am digressing a little here, cyber warfare is a new domain of warfare which is extremely serious where, again, I do not think up until very recently we have realised that this is a domain we have to take amazingly seriously in defence terms, in MoD terms when you are fighting, because you can now influence the battlefield quite dramatically in cyberspace because of the reliance for that for very quick identification and targeting of items, you can start rotting this up and changing things. It is an area we will get better at as well.

Chairman: I think NATO is doing a major exercise on this in Armenia later this year. I do not think in the past, as far as I know, they have ever included cyber attacks in those exercises, but I guess it will not be long before they are including that in the simulated exercises, which are very impressive—you are perhaps aware of them—and that may happen in the future.

Q288 ***Lord Hodgson of Astley Abbotts:*** Minister, your responses to us this morning have shown the frightening, challenging and certainly immediate nature of the threats we face and also the way they are interlinked between different sectors of the economy within and without government. As yet I think there is no "National" CERT emergency response team. Should we have a "National" CERT and if so, do you plan to set one up?

Lord West of Spithead: I think the case for one is not absolutely clear yet and we need to keep that under review, whether we should have a "National" CERT or not and it is something we are looking at. When one looks at some of the countries in the EU, they have no CERTS at all and they need to get a kick-start and they have got to get going. We have a number of CERTs already. We have GovCertUK in CESG who go out amongst all the GSI.GOV.UK.nets and things like that. We have CPNI's CSIRTUK as well. We have MODCERT to look at the MoD side of things. We are quite well placed compared with America and a lot of the European countries in that our GCHQ look after the security of military nets and also of government nets, whereas in America, for example, NSA only looks after military nets, which means DHS has to do the government nets and the dot.com nets, the civil nets; CESG does work for those as well, so does CPNI. We have a number of specialist CERTs working in these areas already who can be called upon by government to do things. That is all on the web as well, who to call when you have got a problem, and we are trying to educate industry more about who to get hold of. Maybe there is a case for having a centralised one; as I say, I think we need to look at it a lot more closely to see if there is. I do understand from within Europe why they do because if you go to a lot of the European countries, they do not have these sorts of structures at all. You absolutely need a team who can go and barnstorm and dive into things to give assistance and do the right sort of work when something has gone wrong as long as you will be able to identify it. This goes back to this issue, quite often lots of people do not realise that people have got into their systems and are doing things. That is quite a tricky thing to spot if you have allowed yourself to be opened up to it because these things are so clever. Now they will go through normal firewalls and things like that, there will be no indication and they are sitting there and they will pass out data of the type they want from within your system, not all the data just the bits they want when

they want to, and you will not be aware of it. These are real issues to come to grips with.

Q289 ***Lord Mawson:*** We have had quite a bit of conversation in this Committee about ENISA and in many ways for me it illustrates this conflict of cultures between the response of the European Union to these questions and the whole cyberspace global entrepreneurial environment we are talking about, in a sense the tension is in this. What is your view of ENISA's size and location? Are they going to be able to deliver what is asked of them in this programme?
Lord West of Spithead: The first thing I would say is I do think and I am supportive of having an EU centre of excellence. I think that makes sense. As I say, this is an issue the EU has not got to grips with and they need to get to grips with it and, therefore, a centre of excellence is good. It is very small. I am not saying that big is best because quite often big is worse, but I think that needs looking at quite closely to make sure it is able to do the things the EU wants it to do. As I say, the EU will not directly protect things, it has got to direct nations because they will be doing this themselves, but it needs to have a structure and a way of encouraging and getting them to do these things. The location, I know it is not easy for visitors to get out there and things like that. I am not sure—again, this is my ignorance—whether it is absolutely finally decided it will stay in Crete or whether this is still flexible to move elsewhere in Greece, I do not know and I am not sure where that stands. I can understand pushing things out from the centre and putting them out into various nations, but sometimes it means they do not have the direct access to the things they need to as readily as they should do and I think we need to think about that quite carefully in this case. One could argue, "Well, hang on, we are dealing with cyberspace, we are dealing with links. Surely if all the links are right it does not matter where the hell you are. We can all work from home or why not work from Crete," but you do often need to be where the centre of power is and I think we need to think about that and I am sure the EU will be doing that.
Chairman: With the great co-operation of everybody we have got through all our formal questions with 10 minutes to spare, so let us make best use of that 10 minutes with any other thoughts which Members of the Committee have.

Q290 ***Lord Hodgson of Astley Abbotts:*** Can I go back to Lord Mawson's point and the question of bringing in people from the outside to the committee, which Dr Marsh said was being pursued. One of the issues will be how you attract people of the right quality. That is to say, in industry if you have good people, they are doing the job they are paid to do; too often the second tier people are sent to sit on government committees and so on. Have you any plans to make sure that you are able to attract people who are at the leading edge of this very fast moving world?
Lord West of Spithead: I will let Dr Marsh talk in a second on this because he is doing the nitty-gritty of this, to be quite honest. As far as I am concerned, and with my discussions already with the people I have talked to in industry, they are very keen to get alongside us. The fight will be—because we will only be able to have one company or two, we cannot have lots and lots of people moving around there—various firms saying, "Hang on, I would like my man to go", I think we will have a very good choice and we will need to sit down and select who we want. He will also have to represent all of industry, so there are issues there. We cannot give a leg up to one group and not to all of them, but it will give us a field of choice which is rather valuable. I do not think we will have a problem in terms of quality. As I say, I will let Dr Marsh talk a little more on that.
Dr Marsh: I would certainly support that. In this field I have not experienced any reluctance of industry to get involved, they see it as important and they are keen to engage as much as they can. As the Minister says, we need to be very careful that we are not giving a commercial advantage to one particular company at the expense of others. That is where some of the challenges about bringing people in to the organisation are concerned. Nevertheless, even if we are not doing that formally, where we have got the groups of people together, it is not just seen as another tedious government committee, we have had real engagement from top quality people all across the board.
Lord West of Spithead: In terms of funding, I would expect industry to pay for this post, and I am sure that will not be a problem. I personally rather like people working for the money they are paid for and not expecting a bonus to do any work, but that is a personal view. That is what I would hope would happen.

Q291 ***Lord Harrison:*** Despite your later comments about cyber warfare, Lord Richard rightly explained that a number of our witnesses said that the internet was very defensible, partly because of its amorphous nature, such that if you attacked one bit of it it almost was self-healing; it is difficult to cut the throat of the internet, as it were. Are you doubtful of that? I accept what you say about cyber warfare and I think that is extremely important. Do you accept though the resilience that some witnesses have spoken to us about?
Lord West of Spithead: The internet itself is very resilient and that is part of the difficulty, defending ourselves from specific attacks on it, let us say, for example, an extremist website, because they can pop up anywhere, be carried on anything. It is the flexibility of it because it is designed to let you talk and

do these things. I do not see the internet itself being brought down. That would be very difficult to do; it is resilient, but within the internet people can do all sorts of things. They can grab data from you, they can make things that you run by messages that go through the internet run in a different way. Those are the things that are really worrying, but it is not a factor, destroying the internet itself. It is two separate things.

Q292 ***Lord Mackenzie of Framwellgate:*** Minister, in the light of the breaking news this morning with China and so on, does the Government have mechanisms to de-brief the Google people as to the type of penetration that has taken place and gain intelligence from this distance, or does it not?
Lord West of Spithead: Yes.

Q293 ***Lord Mawson:*** You know a great deal more about warfare than I do but it seems to me that what we are talking about here is warfare. There is a view out there that somehow the internet is something that you can do in your living room and we can all talk on line and it all works. My experience of developing an IT network has been confirmed by some of this discussion, actually: it is not like that at all. It is about individuals and small groups of people who come together and begin to work together and form relationships and build trust out of which those innovations, IT and a whole range of things come; that is how it really is. It is about people and relationships fundamentally; the technology is really just a tool. If it is true and if it is about building cultures—and I assume the SAS in a sense is a culture one nurtures because it has a specific job to do in warfare and you have got to do certain things to create that culture—what do we need to do to start to grow those small teams and those small pieces of culture practically that can begin to deal with this sort of warfare? It seems to me it is of that order where we need to get to and it is about the mixtures of those kinds of people to really take on a war like this. I may be wrong; warfare is not my expertise, but it feels as though it is something like that.
Lord West of Spithead: That is quite a complex and in a sense almost philosophical question in some ways. Clearly, the internet was started by a small group of people—

Q294 ***Lord Mawson:*** Two people in a garage, actually.
Lord West of Spithead:— thinking about things and talking about "How can we connect to . . . " and it started with a very altruistic view. People were trying to latch onto it to make lots of money out of it but the idea was to share information and be able to talk, and within cyberspace basically, yes, you get small groups. That is one of the issues with extremists and radicalisation. These are small groups who are talking. They are within cyberspace but they are working in exactly that way. The answer is that, yes, within our large structures we have small groups doing certain things. When I was Chief of Defence Intelligence I set up what was called the DTIO that was looking at the whole issue of information operations and warfare. That has now become the DIO. I do not know quite why the "T" has changed; there are people who like changing acronyms within the MoD. That looks at all of these aspects of psychology, of cyberspace, of connectivity, of how groups work together, profiling of people, all sorts of issues, all of which is tied together to be able to apply pressure, if one needs to, and as we move to the future I think the kinetic part of it, although it is still important on certain occasions, is probably getting less than some of those other parts in terms of how one applies these pressures to make people—it is normally leverage—do what you want or not do something they want to do which you think is bad for the common good. That package is something we are looking at very closely and we are working on and we are already involved in that.
Dr Marsh: The element of small personal networks is still vital, I think, for the internet. The Internet Engineering Task Force is still at the heart of a lot of the standards for the internet development. We have seen how the problems that the domain name service experienced a couple of years ago when it was under attack were largely solved by the experts in that area getting together and discussing these things and working out robust solutions. These networks are to a large extent enabled by the internet itself, I think, and they are still very valuable components and we need to engage with those and we do engage with those whenever we can.

Q295 ***Lord Hannay of Chiswick:*** To address this problem, is not what is required something that we are not terribly good at, which is having a greater degree of exchange between the small entrepreneurial part of this business and the big animals, the Government, the Civil Service, ministers, and so on? We have not always been very good at this in the past and I do not think we are still very good at it. You need more interchange, do you not? You need to be able to draw more on actual experience and not be hiring people for life but hiring people for a short time? Probably you are doing it all already. Making more interchange between the entrepreneurial sector and the governmental would seem to be one part of responding to this.
Lord West of Spithead: And I think the answer, as you have already said, is that we are doing this and it is something we are putting a great deal of pressure on. There are issues, as I have said, in terms of security about who you can tell certain things to. There are issues of scale. There are great benefits sometimes from something very small which creeps in under the radar, but the moment anything big focuses on it it is

doomed. If, let us say, China focused on some little group and said, "Right; we want every bit of data from there and we want to stop it functioning", that would happen like that. There is a whole number of factors that one needs and so we need to pull them into our structure so we can look after them and use all of their special skills to do these things. That is something we are pushing very hard. As I say, the Cyber Security Strategy came out last summer. There was work going on before, but a lot of these areas are areas we have been working in flat out since then and Dr Marsh is dealing with that one, and so it is too early in a sense for us to give details of exactly what we are doing but it is very important and it is something we have got to do.

Q296 ***Chairman:*** Minister, we were told you had to leave at 10 minutes past 11. We have kept you for one minute, for which I hope you will forgive us. Can I ask whether you would be kind enough to send us further information? You said right at the beginning of the session that there were constant attacks on various systems and you mentioned the Post Office. You also told us that there was evidence of state attacks compared to attacks by what I call gifted amateurs, and you mentioned aero engines. I wonder if you could send us a note just suggesting to us the extent of state-based attacks and as much detail as you feel able to give us. It is an aspect of our inquiry we have not heard about in such an authoritative way before and I think if you would be kind enough to let us have a short paper as soon as possible, because we are going to begin drafting immediately, it would be very helpful indeed.

Lord West of Spithead: I am sure we can do that. There will be constraints and, as I mentioned, sometimes the attribution is quite difficult. One has to say, "It is suspected that . . . ", because to show that one has chased it through and how you have done it to prove it is something I would not want to put on paper at this sort of level.

Chairman: We understand that. Minister, you have been very frank with us, you have been very full with us, and I think we have been very impressed by your vigorous approach to these problems. We are particularly grateful to you. As you realise, this is our last evidence session and we shall begin drafting our report which we hope to produce during March, but it has been a most intriguing morning and I am sorry we have kept you for three minutes beyond your time. Thank you for coming.

Letter from Lord West of Spithead

Following on from the oral evidence I presented to the Select Committee on 13 January 2010, I am writing to offer supplementary answers in response to one of the two of the questions posed during the session.

As Minister for Digital Britain at the Department for Business, Innovation and Skills (BIS), the Right Honourable Stephen Timms MP has agreed to provide an answer to the first of these questions, on the dissemination of lessons learned during Exercise White Noise, directly to the Committee.

With regard to the extent of state-based attacks in cyber space, the UK Cyber Security Strategy published in June 2009 identifies established, capable states seeking to exploit computers and communication networks as the most sophisticated threat in the cyber domain.

Large scale cyber attacks frequently make the news, as demonstrated by coverage of the alleged attacks on Google and aimed at the email accounts of Chinese human rights activists, among others. A network of computers carried out a denial-of-service attack on US government websites in July 2009, and brought down 11 South Korean government websites the following week. Denial-of-service attacks on Georgian government and media websites during the Russian invasion in August 2008 severely hampered Georgia's ability to disseminate accurate information about events on the ground. And a series of denial-of-service attacks against Estonian government and commercial websites in 2007 prevented Estonians from accessing accounts and conducting e-commerce for several weeks.

However, definitively attributing cyber attacks to state actors, cyber terrorists or others is extremely challenging. By its very nature the Internet is highly connected with hackers and criminals able to transit many time zones and many countries in a matter of seconds.

Whilst the Government is actively responding to the threat posed to the UK by our growing dependence on cyber space, it is in the interests of national security for the Government to refrain from publicly providing details of any specific attacks.

Letter from Stephen Timms MP

During the oral evidence by Lord West on 13 January, Lord Avebury asked about the lessons learnt and the dissemination of the results of Exercise White Noise.

I am glad that Lord West was able to report that the Exercise had been a success. Indeed, as the Minister with responsibility for the response during the Exercise, I found it realistic in terms of the pressure that Ministers and officials would face and certainly worth the effort of the large number of people involved in planning and playing.

Lord West gave an accurate summary of the operational lessons that the Department learnt from the exercise. We now have a clear agenda for improving the ability of our staff to meet the specific roles, work in teams and manage shift changes, demonstrate leadership and be able to use the information coming in from the industry and other Government Departments. We have learnt a number of lessons around communication between key players in the management of an exercise and, importantly, with the public through proactive engagement with the media.

Together with the telecommunications industry, we need to make progress on establishing a back-up communication channel to avoid the obvious problems of not being able to manage a communications failure through lack of communications. This will need to be a priority for our work in the industry group EC-RRG in the coming year building on the useful groundwork that has already been done.

The exercise had a separate value for the Government as a whole in that the preparation of the scenario and the identificaiton of the sort of issues that would ensure, caused key Government Departments to look at their own dependency on the PSTN. The Cabinet Office will ensure that this work feeds into the ongoingprocess to improve the resilience of the machinery of Government.

Given that this Exercise featured as one of our Digital Britain commitments, I propose that we put an account of the exercise and our planning to ensure we implement the improvements identified as a result of the exercise on our web site and any other appropriate sites.

I am copying this letter to Lord West at the Home Office.

12 February 2010

Written Evidence

Memorandum by The Association of Chief Police Officers (ACPO)

Introduction

1. I am Janet Williams, Deputy Assistant Commissioner of the Metropolitan Police Service. In April 2008 I was appointed the ACPO Lead for e-Crime for England, Wales and Northern Ireland. The ACPO definition of e-Crime is: "The use of networked computers or Internet technology to commit or facilitate the commission of crime". My answer deals with the UK's response to improve Europe's incidence response capability as outlined on page one of the call for evidence.

2. The first significant national police response to e-Crime in England, Wales and Northern Ireland was the creation of the National Hi-Tech Crime Unit (NHTCU) in 2001, along with 43 local Hi-Tech Crime Units at force level. The absorption of NHTCU into the Serious Organised Crime Agency (SOCA) in 2006 however created a gap at national level within the Police Service. This gap led to a reduced focus on mainstream e-Crime prevention issues, a lack of clear co-ordination of police e-Crime resources, and a reduced capability to investigate large-scale e-Crime that did not fall within the remit of SOCA. In April 2008 the growing prominence of e-Crime led ACPO to create the ACPO e-Crime Portfolio under my leadership.

3. In September 2008 the Home Office announced it would provide part funding over three years to establish a Police Central e-Crime Unit (PCeU), to be hosted by the MPS as Lead Force for e-Crime. In January 2009 the National e-Crime Programme was created to co-ordinate the growing number of e-Crime initiatives being identified and implemented under the ACPO e-Crime Portfolio.

4. At a strategic level, industry research and law-enforcement intelligence analysis indicates that e-Crime is a large and growing problem in the UK. Although the difficulties involved in gathering accurate data on e-Crime are widely acknowledged, ACPO is committed to developing more reliable and consistent measures against e-Crime.

5. One of the most significant challenges is under-reporting. Victims of e-Crime are often reluctant to report incidents to the police, either through embarrassment (for example, having been deceived by an advance fee fraud) or through fear of damage to their commercial reputation (for example, having suffered a data breach or a DDoS attack). In some cases, victims are genuinely unaware that an offence has been committed (for example, when their computer has been compromised to form part of a BotNet). Of particular concern is the belief by some victims that the police will not act if they report computer-related crime.

6. Although forces can record and investigate e-Crime, the nature of e-Crime and the structure of existing recording frameworks make analysis at a national level difficult. There is currently no central reporting point for e-Crime. It is proposed that the National Fraud Reporting Centre (NFRC) should take national responsibility for the reporting of e-Crime alongside fraud. Changes are also required to ensure that e-Crime is included as a separate category within overall measures of crime and public confidence in the police, such as the British Crime Survey.

Law Enforcement Challenges of e-Crime

7. Investigation and prosecution of criminals involved in e-Crime presents some unique challenges to the law enforcement community.

8. The Internet allows criminals to target potential victims from anywhere in the world, and enables mass victimisation to be attempted with relative ease—a single e-mail infected with malware can be sent to millions of recipients. The Internet provides the criminal with a high degree of perceived anonymity, as well as creating jurisdictional issues that may impede rapid pursuit and prosecution of offenders. In addition there is not yet a clear distinction between issues that are best dealt with through better regulation and those that require law enforcement action.

9. The technical nature of the methods used by those perpetrating e-Crime creates additional complexity throughout the criminal justice process—from capturing appropriate details when the crime is reported, through the complex regulatory processes required to obtain data on internet activity, to securing and preserving potentially volatile evidence in a time critical way that ensures legal compliance. When a prosecution is brought before the courts, a jury may be faced with complex technical evidence that they need to understand to make a decision on the guilt or innocence of the defendant.

10. The pace of technological development provides criminals with a continuing stream of new opportunities and methods of attack, as well as challenging the Police Service and other law enforcement agencies to ensure their own knowledge and expertise are kept up to date. The need for a better understanding of e-Crime applies across the Criminal Justice Sector, including not only the Police Service, law enforcement agencies but also the Crown Prosecution Service and the Courts.

Police Central "e"crime Unit (PCeU) Vision, Mission and Strategic Objectives

11. Vision statement—"To provide a safe and secure online and networked computing environment that enhances trust and confidence in the UK as a safe place to live and conduct business".

12. Mission statement—"To improve the police response to victims of e-Crime by developing the mainstream capability of the Police Service across England, Wales and Northern Ireland, co-ordinating the law enforcement approach to all types of e-Crime, and by providing a national investigative capability for the most serious e-Crime incidents".

13. Strategic Objectives

(a) To reduce the harm caused by e-Crime at a national level

(b) To increase national mainstream capability to deal with e-Crime across police forces

(c) To co-ordinate the national approach to e-Crime

(d) To increase opportunities to prevent e-Crime and make it more difficult to commit

(e) To improve national investigative capability for the most serious e-Crime incidents

(f) To develop and capitalise upon partnership engagement with industry, academia and law enforcement, and government both domestically and internationally.

14. Priorities

(a) Creation of a comprehensive police response to e-Crime in the UK will require long-term and ongoing development of police structures, processes and capability.

(b) Immediate priorities have been identified as:

(c) To implement a Forensic Triage process to target e-Crime resources effectively and reduce computer forensic backlog within forces

(d) To improve the accuracy of e-Crime recording

(e) To raise understanding of e-Crime within the Police Service, and improve frontline officers' skills

(f) To increase police specialist e-Crime investigative capability

(g) To establish processes to co-ordinate police e-Crime response across the country

(h) To build effective partnership relationships with industry, government and academia

(i) To educate the public on the action they can take to protect themselves, and to prevent e-Crime.

15. Critical Success Factors Achievement of this strategy will be dependent upon:

(a) Continued support and funding for e-Crime as a priority at Government level

(b) Engagement by industry—willingness to work in partnership with each other and law enforcement, and support prosecution of offenders

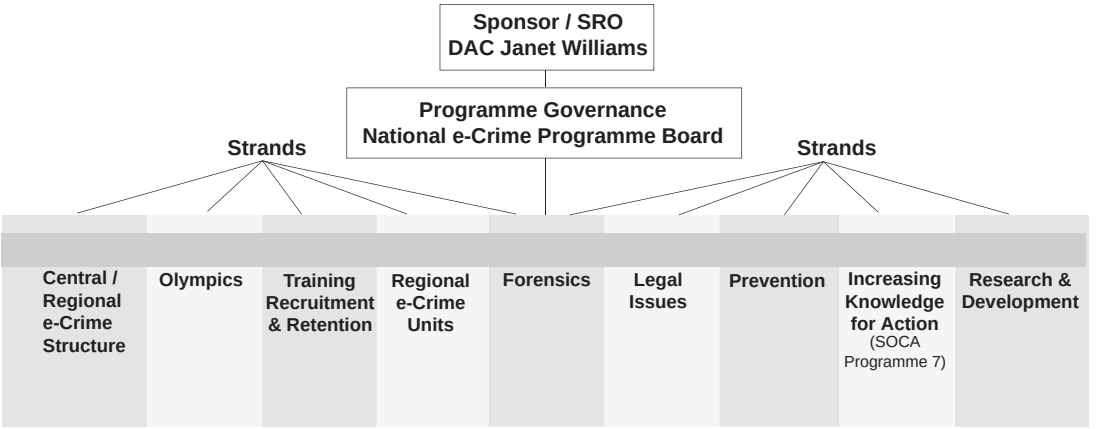
(c) Cooperation between all law enforcement agencies to tackle e-Crime

(d) Increased understanding of e-Crime across the Criminal Justice Sector.

Specific Initiatives

16. In addition to the development of police infrastructure, a number of specific initiatives to improve the police and law enforcement agency response to e-Crime are being driven forward by the ACPO e-Crime Committee. Membership of the ACPO e-Crime Committee is drawn from the principal police forces and agencies involved in e-Crime, allowing an integrated national approach to be developed and implemented.

17. The work of the Committee is split into nine Strands, under the ownership of relevant committee members.



Remit and Key activities of each Strand

18. The ACPO e-Crime Committee has set the remit and key activities for each strand. The key activities within each area will continue to develop to reflect priorities and the changing e-Crime environment. A brief outline of each strand is documented (a–i).

(a) Central/Regional e-Crime structure

19. Remit: To establish the PCeU as a central co-ordination point for the National e-Crime Programme, and to develop the Central/Regional e-Crime structure.

20. Key activities:

(a) Co-ordinate ongoing development of the National e-Crime Programme

(b) Establish the Police Central e-Crime Unit

(c) Direct the roll-out and structure of regional collaborative e-Crime hubs.

(b) Regional e-Crime Capability

21. Remit: To support the design and roll out of a regional e-Crime structure across England, Wales and Northern Ireland

22. Key activities:

(a) Design and implement the regional e-Crime pilot model

(b) Co-ordinate standard setting to enable inspection by HMIC and against ISO standards

(c) Process map e-Crime response within the pilot model

(d) Secure commitment of forces to the regional collaborative e-Crime model.

(c) Olympics (subject to separate funding)

23. Remit: to prepare UK law enforcement to respond to e-Crime incidents connected to the Olympics.

24. Key activities:

(a) Establish the e-Crime response required to deliver appropriate policing capability and capacity

(b) Deliver the Olympic e-Crime threat assessment in consultation with other agencies

(c) Review e-Crime threat and proposed response re Vancouver games

(d) Identify key crime enablers and create a prevention action plan prior to the 2012 Olympics

(e) Conduct an impact assessment of the Olympics on non-host forces for dissemination.

(d) Training, Recruitment and Retention

25. Remit: To ensure that high quality training is provided for e-Crime investigators; and to implement accredited e-Crime training for police officers who are not e-Crime specialists.

26. Key activities:

(a) Review and revise national occupational standards (NOS) in relation to e-Crime

(b) Review and revise all bespoke e-Crime training courses and major review of National Curriculum

(c) Introduce an appropriate level of e-Crime content into all police training

(d) Deliver a training package to support usage of the forensic triage tool identified by the forensic triage project.

(e) Forensics

27. Remit: To develop the ACPO strategy for forensic search, retrieval, seizure, examination and analysis process of digital forensics; and to develop an ACPO forensic best practice triage process for England, Wales and Northern Ireland.

28. Key activities:

(a) Review and produce findings on the retrieval and management of digital forensics

(b) Create a risk-based matrix with prioritisation guidance for e-Crime forensic work

(c) Identify the most appropriate and cost effective tool for forensic triage

(d) Develop the training user requirement and standards for use of the selected forensic tool

(e) Produce and disseminate a hash set library to be brigaded nationally, in partnership with CPS and CEOP

(f) Develop a process and user requirement to automate the grading of images, thereby reducing the national backlog of forensics by speeding up computer and media retrieval.

(f) Legal Issues

29. Remit: To develop legal guidance for the police response to e-Crime.

30. Key activities:

(a) Identify and address legal disclosure issues

(b) Collate existing disclosure procedures and identify best practice

(c) Co-ordinate and liaise with the Attorney General's office on e-Crime legal issues

(d) Produce evidential standards in respect of forensic triage project, to meet the standards set by the Forensic Regulator

(e) Assurance of local CPS e-Crime awareness

(f) Produce legal guidance in relation to e-Crime.

(g) Prevention

31. Remit: To identify national opportunities and activities to improve e-Crime prevention; and to set standards for e-Crime prevention.

32. Key activities:

(a) Review existing prevention advice and establish best practice guidance for the future for law enforcement and industry partners

(b) Identify force e-Crime prevention SPOCs to create awareness and standards of e-Crime security within law enforcement and industry

(c) Produce and agree "kite marked" standards for e-Crime prevention within law enforcement and industry

(d) Work with the insurance industry to identify incentive opportunities

(e) Support the implementation of e-Crime specific training for crime prevention officers.

(h) Increasing Knowledge for Action (SOCA Programme of Work)

33. Remit: To reduce the harm caused to the UK by the exploitation of technology, primarily Information and Communications Technology (ICT) by serious organised crime; to deter organised crime groups (OCG) from using ICT to attack UK victims; to develop new investigative and intervention tools to disrupt the use of ICT by organised criminals.

34. Key activities:

(a) Conduct effective, targeted interventions disrupting serious organised criminals' use of ICT and other technologies to commit offences or to launder the proceeds of crime

(b) Develop timely and accurate knowledge products to identify vulnerabilities and opportunities, and to build knowledge and understanding of the criminal use of ICT

(c) Develop and use specialist investigative techniques in support of law enforcement activity

(d) Disrupt or seize criminal finances and profits

(e) Conduct targeted initiatives with the private sector to deny opportunities for criminals to exploit ICT and raise public awareness to reduce criminal opportunity

(f) Undertake better planned, more effective multi-agency operations, with clear objectives, performance measures and impact analysis.

(i) Research and Development

35. Remit: To support the other work strands by providing expertise on new and emerging technology.

36. Key activities:

(a) Research new technology, and develop new technology threat assessment

(b) Research, product test and kite mark new e-Crime law enforcement technology, such as the forensic triage tool

(c) Establish evidential standards for analytical tools.

37. The delivery and co-ordination of these functions is managed through the Police Central e-Crime Unit (PCeU). One of the primary functions of the PCeU is to provide a national investigative function for the most serious e-Crime incidents, using its own specialist expertise and leveraging wider police resources such as traditional police investigative methods such as surveillance, forensics and financial enquiries to pursue investigations.

38. Cases that fall within the PCeU Case Acceptance Criteria include:

(a) Significant intrusions ("hacking") into government, commercial or academic networks

(b) Denial of service attacks, and other criminal use of BotNets

(c) Significant data breaches

(d) Significant false identity websites

(e) Mass victimisation e-Crimes, such as large scale phishing

(f) Electronic attacks upon the Critical National Infrastructure (subject to separate funding and agreement).

39. Since April 2009 the team has been responsible for in excess of 50 arrests for Computer Misuse Act offences.

Partnership

40. Partnership working is critical in order to effectively tackle e-Crime. Law enforcement agencies, commercial companies, government departments and universities have complementary skills and knowledge in relation to e-Crime. Information and intelligence on e-Crime is distributed across all of these organisations, and the full picture can only be properly seen if all these pieces are brought together. ACPO is therefore committed to work in partnership with others to tackle e-Crime.

e-Crime law Enforcement Agencies

41. The Police Service works in close collaboration with other government agencies whose remit includes e-Crime intelligence, enforcement and prevention activity, principally the SOCA e-Crime unit and the Child Exploitation and Online Protection Centre (CEOP). To ensure clarity of responsibilities, the e-Crime remits of these agencies are specifically excluded from the remit of the PCeU.

SOCA e-Crime

42. SOCA e-Crime grew from the integration of the National High-Tech Crime Unit into SOCA in 2006, and provides SOCA with the specialist knowledge and techniques needed to fight organised criminal enterprises. The remit of SOCA e-Crime includes the collation of both strategic and tactical e-Crime intelligence at NIM level three and subsequently actioning of it. SOCA Programme of Activity 7, is closely integrated with the ACPO e-Crime Strategy, focuses specifically on developing knowledge in relation to tackling the exploitation of technology by organised criminals.

Child Exploitation and Online Protection Centre (CEOP).

43. The Child Exploitation and Online Protection Centre (CEOP) is the UK national centre dedicated to tackling the sexual abuse and exploitation of children and young people, including cases in which technology may be a factor in that abuse or exploitation. Whilst first and foremost a child protection agency, CEOP has a wide remit including intelligence gathering and dissemination, supporting the work of public protection through the offender management team, behavioral analysis, financial investigation, victim identification and covert internet investigation. The centre also initiates harm reduction measures such as education programmes for children and training for frontline professionals. CEOP acts as a single point of contact for reports of sexual abuse and exploitation from the public, the internet, children's charities and law enforcement, through its online reporting mechanism. A representative of CEOP is a member of the ACPO e-crime committee.

Other Law Enforcement Agencies

44. The Police Central e-Crime Unit also works in collaboration with other police and government agencies both within the UK and abroad to develop joint solutions to e-Crime issues.

The National Fraud Authority (NFA)

45. The NFA was established in October 2008 to take forward the Government's response to fraud, building on the 2006 Fraud Review. It is working with public, private and third sector organisations to initiate, co-ordinate and communicate counter-fraud activity across the whole economy. As fraud is often the primary purpose of e-Crime, the ACPO e-Crime Strategy and members of the PCeU contribute to the achievement of the National Fraud Strategy and are members of the relevant NFA programme boards.

Association of Chief Police Officers in Scotland (ACPOS)

46. ACPOS sets strategic objectives for policing in Scotland, including development of the National e-Crime Strategy for Scotland. ACPO and ACPOS work in partnership to ensure an integrated approach is taken to e-Crime policing issues across the UK. Where appropriate Police e-Crime Units in Scotland work with colleagues in England, Wales and Northern Ireland to share intelligence, conduct investigations and prevent e-Crime. A representative from ACPOS is a member of the ACPO e-crime committee.

National Police Improvement Agency (NPIA)

47. The NPIA leads on training and development within the Police Service, as well as promoting innovation in professional practice and maintaining the national police IT infrastructure. The NPIA plays a key role in developing and delivering e-Crime training curricula to meet the needs of all officers and staff, and is represented on the ACPO e-Crime Committee. The NPIA supports the training and development of specialist e-Crime officers and front-line police officers, raising knowledge and understanding of e-Crime across the Police Service.

Centre for the Protection of National Infrastructure (CPNI)

48. CPNI is the Government authority that provides protective security advice to businesses and organisations who run the national infrastructure. Their advice aims to reduce the vulnerability of the national infrastructure to terrorism and other threats, keeping the UK's essential services safer. CPNI advice is targeted primarily at the critical national infrastructure (CNI)—those infrastructure assets (physical or electronic) that

are vital to the continued delivery and integrity of the essential services upon which the UK relies. The PCeU at a national level works with CPNI to ensure that time-critical alerts and best practice is shared and disseminated appropriately.

Get Safe Online

49. Get Safe Online is a public-private partnership, providing a one-stop source of information and advice for private citizens and small to medium sized businesses on computer safety. It aims to raise public awareness of potential online threats and vulnerabilities, and educate people on the action they can take to improve their computer security and use the Internet safely. Information and advice provided to callers making complaints to the NFRC will harmonise with that provided by Get Safe Online, and callers will be made aware of Get Safe Online as a good source of further information and advice about computer security and online safety.

50. The PCeU is also establishing information and intelligence sharing protocols with other government agencies that contribute to tackling e-Crime, such as HMRC, and UKGovCert.

Industry

51. The police continue to develop partnership relationships with industry, through representative bodies and forums, as well as liaising directly with individual companies in the course of investigations.

Industry Representative Bodies

52. The police have established relationships with industry representative bodies within banking, payment services, telecommunications, retail and IT security to identify the latest e-Crime trends and work in partnership to mitigate them, and to identify specific investigative opportunities. Liaison with industry representative bodies also creates effective communication routes for the dissemination of specific e-Crime prevention advice, alerts and judicial notices.

53. An active and effective partnership with industry bodies will enable the police to identify and build relationships with key industry personnel whose specialist skills are critical to the fight against e-Crime.

54. The police will continue to develop and expand these partnership relationships with industry representative bodies, focusing particularly on sectors where there has been less contact in the past to gain a full picture of e-Crime across industry.

MPS Operation Sterling Industry Fraud Forums

55. Over the past three years Operation Sterling, the MPS strategy for combating economic crime, has established a series of sector-specific industry fraud forums. Individual forums have been formed for Vehicles, Hotels, Construction, Property, Travel, Banking, Recruitment, and Vetting & Screening. Although Operation Sterling was the catalyst for the formation of these forums each group is self-managed by its members based on a written constitution. The forums have an increasingly national focus, bringing together companies to identify current fraud trends within their sector, develop preventative action and disseminate this across their industry.

56. As a next step the police will work with the Sterling industry fraud forums to establish an e-Crime subgroup for each sector, enabling members to share information on e-Crime activity within their industry, pinpoint issues and trends, and work in partnership with the police to identify specific investigative or preventative opportunities. The relationships created within these e-Crime subgroups will also enable rapid formation of taskforces when these are needed to tackle specific e-Crime issues.

International

Europol

57. Pan-European police liaison on e-Crime is achieved through the Europol ICT Working Group. This provides a forum for:

58. Sharing details of national crime reports and operational intelligence on e-Crime. This will be significantly enhanced by the introduction of the European Information System (EIS) in 2009, enabling faster sharing of operational intelligence for live investigations.

59. Collaborative working on specific cases through the use of joint intelligence analysis tools.

60. Discussion of e-Crime trends and issues through a secure online police forum across all 27 EU states.

61. Both SOCA and the PCeU are actively involved in work with Europol, and are members of the group developing a new methodology for collaborative working on e-Crime amongst Europol members.

Interpol

62. Interpol enables police forces around the world to cooperate on e-Crime through the Interpol European Working Party Group on IT Crime (EWPGITC). This Group allows police e-Crime Units to:

63. Share information and intelligence on e-Crime.

64. Promulgate best practice in e-Crime investigations (through the Interpol IT Crime Manual) and other e-Crime areas, such as forensics and new developments in technology.

65. Develop and deliver IT Crime courses, sharing knowledge and skills between police forces.

66. The PCeU and SOCA are members of EWPGITC, and the PCeU acts as a National Central Reference Point for the Police Service on global e-Crime investigations that are co-ordinated through Interpol, providing a 24/7 response.

Other International Law Enforcement Agencies

67. In addition to participation in Europol and Interpol, e-Crime Units co-operate bi-laterally with individual international law enforcement agencies (such as the FBI and the US Secret Service) to pursue specific e-Crime enquiries. Direct liaison of this type is conducted through legal attachés and police liaison officers in Embassies and Consular Offices.

68. A good example of the benefits to be gained from international co-operation is the National Cyber Forensics and Training Alliance (NCFTA), based in Pittsburgh USA. Established in 2002, this non-governmental, not-for-profit corporation provides workspace to facilitate collaboration between industry, academia and law enforcement on e-Crime, enabling them to effectively identify and address cyber-related threats through intelligence analysis and dissemination. The NCFTA provides a good model for collaborative working between all partners in combating e-Crime, and a relationship has already been established between ACPO and the NCFTA.

Academia

69. A substantial number of Universities undertake research and teaching on information security, including centres of expertise at the University of Westminster, Royal Holloway (University of London), Cranfield University, University of East London and University of Glamorgan. These institutions have developed specialised areas of expertise and research in areas such as networks, business security, forensics cryptography, risk and audit.

70. In November 2008 it was announced that Queen's University Belfast had been granted funding for five years totalling in excess of £20 million to set up a new centre to combat e-Crime.

71. Its "innovation and knowledge centre", which will go by the name of the Centre for Secure Information Technologies (CSIT), will house experts in fields including data encryption, network security systems, wireless-enabled security systems and intelligent surveillance technology.

72. In addition to its own work, Queens University has agreed to lead the coordination and tasking of e-Crime academic research in collaboration with the PCeU.

Cyber Security Operations Centre (CSOC)

73. To support the CSOC, I have committed a full time member of staff from the PCeU and one from the Counter terrorism Command. The police requirements from CSOC are focused on:

(a) Operations to detect serious organised criminal networks activity.

(b) Operations to seize serious organised criminal networks assets.

(c) Operations to mitigate harm caused by serious organised criminal networks.

(d) Intelligence relating to 2012 Olympics and intelligence to identify serious organised criminal networks or criminal exploits directed at causing harm to or damage to the reputation of the games.

(e) Identify opportunities to exploit new technology or identify the criminal use of new technology.

(f) Identify threats to National Security (including terrorism, espionage and proliferation) from cyber crime.

(g) Develop intelligence to a stage that facilitates proactive and/or reactive investigations.

(h) Identify and share learning and best practice from international partners.

(i) Identify prevention opportunities to share with individuals and industry.

74. The products required are:

(a) UK threat assessment for e-crime.

(b) UK threat assessment for cyber terrorism.

(c) UK threat assessment on any nexus between e-crime and terrorism.

(d) Tactical options paper on operational capability across stakeholder agencies.

(e) Regular tactical assessments of the cyber crime threat, to identify emerging trends and methodologies.

(f) Strategic profiles to inform of new and emerging trends and technologies including horizon scanning.

Legislative Gaps and Issues

75. Law enforcement experience is that legislation has not kept up with the activities of the cyber criminals. They use the anonymity of the Internet to disguise their activities, the latest systems vulnerabilities to exploit their victims stealing swathes of personal details and subsequently use these credentials to defraud the UK finance and retail industries.

76. The speed at which the criminals work and the geographical boundaries that they cross globally often cause law enforcement to create lengthy reports for authority to respond in order to gather evidence. The requirements of the Regulation of Investigatory Powers Act (RIPA) and processes to action Production Orders and Mutual Legal Assistance Treaty requests for evidence creates the impact of slowing or stalling any investigation. The cost of investigations across "e" crime is not seen as a priority for policing.

Future

77. Whilst plans are in place for engagement across the EU but government IT systems make it extremely difficult to collaborate, exchange information and intelligence.

Response to the Specific Questions Raised on the Call for Evidence Paper

Botnets

78. Police experience is that the criminal use of botnets causes significant harm to the UK. They are manipulated both as a precursor to crime and a crime enabler. They are used to infect personal and work computers with crimeware, send out spam, steal personal credentials and as a denial of service tool. The stolen credentials are then used to carryout fraud, identity theft or takeover (sometimes to facilitate entry to a country) as well as being sold on as a commodity. The threat goes alongside the use of phishing websites and infected genuine sites to carryout mass market fraud, harvest credentials and infect further machines as botnets.

79. A number of recent police operations have identified the extent and harm caused by the criminal use of botnets. The most recent involved the use of a Zeus Trojan to create a 15,000 strong botnet. This was stealing 200,000 lines of data a day. Just one drop site server seized by police in the UK contained 45,000 individuals personal details including login details for there bank and credit card accounts, online shopping channels as well as passwords for social networking sites and email. The individual harm that could have been caused as well the impact on retailers is considerable and the cost incalculable.

80. In consideration a pan European approach legislation is a barrier. Each country in the EU has its own legislation which on occasion cannot be compared like to like. An example of this is an offence to spend spam in some countries but not others. Some countries will not take action to secure evidence unless an offence relating to a victim within the host country exists. The need to request evidence or make investigations through letters of request greatly reduces the speed at which police and law enforcement can cooperate. The picture is fragmented and in the UK at this time there is not a cross government/agency response to incidents. In time through the development of the PCeU and the Cyber Security Operations Centre this will improve.

81. The PCeU has formed a virtual task force (VTF) within the finance world in order to improve the speed and quality of information and intelligence on cyber crime. The aim of the VTF is to provide a forum for coordination of actions required to mitigate the risks associated with financial e-crime, and to forge closer working relationships between public and private institutions. The VTF operates in a manner on the principle of contributing to public benefit, rather than working for parent, contributing, organisations. The VTF operates at Strategic and Tactical levels, with the Strategic forum remaining responsible for developing doctrine, policy and for stakeholder management, whilst the Tactical forum implements policy through development and implementation of tactics, training and procedures. The VTF is constructed as a voluntary

participatory framework to share information and intelligence through a fast track process to achieve the strategic objectives, reducing the harm caused by e-crime and maintain public confidence. The police would advocate such a response across the EU.

82. The experience of police in relation to ENISA is that they appear to be very project focused rather than providing a timely and specific response.

83. By 2010 the police would hope to see an improved framework and structure, co-ordination and policy to assist in delivery of a response to a cyber attack. We see the need is urgent and therefore the sooner activity begins the better. Potential for attacks exist now as widely evidenced in media reporting on the recent attacks on industry and law enforcement.

November 2009

Memorandum by Boxing Orange Ltd

1. Introduction:

1.1. I am writing as both Co-Founder and Director of Boxing Orange Ltd which was formed in 2001. We are a pure-play security service based organisation with over 120 private sector customers in the UK as well as a number of public sector customers across various government departments. Approximately 30 members of staff are SC cleared and proficient in managing and protecting confidential data.

1.2 The frequency and complexity of cyber attacks is increasing at an alarming rate. Attackers are circumventing signature based anti-malware tools by changing the code just enough to sneak past filters. This is a challenging situation for all Cyber Security Companies because the systems they sell to detect attacks are failing to protect their clients. All forms of botnet enabled attacks have increased including Phishing and DDoS with botnets becoming more complex, more powerful and able to make use of increased computing power making them a formidable adversary.

1.3 The UK Banking system has been under attack from botnets with a reported 44,000 phishing websites targeting UK Banks and Building Societies. Banking fraud has increased by a staggering 132% with losses totalling £52.5 million, compared to £22.6 million in the previous year.[1]

1.4 There have been numerous DDoS attacks against high profile targets over the past six months including UK and US Government sites. The cyber criminals have developed new methods of Command and Control of the botnets which are able to defeat current protection and mitigation systems.

1.5 The systems used to protect the industry have remained stagnant and relied on the same traditional detection methods. They are reactive systems that rely heavily on known signatures and attack vectors and are failing to protect clients, while failing to keep up with current trends in Cyber Attacks. A new system and approach is needed to protect these customers.

In Response to the Issues Raised:

2. Threat Analysis:

2.1 *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?*

I believe the internet to be vulnerable to wide spread technical failures however I do not necessarily believe it to be at risk from natural disasters.

2.2 *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is the regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

The industry has done a great deal to ensure resilience and stability and cannot be held responsible for individual attacks. To prevent attacks we believe the onus should be on individual departments and businesses, in essence, the end user. A good example of regulatory intervention is the Payment Card Industry (PCI) who implemented basic industry standards. This has, however, been very slow to take effect due to the difficulties in trying to enforce regulations that are not a legal requirement. The USA is a good example of greater intervention with businesses being better prepared for any attack through the use of HIPPA, Sarbanes Oxley, etc.

However the introduction of compliance and Government regulation cannot be used as an excuse to remove risk management and so a collective, collaborative approach is required between Government, Business and the end user. All have a part to play in the fight against cyber attacks.

[1] Source: Garlik Cyber Crime Report 2009.

2.3 *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in spring 2007 and Georgia in August 2008. Is this concern justified?*

Your concern is absolutely justified. The UK, USA and Sweden have all had warnings in the past six months that such an attack could take place. I feel that at present the UK has not made adequate plans to deal with or mitigate against these attacks.

2.4 *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

I don't feel qualified enough or have sufficient knowledge of IT Security in the military to be able to answer the question. I do, however, believe that Boxing Orange has the technology to solve your issues and is continuing to develop this technology to combat future attacks.

2.5 *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at European level?*

Firstly, you should be very concerned about the criminal damage botnets can potentially cause UK industry. The scale of the problem is wide spread but I believe the extent of the problem can be tackled at a local level, with cooperation at a global level where appropriate.

3. International Repsonses:

3.1 *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

I believe a UK only tactical approach is the quickest solution and would be sufficient to deliver infrastructure protection at a national level. A Pan-European strategic approach is good in theory but would push timescales back and introduce more complications.

3.2 *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see now such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

I believe public-private partnerships are the way forward both at a local, national, and European level.

3.3 *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

Yes there needs to be a move amongst both the public and private sectors to share intelligence data and information. Commercial organisations see their protection as a business advantage and are not prepared to share the attacks they have defeated or indeed divulge attacks that have beaten them.

3.4 *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

Yes, absolutely, this is what needs to happen.

3.5 *Are Government operated Computer Emergency Response Teams (CERT's) an appropriate mechanism for dealing with Internet incidents?*

Government operated CERT's are not an answer in themselves in dealing with Internet incidents but can act as a hub for a partnership between public departments and agencies and private enterprise. This allows for information sharing, strategy formulation and coordinated responses to incidents.

3.6 *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

There should be scope for the UK approach to be enhanced while integrating with a European-wide system. A defence in depth approach.

3.7 *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

A European and worldwide approach would be ideal. However the problem is that there are approximately 190 countries of which only approximately 30 will share information and data on international attacks. The US is slightly ahead of the European Union when it comes to their policies and strategy with regards to cyber

threats. There is much Europe can learn from the US approach but cultural, legislation and commercial sector differences need to be taken into account.

Until such a time exists when a worldwide strategy can be defined and agreed upon a European-centric approach should be pursued.

4. European Network And Information Security Agency (ENISA)

4.1 *The Commission sees a major role for ENISA in developing national CERT's and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

ENISA does have a role to play as an advisory body with the development of national CERT's and the deployment of EISAS. Cert's need to be developed on a national level but ENISA can bring best practice, experience and knowledge together from the various member states.

4.2 *Is ENISA being effective in its role, or does it need to reform?*

ENISA has in my view been a partial success in its role to improve network and information security in the European Union. I do not believe ENISA has been proactive enough in engaging with private sector security companies such as Boxing Orange. The agency needs to refocus and raise its profile within the security arena both at a European level and a national level.

5. Timescales

5.1 *Most of the Commission's plans are to be put in to practice by the end of 2010. Is this timescale realistic?*

Yes the timescales are realistic but will require the assistance of specialist companies like Boxing Orange.

6. Summary

In summary, you need to have a surveillance system which is tracking botnets using honey pots; proxy servers; spam capture systems; web crawlers and covert internet investigators (multi-lingual); and you need to have DDoS protection in place both locally and in the cloud. This strategy will enable you to mitigate against attacks before they happen and be protected against those that do get through. This use of technology needs to be augmented with the use of clear guidelines, governance and laws which are established in partnership between Business and Government. I have tried to explain in simplistic terms, if you would like further information or clarification on any of the above, please do not hesitate to contact me.

12 November 2009

Memorandum by Professor Jon Crowcroft, Marconi Professor of Communications Systems, Cambridge University

Professor Crowcroft was a member of the Internet Architecture Board, the standards oversight committee for the Internet, from 1996 until 2002.

1. The Internet is a network of networks, and its management is to a very high degree decentralised. This is one of its greatest strengths in resisting attacks. It is hard to find specific weak points, and rare that any particular failure will lead to widespread problems.

2. The Internet is a diverse system with technology (both software and hardware) from a multiplicity of sources, both public and private. This is another of its great strengths. An attack that succeeds at one point may very well not work anywhere else.

3. Rather than concentrate on defending this critical resource through top-down, command-oriented, centralised approaches, I would recommend increasing decentralisation and diversity.

4. For example, recent well documented failures in routing,[2] name serving[3] and web search services[4] have been due to centralised operational errors in ISPs, the root name server organisation, and Google. More distribution and more diversity would reduce the impact of these mistakes.

[2] http://government.zdnet.com/?p=3673
[3] http://www.wired.com/science/discoveries/news/1997/08/6184
[4] http://blog.stopbadware.org/2009/01/31/google-glitch-causes-confusion

5. Government agencies such as telecom regulators should look at current operations across multiple levels and ascertain whether policies are in place to ensure continued diversity.

6. Terrorists and other enemy organisations are themselves organised in decentralised ways. Asymmetric warfare works for them because their targets are centralised and obvious. The net is one infrastructure which resists this, and should be understood to be more robust as a result of this.

18 October 2009

Memorandum by Europol

1. Introduction

The increasing "technicalisation" of the modern world offers many opportunities to the citizen and criminal alike. The availability of modern technology creates both the opportunity for new types of crime, and for new ways of committing more traditional crimes. Together these aspects have become known as "Hightech crime".

There are currently no comprehensive and accurate statistics available to quantify high-tech crime; nevertheless, it is clear from cumulative operational experience and intelligence reporting that this phenomenon is rapidly evolving into a principal criminal threat.

Being virtual, high-tech crime is completely cross-border by nature. The fact that high-tech crime often requires careful planning and expensive investment, against the potential for high criminal profits, attracts the enterprising criminal.

> *"One of the emerging threats is the growing number of virtual OC groups. Criminals from different continents can meet on the Internet and collaborate in crime without personally knowing each other. (…) In such private networks, always protected by sophisticated security features, criminals or scattered cells spread all over the world can meet and organise to commit crimes on the internet; specialists can offer their skills and be purposely hired and paid by OC groups to commit crimes on the internet (or in real life); (…) OC groups operating on the Internet are very difficult to trace." (OCTA 2009, p.22)*

Moreover, European countries increasingly rely upon electronic systems and internet networks. As assessed by the House of Lords, *"Major economic or social damage could be caused if these digital systems are disrupted, either by 'hacking' or 'spamming' attacks, or as a result of technical failures, or as a side effects of a natural disaster."*[5]This vulnerability is now a subject of concern and the risk of cyber-attacks is pointed out by the European Commission as well as by the Draft Stockholm Programme.[6]

It is clear therefore that law enforcement agencies need to keep pace with the technological development of criminals to ensure that the crimes they perpetrate can be effectively prevented or detected. In addition, given the borderless nature of high-tech, capacity must be of a similarly high standard throughout the EU so as not to allow "weak spots" to develop where high-tech crime can flourish with impunity.

This capacity is far from homogeneous in the EU. In fact there is clear asymmetrical development; some MS are forging ahead with great advances in certain areas, whilst other MS lag behind in terms of technology. This creates the need to have a centralised service to assist all MS to coordinate joint activities, promote the standardisation of approaches and quality standards and identify and share best practice; only in this way can a homogenous EU law enforcement effort to high-tech crime fighting be assured.

1.1 *General Purpose of the High Tech Crime Centre*

Cybercrime is an explicitly mandated crime for Europol. The High Tech Crime Centre (HTCC) was established at Europol in 2002. It is a relatively small unit (4 officials) but expected to grow in the future as the centrepiece of Europol's work in this area. The HTCC plays a major role in coordination, operational support, strategic analysis and training.

- Coordination: the Centre assumes a coordinating role on behalf of the Member States to ensure the widest possible harmonisation of law enforcement efforts within the high-tech crime areas, under best practice, research & development, expert groups, and communication platform.
- Investigation support: thanks to technically skilled staff, the Centre supports ongoing cases in the area of internet and forensic investigations in which a high level of expertise is required. The HTCC offers its expertise in response to internal requests from other operational units at Europol or national authorities in the Member States.

[5] Select Committee on the European Union—Sub-Committee F, *Inquiry into EU Policy on Protecting Europe from Large Scale Cyber-Attacks,* October 2009.

[6] EU Presidency, *The Stockholm Programme: An open and secure Europe serving the citizen,* 16 October 2009, COM 14449/09, p.27.

— Strategic analysis: the Centre monitors, researches and records all developments which could have a future bearing on hi-tech crime offering expertise to contribute to the Europol Organised Crime Threat Assessment (OCTA) in order to create specific High Tech Crimes Threat Assessment and supplying advice to Member States on what measures to take to tackle these emerging threats.

— Training: being active in all of the areas described above the HTCC identifies new requirements, operational shortcomings and associated training needs.

In addition, occurrences of high-tech crime are becoming apparent in all other areas of crime which Europol is mandated to deal with, giving it what is increasingly termed a "horizontal" nature. Therefore, Europol has different means to tackle cybercrime within the European Cybercrime Platform (ECCP).

2. European CyberCrime Platform (ECCP)

ECCP originates from the proposal by the French Presidency of the EU in 2008, in which Europol was invited to coordinate a European response to Internet-related crime by creating the ECCP for reporting offences noted on the Internet.

Furthermore, the Presidency invited Europol to develop a common and coordinated strategy to fight Internet-related crimes on an international level.

Europol even goes beyond the French proposal, by enlarging the platform for a wider and coordinated approach to effectively fight cybercrimes, considered high priority in most of EU MS and other countries due to the high rate of cross border criminal phenomena.

The idea fits within existing activities in the area of Internet-related crimes at Europol and comprises the following three main topics:

— The Internet Crime Reporting Online System (I-CROS)

— The Analysis Work File (Cyborg)

— The Internet and Forensic Expertise recipient (I-FOREX)

2.1 *The Internet Crime Reporting Online System (I-CROS)*

The purpose of the Internet Crime Reporting Online System (I-CROS) is to convey information from EU Member States and eventually third parties to Europol[7] related to the offences noted on the internet. Europol through its Europol National Units (ENUs) entry points will receive structured and harmonised information from the national reporting online systems.

The EU JHA Council has tasked the European Commission to allocate the necessary funds for the realisation of the ICROS; Europol is bidding for European Commission funds under a monopoly situation. The project should be finalised through several phases during 2010.

2.2 *The Analysis Work File "Cyborg"*

The aim of this Analysis Work File (AWF) is to target Internet and ICT driven organised crime aimed at financial gain.[8] The scope of the work file includes among others e-banking attacks, complex phishing cases, hacking of (financial) databases. The study that regards the use of BOTNETS is included in the AWF. The eventual goal is to identify active groups with links to Europe and tackle them in concerted action with the involved AWF members. More specifically the focus will be on the crimes defined in Articles 2–8 of the Cybercrime Convention.[9]

The added value of the AWF is to combine the individual investigative efforts of MS, to create a bigger picture of the threat cybercrime poses and to have combined operational action in the end.

[7] Third parties mean the bodies with which Europol has an operational cooperation agreement.

[8] The AWF is a database on a specific crime area which is intrinsically linked to specific forms of operational support offered by Europol. AWF is the only existing legal tool at European level to store, process and analyse factual information ("hard" data) and in particular "intelligence" (or "soft" data), including personal data of sensitive nature at the same time.

[9] *Convention on Cybercrime,* CETS No.: 185, Council of Europe

The AWF has 21 members from EU countries although several third countries and organisations, also from the USA, have shown interest to be associated to the work file.

2.3 *The Internet FORensic EXpertise (I-FOREX)*

The Internet FORensic EXpertise (I-FOREX) system, managed by Europol, will consist of a portal-based facility and comprises all information not related to personal/operational data that is in fact included into the two above mentioned tools. The recipient will not contain personal/operational data.

The information contained in this platform will be uploaded both by EU MS and Europol and will mainly refer to police best practices and training, but not excluding other important cybercrime areas in law enforcement community.

This technical recipient is considered to be a fundamental tool for Europol to support investigations on cybercrime toward EU MS and will aid the investigators to keep abreast of new technical skills. The project should be first implemented during the second quarter of 2010.

3. Training Activities

Cybercrime investigations imply learning-by-doing processes which are formed not only by the theory but also by the practice that plays a fundamental role in the whole loop of skills developments. In fact, this process does include a good training programme simply for the fact cybercrime expertise gets outdated in a very short time unless a regular feed is guaranteed. The training and the exchange of best practices dramatically improves the quality of the daily job of cybercrime investigators. For this reason, the HTCC (unit specialised in cybercrime) has developed its activity in the field of training.

— It stands as the platform for the European Working Group on harmonisation of cybercrime training investigation. The WG is composed by 40–60 permanent members belonging to law enforcement, private sector, academia, and international organisations.

— It offers its expertise in delivering part of the training organised by SC3 Crime against Persons Unit on combating the sexual exploitation of children on the internet.

— It supports external requests to deliver training such as Interpol and CEPOL.

4. Questions from the House of Lords

The Call for evidence focuses on large-scale cyber-attacks on critical national infrastructures, whereas Europol especially deals with organised crime in this area. Europol is therefore not competent to answer every question of this inquiry but the one related to criminal activity.

— *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

BOTNETS is a growing phenomenon. According to our information, the technique is used increasingly by Organised Crime groups to conduct cybercrime activities and to support other forms of crime, including fraud. We are also aware of and concerned by the new generation of malwares that point at not only to disrupt the system attacked but also to extract data (personal and financial); there is an underground economy built up on the use of BOTNETS.

5. Acronyms

AWF	Analysis Work File
ENU	Europol National Unit
EU	European Union
HTTC	High-Tech Crime Center
ICT	Information and Communication Technology
JHA	Justice and Home Affairs
OCTA	Organised Crime Threat Assessment

November 2009

Memorandum by Dr Stefan Fafinski

Introduction

1. I am pleased to accept the invitation of the Committee to give evidence in response to its inquiry into EU policy on protecting Europe from large-scale cyber attacks. This evidence is restricted to my personal areas of expertise and is submitted on an individual basis.[10] For the avoidance of doubt, the views expressed in this memorandum are my own and must not be attributed to any organisation.

2. This memorandum covers the section of the Inquiry concerning International responses. It is structured with a discussion of the area followed by responses to some of the individual questions raised by the Committee.

International Responses

3. The Commission's desire for a governance network that crosses the public-private divide is not surprising. In 1994, the Bangemann Report considered that the exploitation of the new technologies required to participate in "the new industrial revolution" would require "partnership between individuals, employers, unions and governments dedicated to managing change".[11] This partnership would mean "developing a common regulatory approach"[12] and thus reflected the European policy objectives of flexibility, legal certainty, harmonisation and technological neutrality.

4. The Commission produced a report in 2001 entitled "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime".[13] This report echoed the economic risks associated with computer misuse that were raised in the debates leading to the enactment of the Computer Misuse Act 1990 some 10 years previously.

5. The Commission went on explicitly to acknowledge that there are potential extra-legal means of governance which have a role to play alongside legal regulation, proposing a number of non-legislative actions.

6. The first of these was the establishment of an European Union forum to "enhance co-operation" between law enforcement, internet service providers, network operators, consumer groups and data protection authorities. This forum would aim to raise public awareness of risks, promote best practice, develop counter-crime tools and procedures and encourage the development of early warning and crisis management mechanisms. Such a forum would represent a dynamic networked approach to computer misuse which would be significantly more flexible and responsive than any potential legislative response. The second was the continued promotion of "security and trust" through products and services with "appropriate" levels of security and more liberalised use of "strong" encryption techniques. The third was increased training of law enforcement staff and further research in forensic computing. The final area was a study to "obtain a better picture of the nature and extent of computer-related crime in the Member States".[14]

7. The 2005 Framework Decision[15] identified the threats arising from attacks against information systems as "organised crime" and the "potential of terrorist attacks against information systems which form part of the critical infrastructure of the Member States".[16] The nature of these threats is distinct from the economic concerns raised in the Bangemann Report. However, the Framework Decision does reiterate the desire to approximate the criminal law in an attempt to transcend jurisdictional difficulties between states in the interests of:

> …the greatest possible police and judicial co-operation in the area of criminal offences…and to contribute to the fight against organised crime and terrorism.[17]

[10] I am a Lecturer in Law at Brunel University and a Director of Invenio Research Limited. I have over 20 years experience in the information technology industry, holding senior management positions in software product design, development and programme management. I have subsequently researched, published and lectured extensively on e-crime, computer law and computer misuse and won the 2006 British Association for the Advancement of Science Joseph Lister Award for my work on cybercrime. I am a Chartered Engineer, a Chartered Scientist and a Chartered Information Technology Professional. I am a Court Liveryman of the Information Technologists' Company, the City of London Livery Company for Information Technology. I am also a Fellow of the Institute of Directors, the British Computer Society and the Royal Society for the Encouragement of Arts, Manufactures & Commerce. I am a Member of the Society for Computers and Law, the British Society of Criminology, the Society of Legal Scholars, the Socio-Legal Studies Association and the Fraud Advisory Panel. I hold a Bachelor of Laws degree with first-class honours and a Masters degree in Natural Sciences from St John's College, University of Cambridge. My doctorate from the University of Leeds concerned the legal and extra-legal governance of risks arising from the misuse of information technology.

[11] Bangemann, M and others, "Europe and the Global Information Society" (the Bangemann Report) (1994) <http://ec.europa.eu/archives/ISPO/infosoc/backg/bangeman.html> accessed 18 November 2009.

[12] *Ibid,* 4.

[13] Commission (EC), "Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime" COM (2000) 890, 26 January 2001.

[14] *Ibid,* 31–2.

[15] Council Framework Decision (EU) 2005/222/JHA of 24 February 2005 on attacks against information systems [2005] OJ L69/67.

[16] *Ibid,* recitals [2].

[17] *Ibid,* recitals [8].

8. The backdrop against which the Framework Decision is set appears to be emphasising the protection of public interests. This was made explicit in the earlier proposal for the Framework Decision which considered the nature of the primary threat was that to communication network operators, service providers, e-commerce companies, manufacturing industries, service industries, hospitals, public sector organisations and governments themselves.[18] The Council also drew reference again to the "considerable" economic burden associated with such threats.[19]

9. Similarly, the European Commission's later Communication "towards a general policy on the fight against cyber crime"[20] reinforced the need for further training of law-enforcement personnel, further research, the development of technical measures to counter "traditional" crime (such as fraud) in electronic networks and private-public co-operation in the exchange of information and the raising of public awareness.

10. The United Nations considered that priority should be given to the provision of technical assistance to Member States, in order to provide a "level playing field"[21] and thereby harmonising technical capability rather than legal regulation.

11. The G8 Action Plan[22] recommended that there should be a collaborative effort between state and industry to ensure that new technologies are "policeable": that is, they facilitate the investigation of computer misuse via the collection and preservation of robust evidence. This introduces technological design as an additional potential tier of governance. Moreover, the G8 stresses the involvement of industry in the development of secure systems and participation and co-operation in civil contingency planning.

12. The OECD produced a set of guidelines for the security of information systems and security.[23] This provided a set of complementary principles for "participants". "Participants" is a broadly-defined term encompassing "governments, businesses, other organisations and individual users who develop, own, manage, service and use information systems and networks".[24] The principles to which the participants are expected to adhere are awareness, responsibility, response, ethics, democracy, risk assessment, security design and implementation, security management and reassessment. The resulting "culture of security" is one in which these participants take responsibility for their own safety while remaining flexible and co-operative in prevention, detection and response to incidents and respecting the legitimate interests of others. Risk assessments enable the "selection of appropriate controls" which underpins security management of systems containing components for which security has been an "integral part of system design and architecture". This culture is reflexive, undergoing a constant process of review, reassessment and modification.

13. There is clearly an overlap between many of the areas proposed by the various organisations. These fall into a number of broad categories founded on co-operation, information sharing, reflexivity and responsiveness.

CERTs

14. In general terms, a CERT is an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.[25]

15. For Van Wyk and Forno, a CERT exists "to minimise the impact of an incident on a company and allow it to get back to work as quickly as possible"[26] whereas for Killcrece it should act as a "focal point for preventing, receiving and responding to computer security incidents".[27] Wiik refers to the "new emerging survivability paradigm"[28] which proposes that no matter how much security is built into a system, it will never

[18] Commission (EC), "Proposal for a Council Framework Decision on attacks against information systems" COM (2002) 173 final, 19 April 2002, 3.
[19] *Ibid.*
[20] Commission (EC), "Communication from the Commission to the European Parliament, the Council and the Committee of the Regions towards a general policy on the fight against cyber crime" COM (2007) 267 final, 22 May 2007.
[21] United Nations, "'Around the clock' capability needed to successfully fight cybercrime, workshop told" UN Doc SOC/CP/334 (25 April 2005).
[22] G8, "Meeting of Justice and Interior Ministers of the Eight: Communiqué" (10 December 1997) <http://www.usdoj.gov/criminal/cybercrime/g82004/97Communique.pdf> 3 accessed 18 November 2009.
[23] OECD, "Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security" (OECD, Paris, 2002) <http://www.oecd.org/dataoecd/16/22/15582260.pdf> accessed 18 November 2009.
[24] *Ibid,* 7.
[25] ENISA, "Inventory of CERT activities in Europe" (September 2007) <http://enisa.europa.eu/cert_inventory/downloads/Enisa_CERT_inventory.pdf> accessed 18 November 2009.
[26] Van Wyk, K R and Forno, R, *Incident Response* (O'Reilly and Associates, Sebastopol, 2001) 21.
[27] Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).
[28] Wiik, J, Gonzalez, K K and Kossakowski, K-P, "Limits to Effectiveness in Computer Security Incident Response Teams" (Twenty-third International Conference of the System Dynamics Society, Boston, 2005).

be totally secure,[29] replacing the traditional notion of a fortress providing full protection against malicious attack.[30]

16. Over time, however, such CERTs widened the scope of their services from purely reactive emergency response towards the more proactive provision of security services including preventive services such as issuing alerts and advisories and providing training on incident management capability, performance standards, best practices, tools and methods. In the late 1990s the term "Computer Security Incident Response Team" (CSIRT) arose to reflect this broadened scope. Both terms (CERT and CSIRT) are synonymous in current usage.

17. There is a growing realisation that some level of proactive service ought to be offered as well.[31] CERTs therefore address different types of risk on a spectrum from serious electronic attacks on the public infrastructure, government departments or the financial services industry, through online fraud and identity theft to less serious (but more prevalent) harms involving general on-line nuisance.

18. The constituency (that is, the set of potential users) of a CERT can include national, governmental or private organisations. Equally, although some CERTs may be ostensibly linked to particular national interests, some are effectively global, such as the NCFTA, whereas others focus on particular industry sectors, such as the Financial Services Information Sharing and Analysis Centre (FSISAC).[32]

19. Each of these CERTs therefore acts as an independent node, collecting, processing and disseminating information relating to risk, although the differences in their constituencies may mean that the relative prioritisation of risks differs between CERTs. Assuming that each CERT has some data of interest to others, it follows that connecting CERTs which represent both public (state) and private (commercial and individual) interests could produce, in Kjær's terms, a "network… of trust and reciprocity crossing the state-society divide"[33] in the pursuit of shared goals or, in Rhodes' words, an "interorganisational network… characterised by interdependence, resource-exchange, rules of the game and significant autonomy from the state".[34] In other words, interconnected CERTs could provide a response or readiness network consistent with theoretical conceptualisations of governance.

20. In terms of a networked response to a networked problem, it is necessary to examine the nature and extent of inter-CERT collaboration to establish whether information sharing alone is an adequate response or whether CERTs should build relationships with other bodies and assist with collaborative responses to the problems arising from the cyber-attacks.

Collaboration between CERTs

21. UKCERTs is an informal forum of domestic CSIRTs including government, academic and commercial teams, again designed to encourage co-operation and information sharing between the participants. It also invites UK WARPs to its forum meetings. There are similar forms of national cooperation operating in Austria,[35] Germany,[36] the Netherlands[37] and Poland.[38]

22. The European Network and Information Security Agency (ENISA) was established in 2004 by Regulation (EC) 460/2004.[39] ENISA is a European Community Agency; that is a body set up by the EU to carry out a very specific technical, scientific or management task within the Community domain (the First Pillar) of the EU. ENISA's purpose, as defined in its establishing Regulation is that of:

> Ensuring a high and effective level of network and information security within the Community and [to] develop a culture of network and information security for the benefit of citizens, consumers, enterprises and public sector organisations of the European Union.[40]

[29] Lipson, H and Fisher, DA, "Survivability—a new technical and business perspective on security" (Proceedings of the 1999 New Security Paradigms Workshop, Association for Computing Machinery, Caledon Hills, 1999).
[30] Blakley, R, "The Emperor's Old Armor" (Proceedings of the 1996 New Security Paradigms Workshop, Association for Computing Machinery, Arrowhead, 1996).
[31] Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).
[32] <http://www.fsisac.com> accessed 18 November 2009.
[33] Kjær, A M, *Governance* (Polity Press, Cambridge, 2004) 4.
[34] Rhodes, R A W, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 15.
[35] CIRCA (Computer Incident Response Co-ordination Austria).
[36] CERT-Verbund.
[37] O-IRT-O.
[38] Polish Abuse Forum.
[39] Council Regulation (EC) 460/2004 of 10 March 2004 establishing the European Network and Information Security Agency [2004] OJ L 77/1.
[40] Regulation (EC) 460/2004, art 1(1).

23. It does, however, acknowledge that its objectives are without prejudice to non-First Pillar competencies of Member States (such as police and judicial co-operation in criminal matters) and the activities of the States in areas of criminal law.[41] It is specifically charged to "provide assistance and deliver advice"[42] to the Commission and Member States in relation to information security and to use its expertise to "stimulate broad co-operation between actors from the public and private sectors".[43] Part of ENISA's work is in facilitating co-operation between CERTs. It also supports the member states in setting up their own national or organisational CERTs and provides technical support to close the gaps between the Network Information Security competencies of individual EU Member States. Its 2008 work plan included an initiative to facilitate co-operation between Member States to set up new governmental or national CERTs, acting as a "good practice knowledge-base and contact broker".[44]

24. The European Government CSIRTs (EGC) group is an informal organisation of governmental CSIRTs[45] that is "developing effective co-operation on incident response matters between its members, building upon the similarity in constituencies and problem sets between governmental CSIRTs in Europe".[46] It works to develop measures to deal with large scale network security incidents, facilitating the sharing of information and specialist knowledge and instigating collaborative research in areas of mutual interest specifically related to the operational work of governmental CSIRTs. It differs from ENISA in its more limited membership: ENISA is concerned with facilitating communication between all European CERTs, whereas the EGC focuses only on governmental CSIRTs.

25. The Task Force of Computer Security and Incident Response Teams (TF-CSIRT) exists to promote collaboration between European CSIRTs with a research and education constituency.[47] It was established as part of the technical programme within the Trans-European Research and Education Networking Association (TERENA). It has similar aims to the EGC in promoting collaboration, promulgating common standards and procedures for responding to security incidents and providing training for new CSIRT staff.

26. The Trusted Introducer (TI) programme was also established under the auspices of TERENA.[48] It recognises the nature of the trust relationship which is a necessary condition for collaboration between nodes within a governance network. While the inter-CSIRT trust network was originally based upon personal recommendation between members of the particular CSIRTs involved, as the number of CSIRTs proliferated and staff moved on, this personal recommendation method became unwieldy at best. TI therefore exists to facilitate trust between European response teams by formally accrediting CSIRTs who wish to join its community. On a similar regional basis, APCERT was established by CSIRTs within the Asia Pacific region, aiming to improve cooperation, response and information sharing among CSIRTs in the region. APCERT consists of 20 CSIRTs from 14 economies.

27. In October 1989, a major incident called the "WANK[49] worm"[50] highlighted the need for better communication and coordination between teams. The Forum of Incident Response and Security Teams (FIRST) was formed in 1990 in response to this problem. Since that time, it has continued to grow and evolve in response to the changing needs of the incident response and security teams and their constituencies. The FIRST membership consists of teams from a wide variety of organisations including educational, commercial, vendor, government and military.

28. Finally, the Central and Eastern European Networking Association (CEENet) comprises 23 national research and education CERTs. It is primarily a knowledge network which shares information regarding computer network security.

Effectiveness of CERTs

29. The effectiveness of CERTs can be considered at two levels. The first of these is the internal effectiveness of the CERT itself; the ability of the CERT to deal with its workload and service its constituents as a reflection of its technical, financial, organisational and management capability. The second is the effectiveness of inter-CERT communication. If the networked response offered by CERTs is to be valuable, it follows that the

[41] *Ibid,* art 1(3).
[42] *Ibid,* art 2(2).
[43] *Ibid,* art 2(3).
[44] ENISA, "ENISA Work Programme 2008" 24 <http://www.enisa.europa.eu/doc/pdf/management_board/decisions/enisa_wp_desig_ver_2008.pdf> accessed 18 November 2009.
[45] France, Germany, Finland, the Netherlands, Sweden, UK, Norway and Switzerland.
[46] <http://www.egc-group.org> accessed 18 November 2009.
[47] <http://www.terena.nl/tech/task-forces/tf-csirt/> accessed 18 November 2009.
[48] <http://www.trusted-introducer.nl/> accessed 18 November 2009.
[49] Worms Against Nuclear Killers.
[50] CERT, "WANK Worm On SPAN Network" Advisory CA-1989–04 (17 October 1989) <http://www.cert.org/advisories/CA-1989-04.html> accessed 25 September 2008.

propagation of pertinent information between CERTs is key to avoid them existing only as silos of information accessible only to the particular constituency of each individual CERT.

30. In terms of internal effectiveness, the main challenges are described by West-Brown:

> To ensure successful operation, a CSIRT must have the ability to adapt to changing needs of the environment and exhibit the flexibility to deal with the unexpected. In addition, a CSIRT must simultaneously address funding issues and organisational changes that can affect its ability to either adapt to the needs or provide the service itself.[51]

31. Therefore, internal challenges are two-fold: adroitness (both technological and organisational) and availability of resources. In terms of resources, as Salomon and Elsa comment, information security is often viewed as a drain since it is a support service rather than a core business activity:

> Safeguarding the enterprise itself is a fairly unglamorous task, costs money and is difficult to justify to managers unfamiliar with the potential consequences of not having a strong commitment to IT security.[52]

32. Overstretched resources are a common issue within many CSIRTs. As early as 1994, only six years after the establishment of the US CERT at Carnegie Mellon, Smith commented that:

> About the only common attributes between existing Incident Response Teams are that they are under-funded, under-staffed and over-worked.[53]

Moreover, according to Lipson:

> Although the sophistication of Internet attacks has increased over time, the technical knowledge of the average attacker is declining, in the same manner that the technical knowledge of the average user has declined.[54]

Therefore, more people have the capability to launch attacks and the scope, frequency and volume of attacks (and hence the need for CERT services) is continuously increasing.[55]

33. A further complication arises in respect of the scope of "IT security". It spans a wide range of activity within which security-related tasks may fall to groups which are not immediately concerned with security as a core function, such as architecture, network operations, IT strategy or server support.[56] Even where adequately funded and resourced, CERTs must be able to respond swiftly to new forms of technological risk. A CERT organisation should be able to adapt to technological advances relatively quickly. However, the speed of response required in order to be effective is increasing. As Salomon and Elsa comment:

> The "flash-to-bang" time between the discovery of new vulnerabilities (or configuration errors) and the exploit thereof on a wide scale has narrowed considerably…Even assuming efficient processes and good communication, the sheer scale of many corporate security organisations makes effective and timely countermeasures difficult.[57]

34. Communication between CERTs also poses a number of potential problems. As EURIM commented,[58] those running CERTs differ in "cultural values" and approaches to security. These range from those who only engage with trusted organisations to those which purport to provide open services to all. Moreover, some are more open to communication with peer organisations than others and some exist to protect the commercial interests and intellectual property rights of themselves and their customers. A Police Officer in interview offered an interesting illustration of the importance of the routine administrative matters which underpin CERT-to-CERT communication:

> Through our WARP, we got wind of a DDOS attack that was being routed through a country in Eastern Europe. So the obvious thing to do was get in touch with the relevant CERT in that country. Would have been fine—except it turns out that the CERT in question had changed their phone number three years ago and hadn't thought to tell anyone. Certainly would have limited the amount of incoming

[51] West-Brown, M J and others, *Handbook of Computer Security Incident Response Teams* (2nd edn Carnegie Mellon University, Pittsburgh, 2003) 177.
[52] Salomon, J M and Elsa, P, "Computer security incident response grows up" (2004) 11 *Computer Fraud & Security* 5.
[53] Smith, D, "Forming an Incident Response Team" (Proceedings of the FIRST Annual Conference, University of Queensland, Brisbane, 1994).
[54] Lipson, H, *Tracking and Tracing Cyber-Attacks: Technical Challenges and Global Policy Issues* (Carnegie Mellon University, Pittsburgh, 2002) 9.
[55] Killcrece, G and others, *State of the Practice of Computer Security Incident Response Teams* (Carnegie Mellon University, Pittsburgh, 2003).
[56] Salomon, J M and Elsa, P, "Computer security incident response grows up" (2004) 11 *Computer Fraud & Security* 5.
[57] *Ibid.*
[58] EURIM, "Cyber-crime Reporting and Intelligence" (Tackling Crime and Achieving Confidence in the On-line World, Parliament and the Internet Conference, London, 2007).

information they would have got—so, you see, without some sort of proper day to day coordination and action then all these bodies are next to useless.

35. There are also legal concerns affecting CERTs. Graux comments that CERTs require their own legal expertise in order to develop and apply internal policies as well as to determine whether or not a particular incident requires the involvement of the criminal or civil law. He concludes that the need for international legal cooperation and coordination is paramount, requiring the "pragmatic availability" of legal channels of communication.[59] There is, therefore, a role for the law to govern and inform the internal framework of the extra-legal response mechanism of the CERT.

WARPs

36. Warning, Advice and Reporting Points (WARPs)[60] are part of the information sharing strategy of the UK Centre for the Protection of the National Infrastructure (CPNI).[61] They are therefore primarily a domestic initiative, covering the public service, local government, business and voluntary sectors[62] Examples include the National Heath Service (Connecting for Health) Information Governance WARP which provides centralised distribution of warnings and advisories, good practice advice brokering and trusted sharing of electronic related security problems and solutions and PENWARP which serves the journalist community.

37. The WARP model is not new or restricted only to the sphere of computer technology. For instance, the Radio Amateurs' Emergency Network (RAYNET)[63] is a national voluntary communications service for major civil emergencies or related exercises and local community events provided by licensed radio amateurs. It liaises with emergency services, local authorities and other voluntary agencies who could be involved in the integrated management response to major civil emergencies.[64] The Environment Agency also operates an advisory and response service for flood risk.[65]

38. WARPs are predominantly a "bottom-up" initiative, although their increasing importance in the area of contingency planning and management of the critical national infrastructure means that they are strategically part of the "top-down" agenda of the CPNI.

39. Unlike CERTs which generally focus on broader constituencies, a WARP (according to the CPNI) is a "community based service where members can receive and share up-to-date advice on information security threats, incidents and solutions".[66] Therefore, WARPs essentially operate as small-scale CERTs serving a community which may be within a smaller organisation or as a hub to particular organisations or individuals. UKERNA[67] proposed a model within which WARPs reduce incidents by providing preventative advice and CSIRTs respond to those incidents which do, in fact, occur.[68]

40. There is little regulatory constraint to concern WARPs other than a short Code of Practice which requires little from new WARPs over a willingness to co-operate and share information, maintain effectiveness and not to bring the WARP model into disrepute.[69] Agreement to this Code is a pre-requisite for registration with the CPNI.

41. WARPs, therefore are lightly-regulated "mini-CERTs" serving similar needs to a more restricted community. As with CERTs, the trust relationship between WARP members is important and one which is stressed by the CPNI as being crucial to their effectiveness. However, given the smaller scale of WARPs as compared to CERTs, it might be expected that there would be considerably more of the former than the latter in operation, although there actually remains a larger number of CERTs than WARPs in the UK at present. Despite this limited adoption, the role of WARPs within the overall framework of governance responses seems theoretically attractive, extending the reach of the extra-legal response network to parties that may not, of themselves, fall within a CERT's constituency or have the capacity or desire to establish a CERT of their own. However, the very existence of WARPs does not seem to be particularly widespread knowledge.

[59] Graux, H, "Promoting good practices in establishing and running CSIRTs—a legal perspective" (ENISA Workshop, 13–14 December 2005).
[60] <http://www.warp.gov.uk> accessed 18 November 2009.
[61] <http://www.cpni.gov.uk> accessed 18 November 2009.
[62] As at 1 June 2008 <http://www.warp.gov.uk/Index/WARPRegister/indexcurrentwarps.htm> accessed 18 November 2009.
[63] <http://www.raynet-uk.net/> accessed 18 November 2009.
[64] RAYNET now has an associated WARP (RAYWARP).
[65] <http://www.environment-agency.gov.uk/subjects/flood/> accessed 18 November 2009.
[66] *Ibid.*
[67] Now JANET(UK).
[68] UKERNA, "CSIRTs and WARPs: Improving Security Together" (March 2005) <http://www.warp.gov.uk/Marketing/WARPCSIRT%20handout.pdf> accessed 18 November 2009.
[69] ——, "WARP Code of Practice v.2.0" (August 2004) <http://www.warp.gov.uk/BusinessCase/CodeofPracticeV2.0.pdf> accessed 18 November 2009.

42. For the CPNI, the desire to increase the prevalence of WARPs is clear. It believes that WARPs should become 'endemic' in the future, wherever a need is identified, whilst remaining sustainable, co-operative, flexible and versatile. It further envisages linkage between some WARPs and existing CERTs, with some potentially evolving into full CERTs themselves before concluding that "the future of WARPs is bright".[70]

43. There is limited material available in relation to the overall effectiveness of WARPs. This is probably due to their having been in existence a comparatively short time and being few in number. However, given the similarities between WARPs and CERTs in many respects, it seems reasonable to assume that they may both suffer from similar limitations in terms of capacity and inter-WARP communication. The latter may be less significant, since WARPs are focused on domestic concerns and registered WARPs may use a common communications infrastructure provided by the CPNI.

44. Given the smaller reach of WARPs, they may be considered to be the cyber-equivalent of a Neighbourhood Watch scheme. While there is some element of proactive promotion of WARPs from the CPNI, the protection of individuals from computer misuse is not core to its purpose which is properly concerned with the protection of critical national resources from terrorist or other attacks.

The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?

45. A pan-European approach would provide greater consistency in determining those infrastructures which are critical to Europe as a whole as well as the individual Member States. National responses may be fragmented and inefficient, but they would allow each Member State to protect those parts of their own infrastructure that may fall outside the pan-European designation. It may be preferable for a pan-European set of infrastructures to be identified, particularly where these span national borders, while allowing Member States to augment these with other infrastructure components as they see fit.

46. It is likely that multi-national companies would welcome multi-national policies which facilitate greater ease of implementation and management.

The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?

47. Within the various theoretical analyses of risk, there is a common theme of the withdrawal of the direct intervention of the state in the management and regulation of risks in favour of diffuse networks of risk management actors enabling individuals to take responsibility for themselves within the "new legal order" offered through insurance. For O'Malley:

> …these responsibilising processes seemingly democratise government through the mobilising of risk and uncertainty. Individuals and communities are made free to choose how they will govern themselves in relation to a host of insecurities.[71]

48. The question to be considered is how such unforeseen risks should be addressed. This model of risk management by individuals and communities working alongside the state is referred to as "governance".

49. The ambit of the term has expanded to encapsulate something distinct from government which includes non-state contributors. For example, Hyden considers that:

> Governance is the stewardship of formal and informal political rules of the game. Governance refers to those measures that involve setting the rules for the exercise of power and settling conflicts over such rules.[72]

50. For Rhodes "governance…is about regulating relationships in complex systems"[73] and for Hirst and Thompson "governance…is a function that can be performed by a wide variety of public and private, state and non-state, national and international, institutions and practices".[74] Inherent in all these definitions is a recognition of something broader than government which includes informal as well as formal rules, described by Kjær as "networks of trust and reciprocity crossing the state-society divide".[75] This notion of some degree of independence from the state is echoed by Rosenau:

[70] ——, "The future of WARPs" <http://www.warp.gov.uk/Index/indexfutureofwarps.htm> accessed 18 November 2009.
[71] O'Malley, P, *Risk, Uncertainty and Government* (Glasshouse, London, 2004) 11.
[72] Hyden, G, "Governance and the Reconstruction of Political Order" in Joseph, R (ed), *State, Conflict and Democracy in Africa* (Lynne Rienner, Boulder, 1999).
[73] Rhodes, R A W, "The hollowing out of the state: the changing nature of the public service in Britain" (1994) 65 *Political Quarterly* 138, 151.
[74] Hirst, P and Thompson, G, "Globalisation and the Future of the Nation State" (1995) 24 *Economy and Society* 408, 422.
[75] Kjær, AM, *Governance* (Polity Press, Cambridge, 2004) 4.

> Global governance is conceived to include systems of rule at all levels of human activity—from the family to the international organisation—in which the pursuit of goals through the exercise of control has transnational repercussions.[76]

51. As with Hyden, Rosenau's definition of governance also involves the concept of a network: in this instance, a transnational network of states, providing global governance within a framework of international relations. Rhodes provides a complementary perspective:

> Governance refers to self-organising, interorganisational networks characterised by interdependence, resource-exchange, rules of the game and significant autonomy from the state.[77]

52. As Kjær summarises, definitions of governance focus "on the role of networks in the pursuit of common goals". These networks may consist of a variety of state and non-state participants active in a particular area of policy. The degree of cohesion will naturally vary from network to network.

53. Rhodes attempts to draw these definitional strands together in suggesting that the shared characteristics of governance are interdependence between organisations, continuing interaction between network members, game-like interactions rooted in trust and a significant degree of autonomy from the state.[78]

54. It is common ground, then, that governance blurs the distinction between the state and society with the state becoming a collection of networks with no sovereign actor able to steer or regulate. Forms of economic and political organisation are affected.[79] Braithwaite considers that risk management "decentralises the role of the state" compared with corporations and hybrid public/private regulators.[80] Offe concurs, stating that:

> the outcomes of administrative action are in many areas not the outcomes of authoritative implementation of pre-established rules, but rather the results of a "co-production" of the administration and its clients.[81]

55. Lenk considered that the state can no longer control technology by itself and foresaw the potential emergence of a governance approach to its control:

> Taken together, badly designed technology, *misused technology* and unmastered technology concur to put society in a position where it can no longer aspire to regulating and controlling all details through its political institutions. Well-regulated sectors will co-exist with others from where we may expect influences which trigger the emergence of new types of individual and collective behaviour.[82]

56. This viewpoint acknowledges that the state is not impotent in its ability to regulate networked technologies. Hirst and Thompson comment that "if…mechanisms of international governance and re-regulation are to be initiated, then the role of nation states is pivotal"[83] although the partnership between society and the state has necessarily limited the scope of state intervention.

57. Therefore public-private partnerships are an essential component of the governance approach to managing risk associated with networked technologies and infrastructures. The Commission is correct in its aim that public-private partnerships at the European level should be encouraged.

Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?

58. CERTs have two principal functions. The first is proactively to disseminate information regarding prevention of technical vulnerabilities and threats. The second is reactively to provide assistance in response to particular instances of computer misuse. CERTs exist to serve both public and private interests across a range of constituencies. They may therefore operate from both "top-down" (governmental) and "bottom-up" (private) perspectives. However, in isolation, an inwardly-focused CERT will operate as an information silo; that is, it will not exchange relevant information with other CERTs. Indeed, many CERTs have a closed constituency and may not even desire to participate in such information sharing. This lack of reciprocity is fundamentally at odds with the networked approach required within governance theory, even though the individual CERTs themselves may represent both public and private concerns. Facilitating communication and information-sharing between CERTs should therefore lead to a structure more aligned with the governance approach.

---

[76] Rosenau, J N, "Governance in the Twenty-First Century" (1995) 1 *Global Governance* 13.
[77] Rhodes, R A W, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 15.
[78] Rhodes, RAW, *Understanding Governance: Policy Networks, Governance, Reflexivity and Accountability* (Open University Press, Buckingham, 1997) 53.
[79] Stewart, A, *Theories of Power and Domination: The Politics of Empowerment in Late Modernity* (Sage, London, 2001).
[80] Braithwaite, J, "The new regulatory state and the transformation of criminology" (2000) 40 *British Journal of Criminology* 222, 228–9.
[81] Offe, C, *Contradictions of the Welfare State* (Hutchinson, London, 1984) 310.
[82] Lenk, K, "The challenge of cyberspatial forms of human interaction to territorial governance and policing" in Loader, B (ed), *The Governance of Cyberspace* (Routledge, London, 1997) 134.
[83] Hirst, P and Thompson, G, "Globalisation and the Future of the Nation State" (1995) 24 *Economy and Society* 408, 430.

59. This has been achieved to a certain extent at both national and international level through various forums of varying degrees of formality, membership and geographic reach. In essence, there is a state-led imperative for co-operation between institutions which often exists only to serve private interests. Provided that there is at least some co-operation, however reluctantly, it follows that CERTs should have a part to play within an overall governance network on the basis that even limited information-sharing is better than none at all.

60. However, in order to achieve a meaningful role within this network, CERTs need to be effective, both internally in their capacity to cope with the nature and extent of their workload as well as externally in the efficiency of their information exchange. Historically, CERTs have been characterised by constrained resources and increasing workload. Moreover, despite the existence of the diverse umbrella co-ordinating bodies, communications between CERTs are inconsistent, depending upon the cultural values and individual priorities of each CERT.

61. Even though an ideal CERT network seems well-suited as a extra-legal response to the problem of cyber-attacks, it must be recognised that CERTs cannot exist in a legal vacuum. The law still has the role of governing and informing the internal framework within which the CERT operates. However, CERTs do offer the advantage of an alternative response beyond that of the law in isolation and bring private concerns and day-to-day technical incidents into the response network.

Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?

62. Provided that the European-wide system allows the UK to deliver at least the same level of protection against cyber-attacks, its existing approach should not be adversely affected by following a pan-European system, and, given the cross-border implications of an attack on many critical infrastructures, should give the UK a greater level of protection from the consequences of the risk of an attack on another Member State.

Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

63. In recognition of the fact that cyber-attacks on the European critical infrastructure could easily emanate from outside the EU it would seem sensible to adopt a worldwide approach. However, the uniform adoption of a global minimum framework within each nation state with clearly defined cross-border co-operation, investigation and assistance provisions is a panacea.

64. This has been most notable in the criticisms levelled at the Council of Europe Convention on Cybercrime.[84] As Brenner and Clark comment, since it incorporates substantive and procedural law that may not be routine in some Member States then:

> …it means implementing the Convention will be a complicated process for many countries, one that will take time. Consequently, even if the Convention proves to be a viable means of improving law enforcement's ability to react to transnational cybercrime, we are unlikely to see any marked improvement in the near future.[85]

65. This view is echoed by Flanagan who further considers delay resulting from the prospect of constitutional difficulties, the propensity of individual legislatures to "do things their own way" and the "workings of special interest groups to ensure their input into national implementations all around the world".[86]

66. Lewis[87] criticises the effectiveness of the Convention (in common with all international initiatives) on a number of grounds. He considers that there is a lack of incentive for many countries to participate, particularly in those developing countries where computer crime is not yet a significant concern. He further argues that there will be problems with effectiveness even where countries do participate, citing a list of obstacles including the speed at which new technologies are developed, differences in certain substantive values between States, different standards for conviction, the imposition of different punishments upon conviction, the failure of many countries to commit adequate resources to fighting computer crime and the lack of any viable international body to coordinate national agencies and enforce international agreement.

67. Weber[88] also highlights the potential flaws within the Convention, arguing that it will fail without universal participation and will take "years" to ratify. Lack of worldwide participation could lead to safe havens beyond the Convention's reach, meaning that states will still need to take unilateral action against

[84] Council of Europe Convention on Cybercrime (signed 23 November 2001) ETS 185.
[85] Brenner, S W and Clarke, L L, "Distributed Security: Preventing Cybercrime" (2005) 23 *John Marshall Journal of Computer and Information Law* 659, 671.
[86] Flanagan, A, "The law and computer crime: Reading the Script of Reform" (2005) 13 *International Journal of Law and Information Technology* 98, 117.
[87] Lewis, B C, "Prevention of Computer Crime Amidst International Anarchy" (2004) 41 *American Criminal Law Review* 1353.
[88] Weber, A M, "The Council of Europe's Convention on Cybercrime" (2003) 18 *Berkeley Technology Law Journal* 425, 444–5.

individuals in countries that fail to join, ratify, implement or enforce the treaty. For Goldsmith, such unilateral assertions of power might encourage accession to the Convention and facilitate global adoption.[89]

68. The United Nations has the broadest reach of the intergovernmental bodies covering virtually all recognised states. It has adopted broad resolutions in the areas of computer crime; these are recommendations and compel no action on the part of Member States. Legislative action in the form of a UN Cybercrime Convention to build and improve upon the Council of Europe offering is still considered premature. The UN is instead focussing on providing technical (rather than legal) assistance to Member States thereby harmonising technical capability rather than legal regulation.

69. This approach of providing technical assistance is similar to the that adopted by the UN in relation to terrorism. Following the attacks on the US of 11 September 2001, the UN introduced a two-fold mechanism to facilitate global adoption of effective laws against the financing of terrorist activity.[90] The problem that the UN faced was that states such as Yemen, for example, were disinclined to take action since such action was inconvenient, not a national priority and difficult to implement for lack of technical expertise. The UN therefore established the Counter Terrorism Committee to which all states were called upon to report on the steps taken to implement its proposals (many of which required legislative action). As well as acting as a focal point for the UN efforts, this Committee also facilitates the provision of "assistance of appropriate expertise"[91] to states in furtherance of the objectives set out in the Resolution. Therefore, the UN takes a role of co-ordination and assistance rather than direct coercion. However, this arrangement was only brought into being as a result of the political impetus following 11 September 2001. It is therefore reasonable to assume that that a similar co-ordinated international approach to cyber-attacks would require an event of similar gravity to precipitate it. However, the conceptual idea of co-ordinated international technical assistance remains at least theoretically attractive.

70. In the absence of a concerted and committed global response to the issue, a European-centric policy may be the simplest and most compelling option to protect European interests.

18 November 2009

Memorandum by Intellect

1. Introduction

This submission has been prepared by Intellect in response to a call for evidence from the House of Lords European Union Committee—Home Affairs (Sub-Committee F) inquiry into EU policy on protecting Europe from large scale cyber-attacks. Intellect is grateful for the chance to provide input into this debate and would welcome the opportunity to discuss these issues in more detail.

2. About Intellect

Intellect is the UK trade association for the IT, telecoms and electronics industries. It represents over 750 companies ranging from SMEs to multinationals. Its members account for over 80% of these markets and include blue-chip multinationals as well as early stage technology companies. These industries together generate around 10% of UK GDP and 15% of UK trade.

Intellect is a not-for-profit and technology neutral organisation, which provides a collective voice for its members and drives connections with government and business to create a commercial environment in which they can thrive. As the hub for a networked community, Intellect is able to draw upon a wealth of experience and expertise to ensure that its members are best placed to tackle challenges now and in the future.

UK Government, industry, infrastructure and other national interests face a myriad of digital threats—from cyberwarfare to data loss—which need to be met through ever-improving Information Assurance (IA). Across this broad spectrum of policy, market and stakeholder areas, Intellect is working with Government and the technology industry to address the challenges emerging from the Cyber domain.

Intellect's Cybersecurity group has been formed to provide a coherent voice for industry working in "high threat" areas—including defence, security, national resilience, intelligence and organised crime.

The group, which represents around 50 technology companies, works alongside and in partnership with Intellect's wider Information Assurance programmes, which focus on broad public and private sector information sharing, assurance, security and handling.

[89] Goldsmith, J L, "The Internet and the Legitimacy of Remote Cross-Border Searches" (2001) 1 *University of Chicago Legal Forum* 103, 117.
[90] United Nations Security Council Resolution 1373 (28 September 2001).
[91] Ibid, art 6.

The Cybersecurity group's purpose is to communicate industry's positions and needs, provide policy inputs to Government, and facilitate customer-supplier dialogue in "high threat" areas, as follows:

— Championing industry views: A broad range of national and international stakeholders are active in the Cybersecurity field, and Intellect has a leadership role to play in ensuring industry's views on threats, opportunities and exploiting technology are understood at the appropriate levels. The group will articulate and champion coherent industry views on the Cybersecurity market, ensuring that consideration of future strategy reflects industry's capacity, requirements and capability.

— Industry contribution to policy: Following the publication of the UK's first Cybersecurity strategy, policymakers are keen to ensure that Government policies are fit for purpose. Industry is a key partner to the public sector in this area, and the group will provide consolidated industry contributions to governance, industrial, acquisition, and technical policy as appropriate, as well as undertaking joint activities to improve skill levels and drive cultural change.

— Market awareness and engagement: Greater understanding between Government, private sector customers and industry is vital to developing and deploying new capability. The Cybersecurity group will provide linkage between users (including Cabinet Office, CESG, ICO, CSIA and CSOC) and suppliers to share knowledge around best practice, legislative and regulatory information and developments in technology. Intellect also provides a structured and non-prejudicial channel for industry engagement around projects and procurements.

3 Responses to Consultation Questions

1. *Threat analysis*

— *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?*

This is very difficult to answer as it depends on many factors. The infrastructure that underpins the Internet is unregulated, and is very varied in terms of quality, sophistication and resilience. Technical failure of major backbone elements is entirely possible and has the potential to have a very serious impact on the running of the Internet.

— *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

Duplication, fragmentation and diversity in infrastructure have been strengths of the internet. But the quality of the infrastructure of the Internet is unregulated and is not "owned" by a single body. There is a fundamental problem around regulation of Internet—"who do you regulate?" The many and various businesses all spend time, effort and money ensuring the resilience of their services; however, they are extremely dependent on other industry suppliers doing the same. Introducing blanket, internationally based regulation would be complex, time-consuming and fragile. The pace of change of technologies which underpin and utilise the Internet is such that any regulatory intervention would be out of date before it came into effect.

— *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

Yes, the concerns are justified as many items reported in the media demonstrate. Since the field is classified, Intellect members cannot comment further in a public document.

— *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

The military, but especially other civil government organisations such as CESG, GCHQ, CPNI and now the OCS and CSOC, undoubtedly have a role to play and are a source of expertise. But they do not have the capacity or legal mandate to protect the Internet. The government has a role to play in encouraging security measures in a critical part of the UK infrastructure, however, the Internet is not a UK-owned infrastructure, it is a sum of parts, owned by communications services providers, ISPs, software vendors and users.

— *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

We should be very concerned about criminally operated "botnets". There is evidence gathered by several government organisations, as well as security solution providers in industry, that shows that this misuse of the Internet is on the rise. Clearly a common legal framework across Europe, that criminalised aspects of computer misuse, might be of benefit—there are wide and varied inconsistencies in the nature of what is designated cyber crime across Europe.

2. *International responses*

— *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

National responses are likely to be fragmented, if for no other reason than the varied technical infrastructure that each member country enjoys, the different legal frameworks under which they operate and the different sophistication and capacity of native industries within those countries. Multi-national companies would generally be in favour of multi-national policies if practical and workable. Many companies operate at an international level, in terms of provision of services, but have to provide technical infrastructures that are different according to the legal requirements of the country concerned.

— *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

It is difficult to envisage how such measures could be taken at a European level without materially disadvantaging national industry players.

— *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

Probably. Providing this is done in concert with existing national bodies who already provide this kind of response.

— *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

— *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

This is likely to make an already complex matter more complex. Effective national policies should be in place before broadening to a wider multi-national stage. In broad terms, creating effective national policies that are internationally consistent would be helpful to the supplier industries.

— *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

More pressure should be put on countries that do not currently have well formed policies and regulation to reform their own industries and reduce criminal activities.

3. *European Network and Information Security Agency (ENISA)*

— *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

— *Is ENISA being effective in its role, or does it need reform?*

The scale of national endeavours greatly exceeds the present capacity of ENISA. If ENISA is to have a role as a serious centre of excellence and creator of policy, then it needs to be more substantial than is currently the case.

4. Conclusion

Intellect would welcome the opportunity to discuss the issues highlighted in this submission in greater detail, and would be happy to facilitate a dialogue with industry representatives.

20 November 2009

Memorandum by ISACA — London Chapter

1. ISACA London Chapter welcome the opportunity to provide evidence to this Sub-Committee on a topic that is very important to all its members, and members' clients.

2. This response was put together by Sarb Sembhi as President of the London Chapter and does not represent the view of ISACA International in any way.

3. Our response has been inserted into the original "Call for Evidence", as many of our responses are related to the questions that are raised and require a response.

4. As a backdrop, we believe: We are already engaged in Cyber War today—looking at any border device and what is attempting to connect to it will show at the lowest level that members of the public are contending with security, while the criminals are trying to access the device. If (as stated) one opens an "intrusion detection system" (IDS) to look at the intrusive attempts, the logs fill so fast there is no way to keep up with reading the content. This is seen on both the business border device, government, as well as home border device.

Sub-Committee F (Home Affairs) of the House of Lords Select Committee on the European Union is conducting an inquiry into EU policy on protecting Europe from large scale cyber-attacks.

5. Apart from this Sub-Committee, who else in the UK is looking at this, and what is the relationship between all the parties. There is concern that this issue does not get bounced between several organisations over a period of time, as has happened with other issues discussed in Parliament.

Following on from the EU Directive 2008/114/EC "*on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection",* in March 2009 the EU Commission published a Communication on Critical National Infrastructure Protection entitled *"Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience"* (COM(2009)149 final, Council document 8375/09). This document was accompanied by 400+ pages of *"Impact Assessment"* (COM(2009)399 and 400, Council document 8375/09 ADD 1–4) setting out the background to the Commission's approach to this issue.

6. We are concerned that the work on this was actually started several years ago and that it has taken so long to filter through to the lower levels at an EU member state that this time lag does not inspire confidence that responses will be able to get back to the EU level, decided upon and back down again for action (some of which may be vital) to be taken.

7. With regards to the approach mentioned above, we welcome this, but as has been shown by experience in the US, if the approach is too complex and not related to core business, and real actual benefits, approaches will remain as just that, approaches. SME's who form a great percentage of the Critical National Infrastructure will not be able to benefit from all the same approaches that large enterprises can, and this must be tackled at an early stage.

The Commission is concerned that an increasing number of vital services depend on digital systems, and in particular on a working Internet. Major economic or social damage could be caused if these digital systems are disrupted, either by "hacking" or "spamming" attacks, or as a result of technical failures, or as a side-effects of a natural disaster.

8. This is key to the issue—there is a big assumption that the Internet will always be there—however, let us not forget it is ungoverned, but almost US (sic) controlled, and now heavily dependent for business, and the end product of GDP—the question is, what would be the real socio, and economic impact should "it" not be fully, or part available?

Sic—Going back in time when a root server was redirected, the US took a stronger hold on the Internet — they are friendly forces, but how would a government feel if this were a hostile nation/or just a less friendly nation?

9. There seems to be an assumption that Cyber Attacks are confined to Availability or Confidentiality of systems, there needs to be a recognition that attacks to the Integrity of such systems is also vital.

10. Further, that attacks could take place at the device level, ie mobile devices.

The Commission is especially concerned that intentional "cyber-attacks" are growing in sophistication and frequency, and that the risks that services now run are poorly understood and insufficiently analysed.

11. Lip service has been given to this in the UK, the CPNI have avoided the subject, whilst at the same time seemingly doing something about it. It is also interesting that the term Cyber Terror is very much avoided—this is an element which it would seem, does not exist, or has not been publically acknowledged. If your Sub-Committee recognises the term, will all government bodies equally recognise the term having the same meaning?

12. We do not believe that the risks are "poorly understood and insufficiently analysed" since some industry sectors are spending millions every year on protection, and every month an anti-virus or anti-malware vendor produces a report illustrating and explaining (before competitors do) the most recent and "innovation" in new attacks.

13. There seems also to be a trend that attacks are more targeted to individuals or organisations, and not necessarily whole countries (although there are examples of these). Targeting units small than a country, does mean that it may get less attention, as businesses may not want to let information of an attack a subject of public knowledge.

The proposal has four specific goals:

— to bridge gaps in national policies for security and resilience of critical systems;

— to enhance European governance of this area;

— to improve Europe's incidence response capability;

— to improve the resilience and stability of the Internet.

14. We understand and appreciate that the inherent problem with goals can sometimes be that they can be too wide to be meaningless, or too specific to exclude so much of what needs to be included. Further, that the definitions used need to be explained to have a common understanding of what is in and out of scope. We believe that the above goals suffer from these problems.

15. What is a Critical System? — If a nations GDP is at risk, that could also be any business in excess of £"n" pa — and to damage nation does not have to touch HMG, but as we have seen, just the economy.

16. The public perception in the UK of any Action from the EU is very negative in that it is likely to be too little, too late, and inappropriate to local needs. If the EU is to provide a lead, it is important that it doesn't fall into the public perception trap.

This inquiry will focus on what are the proper roles for the EU and its Member States in this important area, where many of the critical systems involved are operated by private industry and not—as was once the case for communications providers—by public bodies. The Sub-Committee welcomes evidence on all aspects of the inquiry, but in particular on the following issues:

Threat analysis

— *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?*

17. The first question here should not be focussed only on "technical failures" but any failures to get a true understanding of the issues.

18. There are plenty of publicly documented cases illustrating natural disasters effects on service delivery (affected by the lack of access to the Internet)

— *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

— *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

19. Such concerns will vary from country to country based on that country's own infrastructure, some are more resilient than others.

— *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

20. Any involvement of any military groups would most likely be done on a risk assessment basis, whereby such involvement would enable movie like scenarios more likely. And would increase the military's ability to use the Internet for its own purposes without outside knowledge. We believe that any military involvement should be very carefully considered and only temporary, wherever it is felt that alternative options are exhausted.

— *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

21. As noted above there are plenty of publicly available research on all types of malware (including botnets) and their spread. The area we think that needs consideration, and seems to have been omitted here is the large volume of research both commercial and academic, and its practical use in protection. It seems that criminals

are making better use of the research to identify new approaches, tweeking existing methodology, to get more effective results.

22. We are also interested in understanding where does the new set up in Greece fit in here — what is their value to this exercise?

International responses

— *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

23. We believe that this analysis is incorrect, as some nations are far more advanced than others, and that those that are behind need to learn from the good practices. To colour all nations with the same brush would be detrimental to the existing efforts of some nations.

24. What is required is a two pronged approach:

First, each nation feeds in good practice, and implements that good practice (in the same way that this exercise is intending to learn from the US).

Secondly, at the commercial national level feed in and share practices at the multinational level for its own commercial advantage.

— *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

25. Such partnerships have been talked about for a long time now. However, we believe that there is far too much commercial opportunities presented here, and (in own opinion) not so much help.

26. We also believe that there may be too many individual nation interests for this to work effectively at an EU level.

— *Are there indeed failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

27. NORAD at Iron Mountain are a good example of processes and facilities for dealing with Cyber Attacks, (and are way ahead of the UK).

— *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

28. We believe there is a need for nationally based bodies to coordinate response to EISAS, rather than the other way around, especially considering that it doesn't make sense to disintegrate local expertise to then put it at the regional level, thus leaving the local level losing out.

— *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

29. We believe that CERTs are slow compared to some of the commercial services out there, (for example Secunia). If the CNI is to rely on CERTs, they would have to change practices to meet the needs of the CNI, until then who else can be relied on?

— *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system — or will this lead to improvements?*

30. We need to know what the UK policy is before we can comment, we do not believe there is sufficient publicity around UK policy for anyone to find it easily.

— *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

31. There has been some criticism about the US policy, as the working practices that were being promoted to government bodies were too complex and too costly to be effectively implemented and as such many government departments were just ignoring the guidance. We agree that there needs to be a consistent approach (whether it is European-centric, US-centric, or any other centric approach), but that the approach must be one that can be adopted and implemented at a national level by both the public sector (government departments), and private sector (both SME's as well as large enterprises). Else which ever approach is offered, it will fail, and the US has several good examples of this too.

European Network and Information Security Agency (ENISA)

— *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

32. ENISA's current work in educating the business community, has had some level of success, we believe that this role cannot be overlooked as part of the strategy to get information out to SME's.

33. Before ENISA plays any role in CERTs or developing EISAS, it is important to get CERTs running effectively right across the EU, which is not the case at present.

— *Is ENISA being effective in its role, or does it need reform?*

34. ENISA should be tasked with assisting with compiling research (commercial and academic) that is of relevance to this field, and disseminating to those organisations that need to be aware of it in a format that would make it useful. Currently, attackers pick up any research they need without complaining what language it is written in (unlike some EU nations), the sooner professionals protecting the CNI are able to use it, the sooner we will be better protected.

35. Apart from the above (collation of security/resilience research), we do not believe that there is any additional requirement for reform.

Timescales

— *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

36. As noted above, it has taken several years to get this far, we think it unlikely that we will see anything useful by the end of 2010.

37. There is a need for workable standards for CNI and those organisations that form the CNI, be they public or private, be they large enterprises or SME's. In this respect SME's may require access to additional funding unless we are to end up in a position of creating unintended monopolies of cash rich companies who are able to comply with guidance (compared with cash strapped companies who have unique expertise in products or services losing business due to non-compliance).

38. We would like to point out some obvious omissions in your call:

— There is no mention of the volumes of research produced by security researchers (private, commercial or academic), the results of which are picked quicker up by criminals and put to bad (but effective) use.

— There is no mention of the role of Law Enforcement, nor of the data that is collected by intelligence services run by nations to feed into protecting the CNI at an EU level.

— There is no mention of data sharing from and between the various sectors that form the CNI that is currently taking place already.

13 November 2009

Memorandum by ISSA-UK and BCS

1. Introduction

1.1 ISSA-UK, Information Systems Security Association and BCS, the Chartered Institute for IT, are pleased to submit a joint response to the House of Lords Select Committee into EU Policy on Protecting Europe from Large Scale Cyber Related Attacks.

1.2 Global hacking and spamming attacks have become progressively more frequent and, in some cases, serious threats to government and business interests. The threat of hacking has become an increasing nuisance to all organisations and it drives up the cost of security countermeasures. It is widely predicted that there is much worse to come. There are clear trends in the exposure of information systems and infrastructure. Each of these gives rise to concern and collectively they create a major security threat to all networked IT services that demands a coordinated and mandated security response by all government and business stakeholders. It is noted that the recent establishment of a Cyber Security Cell in the Cabinet Office and at GCHQ is a welcome response to these threats/attacks.

1.3 There is no doubt that government and business systems processing sensitive citizen information and supporting critical national infrastructure are becoming increasingly complex, connected and therefore vulnerable to damaging cyber attacks. This exposure is further amplified by the growing use of outsourcing, off-shoring and "cloud computing" services, all of which serve to reduce both the visibility of security risks and our ability to respond to them.

1.4 It is also clear that the growing use of electronic channels for delivery of key business and government services greatly increases citizen dependency on critical national infrastructure. This is underpinned by on-line sensors, high speed networks and centralised databases, all of which present attractive targets for agencies that wish to steal data or disrupt business operations.

1.5 There is evidence that organised crime, terrorists and hostile intelligence are all actively seeking to steal data and damage national interests. As time goes on, we will see a much greater sophistication and subtlety in the way they approach their attacks. Denial-of-service and espionage attacks represent the tip of an iceberg of emerging security threats. Beyond these threats lies the real threat of selective modification of data in order to manipulate perception, undermine customer confidence or destroy the value of business services.

1.6 Corruption of critical data records can create long-term, perhaps unrecoverable, damage to an enterprise. These are serious, long-term threats but they should not deflect attention from the more immediate problem that industry and government agencies today are still largely unprepared to defend against many less sophisticated threats, some of which can cause real damage to business interests but, at the same time, can be mitigated to a large extent by basic management practices such as good contingency planning and crisis management.

1.7 National policies are slow to develop and even slower to implement. This subject area is fast moving and demands a fast-track process, capable of driving through radical change across an inter-dependent, networked community. Traditional processes for implementing public policy are not sufficiently agile to counter emerging security threats.

2. Threat Analysis

How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?

2.1 The Internet is an unusual medium for global communications; a country could lose access to the Internet while all other countries could still use it. The Internet is susceptible to failure, from the mundane accidental digging up of a fibre optic backbone of the telecommunications network, to the more specific act of a power failure in Docklands arising from heavy flooding or perhaps a malicious attack on the grid system. All have the signature of a Cyber Attack. Other failure mechanisms include software failures in Internet components such as routers. Routers are commercial items and software quality standards may be less stringent than for government/defence systems, as facilities and features of the software and devices become ever more sophisticated and difficult to test. The interdependency of communications and energy sector creates a significant vulnerability to cascaded failure.

2.2 The massive distribution of the Internet makes it intrinsically resilient. A major attack against DNS Rootservers in 2002 was not able to take it down. But individual enterprises and critical infrastructures can be vulnerable to attack. The nature of the attacks, however, is largely the same, so there is significant potential cooperation across private and government sectors to prepare and respond to future attacks.

2.3 Government increasingly relies on private sector services, and both industry and government increasingly rely on SME services, many of which have little or no security in place. Small sub-contractors represent the soft underbelly of Critical National Infrastructure, as well as business services handling sensitive citizen data. Much more needs to be done to educate and motivate this sector, as well as to translate policies and standards designed for large organisations into something applicable to much smaller business units.

2.4 SMEs often perceive the advice offered to larger enterprises to be less relevant, patronising or simplistic, though such advice might encourage simple, practical and economic security improvements. Advice to this market has traditionally focused upon the needs of the larger SME, the very different scales of business are not always taken into account. An encouragement of "cloud computing" solutions with appropriate embedded security installed by technical experts is likely to present a viable solution, but this service must be made attractive, competitive, and demonstratively secure. Much more needs to be done to educate and motivate this sector, as well as to translate policies and standards designed for large organisations into something applicable to much smaller business units.

2.5 Rapid changes in the security risk landscape coupled with widespread ignorance of the consequences to business operations demands a step change in our education, skills and response to emerging security risks. Two current trends present particular concerns. The first is the understandable tendency for cash-strapped business managers to accept increasing levels of risk rather than invest in expensive countermeasures in the

current financial environment. The second is the difficulty in making a financial business case for controls that address unprecedented incidents, especially where the consequential damage to individual company interests might be limited, though there might be a hazard to external parties, such as employees or citizens.

2.6 Contemporary risk assessments carried out to determine security countermeasures for information systems have generally been developed in a climate in which local, short term financial interests are paramount. Such practices are hard to adapt to a changing risk landscape in which unprecedented levels of consequential impact might arise for customers, employees or business partners.

2.7 There is an argument for establishing minimum standards of security for situations in which the potential harm from an incident is to parties other than the organisation responsible for addressing the risk. We believe that this can be partly addressed through enhancement of the existing ISO/IEC 27000 standards, though a high-profile sponsor would be needed to drive through such a change. Such standards need however to be carefully constructed to ensure they are realistic, acceptable and adaptable across different sized companies and industry sectors without unreasonably favouring particular organisations.

2.8 There are two elements in play. One is the network infrastructure and the other is the service provider who provides the IP overlay network that is the Internet. Very few Internet Service Providers (ISPs) own their own network infrastructure. Without a resilient infrastructure, there is no guarantee that the ISP will be able to employ it to create a resilient network. To sustain networks and infrastructures in the UK, some form of regulation will be required to provide the resilience and assurance to counter Cyber Attack.

The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?

2.9 We believe that the cyber attacks against Estonian and Georgian governmental sites could have been mitigated if there had been effective procedures and resources in place. Some parts of the private sector, such as the online payment and gaming sectors, have been targets for many years and have been able to successfully mitigate many attacks. Research to gather learning points and best practices from these industries would be beneficial to the wider community.

2.10 It is believed the threats are real and a major concern to government and business services. The nature of the threats however presents a major challenge for traditional forms of military protection and response, because the assets at risk are intellectual rather than physical; the battle space is used for day-to-day business, and the attackers exploit innocent intermediaries. Cyber warfare demands a radically different response, which has as yet to be adequately articulated, debated and agreed.

The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?

2.11 The impact of these attacks if targeted against the UK's Critical National Infrastructure could severely damage the economic and civil balance of the nation. It is not considered appropriate for the military to be charged with Cyber defence: the military do not have enough resources to carry out this function. Cyber defence is the responsibility of government and the UK has taken the lead by the establishment of a Cabinet Office Cyber Security Centre.

How concerned should be we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?

2.12 Botnets are used to perpetrate a host of different attacks including DDoS, Keylogging, Warez, Spaming, Phishing, Web-scraping in fact any form of attack that can be automated and requires anonymity. "Botnets" are of interest to many bodies, including those with commercial, criminal, military or terrorist, intelligence interests. The scale of the problem and the future potential is large and growing. It demands a coordinated approach by all stakeholders. It cannot be addressed by, for example, law enforcement or military action alone.

2.13 The reason that botnets are effective is because they are relatively easy to establish. On the other hand, they are also relatively easy to detect and to mitigate. We believe that a concerted effort by government and private sector would be both feasible and beneficial to all parties. Greater coordination of resources to absorb attacks, spot botnets and gather forensic evidence would add significant additional resilience to mitigate botnet attacks.

3. International Responses

The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?

3.1 The Internet and the "cloud computing" services it supports present attractive economies of scale but do not guarantee service levels. Customers must accept a degree of risk of disruption in the pursuit of cost savings and convenience. On the other hand, however, the business impact of Internet failures is becoming progressively greater and justifies a degree of intervention to safeguard those interests. We need to strike the right balance to ensure business and customer expectations of service levels are reasonable and realistic.

3.2 The resilience and stability of the Internet demands a collective, networked international incident response capability across industry and government. Currently this is done on a highly selective basis with only a small proportion of major organisations (and extremely few Small and Medium Enterprises) operating a computer emergency response capability.

3.3 International companies and any enterprise with an international customer base will generally seek a global rather than a European solution. In the absence of an international response, however, a European response is a step in the right direction. However, as global as the Internet is, local factors remain significant for budgeting, sales and marketing within specific cultural, linguistic, logistical and regulatory regions. There is benefit therefore in adopting a tiered strategy that ensures an effective response at several levels.

The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?

3.4 In the security field, public-private partnerships tend to be talking shops rather than joint ventures. They are useful for sharing best practices but by themselves are unlikely to drive through the required levels of change. There is evidence however that attacks can be launched by private sector organisations on government targets, and *vice versa*. There is therefore a good, logical case for a shared public and private response effort and protective infrastructure.

Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?

3.5 High impact, low probability events are hard for individual organisations to address, especially where there is a degree of systemic risk involved. Greater invention is needed across individual market sectors to identify and progress opportunities for improvement.

3.6 The Internet is becoming the major communications highway of commerce and indeed the majority of the population. Both central and local government services are turning to the Internet for increased efficiency and citizen engagement. However the Internet is nothing more than a number of disparate commercial IP based networks that are interconnected. The issue here is what happens when a major network service supplier goes bankrupt and the network is no longer available.

The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?

3.7 Experience with early attempts at Information Sharing and Analysis Centres (ISACs) demonstrated that, in practice, sensitive incident information is very hard to share across different industry sectors and international communities. Perceptions of the fundamental purpose and benefits of such circles also vary widely, encompassing education, networking, mutual support and collaborative response as well as the difficult problem of incident sharing. Incident response is a highly focused, disciplined and specialist demand which requires a different level of engagement from informal networking. Such approaches add value but need clear objectives, funding and levels of commitment.

Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?

3.8 CERTs are a useful, effective and essential response measure but they demand high standards of skills, training and rehearsal, and they are unlikely to have sufficient capacity to deal with widespread multiple incidents, as might be encountered in a large scale major cyber incident. We need a greater number of

professional CERT teams across industry and government, although this might prove expensive for many organisations to maintain.

Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?

3.9 It is considered that the nation needs a Government or Agency body to oversee/co-ordinate cyber protection. It is an area where legislation is required eg If ISPs in the UK were mandated to accept email only originating from registered email servers, then spam would be reduced as botnets sending spam would not be able to function. If all ISPs in the EU were so mandated, then the spam transmission would drop substantially.

Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?

3.10 Policy makers need to be close to government departments and industry. The prospect of a remote, ivory tower, central policy unit is not attractive. It is unlikely that existing policies will be fit for purpose as we move forward. Policies must be under regular review by those who operationally employ them not just those who legislate.

3.11 The UK needs both local support and international intervention. A European approach can serve to bridge this gap as well as to drive a wedge between such interests. US perception and practice in security is different from UK and Continental Europe with more emphasis on technology and less on the human factor. There needs to be international consistency. The UK should adopt a much more positive attitude to working with the US, thus allowing the UK to bridge the gap between the EU and US.

4. European Network and Information Security Agency (ENISA)

The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work? Is ENISA being effective in its role, or does it need reform?

4.1 We are not aware of any major impact or specific success arising from ENISA, though the concept of a European centre of excellence is a good one in theory. It is not clear whether in practice such a body could maintain the level of skills needed to provide the necessary leadership in this subject area. However the need for a central, strong CERT capability is widely supported. The role and contribution of ENISA over recent years should be reviewed in light of the increasing Cyber Threat.

5. Timescales

Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?

5.1 It is hard to imagine that any major change could be driven through in such a short timescale. Cyber security demands immediate attention but most change needs to evolve through distinct stages of process maturity over a number of years. There are potential short term achievements however, such as, for example, the establishment of a shared, global infrastructure and response capability to detect botnets.

6. Conclusion

6.1 Technology is our primary hope in dealing with large scale, sophisticated, targeted and real-time attacks. The Technology Strategy Board has been excellent in investing in applied research; the UK has a strong research community with very good links between government, academia, industry and the various associations that take an interest in security. In addition to CERTs we need to strengthen co-operation and information sharing throughout the various players who constitute the community that is likely to develop our next generation of defences; genuine sharing depends on trust and it is hard to see that trust operating more effectively at the European level than at the national level. The UK should focus on building on what we have and aim to provide leadership in Europe.

February 2010

Memorandum by Professor Farnam Jahanian

FOUNDER AND CHAIRMAN OF THE BOARD, ARBOR NETWORKS

1. Farnam Jahanian is Professor and Chair of Computer Science and Engineering at the University of Michigan and co-founder of Arbor Networks, Inc. Prior to joining academia in 1993, he was a Research Staff Member at the IBM TJ Watson Research Center. His research interests include distributed computing, network security, and network protocols and architectures. He holds a master's degree and a PhD in Computer Science from the University of Texas at Austin. He is a Fellow of IEEE and a Fellow of Association for Computing Machinery.

2. The author of over 90 published research papers, Farnam has served on dozens of advisory boards and government panels in recent years, including Internet2's External Relations Advisory Council, Chairman of the Board of Arbor Networks, and National Advisory Board for UM Office of Technology Transfer. He is the recipient of a National Science Foundation CAREER Award, the Amoco Teaching Award, the 2005 recipient of the Governor's Award for Commercialization Excellence, and an ACM SIGCOMM Test of Time Award in 2008.

3. Arbor Networks was founded in November 2000, based on research conducted at the University of Michigan and funded in part by a US Defense Advanced Research Projects Agency (DARPA) grant. Today, Arbor Networks is respected around the world as a leading provider of security and network management solutions for global business and government networks, including 90% of tier-one and 65% of tier-two service providers globally and many of the largest enterprise networks in use today. Arbor's solutions give customers a single, unified view into their networks' performance, helping them to protect their network infrastructure by quickly detecting anomalous behavior, enabling them to mitigate network security threats and ensure a high quality Internet experience for millions of end users.

4. BACKGROUND AND PROBLEM STATEMENT

5. The open nature of the Internet has clearly had a tremendous benefit for the world's economy and people. Its open access is key to this success. For all the benefits this brings individuals and businesses, this open access also lowers the barriers to action against a group or even a state, sometimes tipping the balance in their favor. These challenges do not exist in the real world, and we have to learn how to address them quickly.

6. The Internet's technologies have proven to be resilient to isolated failures due to equipment malfunction, configuration errors, and natural disasters with no single, central dependencies. Indeed, the Internet's history is littered with such events. Outages, however isolated, typically last a few hours at most before services are restored. Companies operate the Internet backbone with adequate resources for power and connectivity, with staffing to match. Service providers consistently strive to ensure smooth operations as it is their core business, and failure to do so will lead the market to simply discard them.

7. In the late 1990s, a series of high profile DDoS attacks against emerging electronic commerce providers and ISPs forced many to invest in new technologies to protect their own infrastructure. Arbor Networks was born out of this market need, and nine years later our products help protect a majority of the ISPs that form the Internet backbone.

8. One of the main objectives at Arbor Networks has been to foster real-time cooperation and coordination between providers to identify and mitigate these threats as close to the source as possible before they cause significant collateral damage across ISPs. This is not as easy as it sounds because these providers are such fierce competitors in the marketplace. This type of cross-provider collaboration had simply not been done before.

9. To facilitate the type of real-time collaboration that was required, Arbor launched the Fingerprint Sharing Alliance (FSA), a first-of-its-kind industry initiative. This is the first time worldwide telecommunications companies have been able to share attack profiles automatically, allowing providers to consistently protect one another and their customers from today's distributed threats. With the formation of the Fingerprint Alliance, a formerly laborious and tedious process has been replaced with an efficient and automated process, and a larger community can be engaged to solve significant threats to the Internet.

10. Attacks that crippled networks in the early part of this decade, and once threatened the Internet as a global communications and commerce platform, have become well-managed events today despite the growth in scale and frequency of attacks. Certainly, the deployment technology has played a critical role, but it would be a mistake to overlook the critical role communication and collaboration across and between interested parties, from ISP to enterprises to governments, has played in securing Internet infrastructure.

11. Network Security is a fluid topic, where new threats and vulnerabilities are always emerging. In the past 20 years significant efforts has gone into researching threats and solutions to these issues. Additionally, the past decade has seen an emphasis on global cooperation of operations and research groups, across geographic and

competitive boundaries, to ensure a stable and working Internet. Multiple groups now exist for people to work together to the common goal of a healthy network. The protocols that compose the Internet are flexible and resilient, enabling changes and updates to address newly emerging threats.

12. In spite of this resiliency, the Internet is vulnerable at many key points to malicious attack at multiple layers. Arbor has been tracking the growth and increasing sophistication of DDoS attacks for nearly a decade. We monitor literally thousands of attacks per day. In addition to frequency, the size of DDoS attacks has increased exponentially, reaching a sustained size of 49 gigabits per second (49Gbps) in 2009. To put that in perspective, the largest backbone connections that form the Internet core are 40 Gbps. In addition to a notable increase in the number and size of attacks against network infrastructure, Arbor has observed a troubling increase in the number of smaller and more sophisticated attacks—including service-level and application-targeted attacks, DNS poisoning, and route hijacking—are more difficult to manage than larger, brute force attacks and can cause a serious disruption in network service or enable further compromise.

13. For example, in early 2008, a US researcher, Dan Kaminsky, discovered a flaw in how the majority of the world's DNS servers communicate that could allow an attacker to silently alter address mappings for their own gain. In 2007 a routing incident with a Pakistani ISP caused several hours of disruption to the popular video website YouTube; the flaws that allowed this attack still persist to this day with no suitable fixes available. Earlier this autumn, researchers disclosed a flaw in the design of the key protocols to securely communicate with websites, secure sockets layer (SSL), which can allow a malicious party to eavesdrop on a conversation when both parties expect secrecy. These flaws, and more, increasingly demand broad Internet cooperation by vendors to fix and users to deploy with minimum disruption and risk.

14. In the past decade we have witnessed the growth of broadband connected PCs and bandwidth available to the consumer. That same bandwidth is also available to cyber criminals and hackers. In short, attackers have better tools and faster PCs from which to launch their attacks, fueling this problem. ISPs, on the other hand, must securely deliver new and innovative broadband services to more consumers at better prices, all the while upgrading infrastructure equipment.

15. This rise of botnets over the past 10 years has become a multi-national, multi-million euro financial burden, as well. What started from virtually nothing has become a maturing black market economy that threatens the credibility of the Internet as a finance and commerce network. For the consumer with a compromised PC, identity theft and financial fraud are a direct impact. For the businesses and banks they do business with, the impact of these crimes has been growing at an alarming rate. Security companies and ISPs struggle with ownership of the problem and solutions to put an end to these attacks.

16. Also in this timeframe, cyberspace has become a battle space for politically motivated attacks. As newspapers, political parties and groups, dissident groups and governments use the Internet to organize and communicate, it has become a natural target for attackers who wish to silence their opponents. Some of these botnets are operated by criminal gangs while others are operated by purely nationalist attackers. The Internet's protocols and structure is very open, allowing for significantly improved human communications and economic growth, while at the same time enabling these sorts of attacks.

17. Attacks such as those in Estonia (2007) and Georgia (2008) are far from isolated. Indeed, in the past two years such attacks have spread from a few places, such as the former Soviet Union, to many countries around the world. Just this past summer, three British political parties' websites were attacked on the eve of the election, including the British National Party, and also the Conservatives and Liberal Democrats. In the US presidential primaries one of the candidate's websites was attacked by a botnet, and this summer suffered several days' worth of cyberattacks on multiple government and commercial sites. It has become clear that every Internet-connected nation should consider themselves a target at some point in the near future.

18. However, a key differentiator between Estonia, Georgia and much of Western Europe is the Internet presence in the country's backbones. Estonia and Georgia had limited bandwidth to the outside world, far less than the UK, France or Germany, and far fewer connections to the outside world. Furthermore, their ISPs have fewer staffers experienced in large-scale cyber attacks than those in Western European countries.

19. European networks span a wide range of bandwidths, connectedness to the rest of the world and technical resources. Some, faced with an attack such as those that struck at Estonia, Georgia or the US, could handle these attacks quickly with minimal disruptions. Others are likely to struggle to address these attacks, leading to disruptions for the government sites in question, or even, key elements of the national infrastructure. However, with significant resources that are available to many hackers on the Internet, even the largest of Internet presences can be disrupted by coordinated attacks.

20. SOLUTIONS

21. The technology to address these attacks clearly exists in the marketplace and is proven to be effective at mitigating these attacks, but its deployment is not uniform and is largely limited by budget concerns. Training in network defense and cooperative forums to collaborate during such incidents are also available as needed, limited by knowledge of such resources and the proper contacts to become a member. With this in mind, the EC's potential role is to facilitate the deployment of these solutions through grants, targeted initiatives, and a pollination of working efforts. The Internet has become a key medium for national commerce and communications, its protection is therefore a national and EU-wide interest.

22. To address the threats posed by Internet attackers, there must be a mix of technology deployments, information sharing, training of individuals in how to use such technology and response coordination. As we have seen with the Conficker Working Group (CWG) in 2009, technology alone is insufficient to address a major threat. The CWG demonstrated that fierce competitors and broad, cross-industry groups such as ICANN, anti-virus companies, researchers, ISPs, Arbor Networks and policy makers can come together and collaborate to address a threat. The group's efforts have been successful and have essentially locked out the Conficker author, but global remediation of the threat remains elusive.

23. An example of an effective national network defense model comes from Korea. The Korean Information Security Agency (KISA) mandated to ISPs in South Korea that they must be able to stop DDoS attacks and share information between each other and with the government to coordinate such defenses. Specific goals and requirements were laid out, along with a timeline, technology recommendations, and some initial funding, but the technology specifics were left to each provider. This model can be replicated within the EU, and should include international information sharing and cooperation to address these threats.

24. Direct military involvement in running civilian networks during an attack is likely to be counterproductive. Internet operations are so complex and unique to each provider that any outsider is likely to make matters worse without proper acclimation. Instead, assistance should be offered as needed to reach clearly stated goals and requirements, with government or military facilitation of achieving those goals in a timely fashion a key strategy.

25. So many parties, including researchers and industry leaders, are addressing these problems from all angles that forums to work together must be strengthened or created. Domestic and international coordination of parties defending networks requires technical assistance, secure communications channels and project management. One of the primary organizations to coordinate Internet security efforts includes CERT teams (Computer Emergency Response Teams) for government, the civilian sector and private industry. Several countries, including the UK, Germany, and the Netherlands, use the multiple-CERT model, including CERT teams focused on government constituencies and the civilian sector that cooperate closely with domestic CERT teams operated by ISPs or large enterprises. Arbor believes this is an effective model and one that should be considered across the EU, with the goal of every country having an established, effective CERT for the government and private sectors by the end of 2010.

26. Models of an effective public-private collaboration exist already in EU member states. CERT teams can provide that interface between government efforts and the private sector. Examples include CERT-FI staff in Finland, who have members dedicated as liaisons to the information security community, and the Dutch GovCERT-NL staff who have members with duties to gather information from the public sector and to provide some information back. These teams provide the security operations community effective bridges to national law enforcement, domestic ISPs, and their counterparts in other countries. Open, fair communications between dedicated professionals has proven effective at addressing large-scale Internet issues. This model must be replicated at other teams within the EU.

27. None of the Internet's problems respect national boundaries. Because of this, any EC cybersecurity policy must include international coordination bodies to share information in a timely fashion in an EU-specific forum such as EISAS as well as FIRST, a global forum for CERT organizations. Such teams need to be allowed to freely communicate with their peers in foreign countries. At present, barriers exist between allies that prevent information sharing at the pace that is needed, on the order of minutes and not weeks. Political agreements need to be reached and a framework established to facilitate this kind of cross-border cooperation. Without this cooperation, these bodies are largely ineffective.

28. Research groups such as ENISA have a role to play in studying attacks and developing countermeasures. Early warning systems have historically been an effective tool at understanding the Internet's operational threat state. ENISA's efforts are building large-scale monitoring systems such as WOMBAT should be nurtured and broadened to meet the complexity of Internet threats. ENISA's effectiveness so far is modest. To be more effective it needs to be more aggressive and nimble and be willing to assert itself. ENISA's purpose must continue to be operational support of the EU constituency with data and its research.

29. Because the technology to address large-scale cyberattacks exists and is proven in real-world deployments, it is not unreasonable for the EU to proscribe that member nations have the capacity to ensure highly available networks by the end of 2010. As discussed earlier, attacks continue to grow in scale and will soon affect every country. The time to act is now. This is an aggressive timetable and will require the EC to draw upon examples in the EU, such as CERT Polska in Poland, GovCERT-NL in The Hague, and FICORA's CERT-FI in Helsinki, all of whom are recognized as global leaders in CERT excellence. The EC needs to clarify or rectify network monitoring for defensive purposes with its communications regulations. Once that is achieved, ISPs must share industry best practices and adopt them, perhaps with financial and educational assistance of the EC, aggressively.

30. Because the technology to address large-scale cyberattacks exists and is proven in real-world deployments, it is not unreasonable for the EU to proscribe that member nations have the capacity to ensure highly available networks by the end of 2010. As discussed earlier, attacks continue to grow in scale and will soon affect every country. The time to act is now. This is an aggressive timetable and will require the EC to draw upon examples in the EU, such as CERT-PL in Poland, GovCERT-NL in The Hague, and FICORA's Finnish CERT in Helsinki, all of whom are recognized as global leaders in CERT excellence. The EC needs to clarify or rectify network monitoring for defensive purposes with its communications regulations. Once that is achieved, ISPs must share industry best practices and adopt them, perhaps with financial and educational assistance of the EC, aggressively.

31. Based on our experience at Arbor Networks working with ISPs, governments, and others around the world, we find that while we have the technology to combat these attacks, this alone is insufficient to meet these challenges. It is clear that nearly everyone recognizes that addressing the threat of cyberattacks requires a broad coalition. We have working models within the EU and around the world on which to build, and demonstrated interest in service providers and many others who want to cooperate to address these pressing issues.

13 November 2009

Memorandum by Professor Juliet Lodge

1. The threat of large scale cyber attack has been recognized and addressed in deliberations by the EU and member governments with recommendations for the establishment of both national cyber tsars, and possibly a dedicated cyber court. In view of ambient intelligence, the internet of things, ubiquitous computing and states' and citizens' increasing reliance on computers and robots powered by batteries or the grid, and the attendant risks of widescale impact by denial of service attacks as well as destruction or interference with critical infrastructures, many issues need to be urgently addressed.

2. There is a risk of separating the large scale cyber attack scenario from the realities of what could/should be done to better protect systems ab initio. This requires action by governments to require the private and public sectors, both separately and in any partnership arrangements (including those involving outsourcing to third parties here and abroad) to invest in proactive, preventative system security.

3. Privacy enhancing technologies, and baking security requirements into system architectures are essential. But more is required to build trust in the security and trust in the associated methods of governance and auditing among and for stakeholders, industry, governments and citizens. This means that the providers of the systems and associated software should be required to consider the security implications and means to protect security and privacy as a first principle. This should be a life-time requirement for continuously revisiting and proofing the systems, software and applications throughout, from the initial stages of conceiving to selling and updating.

4. Quality criteria should be established to ensure the respect for and operation of systems that are as cyberattack resilient as possible at all levels.

5. The need to respect people's privacy should be an operational principle baked into the technology. It should be a requirement for all those involved in internet governance.

6. The potential risk of not adhering to such principles for the sustainability of trust in government itself should be examined along with the means for ensuring effective, democratic accountability in ambient intelligent environments and applications that will probably be invisible to citizens.

7. Government should be prepared for, and should prepare citizens for, the "internet of things". It should not draft regulations for the net as it is now but project future needs and dangers, opportunities and challenges. It should not rely on industry and ICT vendors to sell it systems and applications that are available today but should insist, for all public policy purposes, and all applications using information of individuals, that principles of purpose limitation, data minimization, data subject consent and control are enabled by the

technology. Trusted ICT kitemarks have their place but political leadership and legal regulation are also required immediately. It is unrealistic to suppose that citizens can understand or have the means to pursue or rely on legal remedies for negligence or liability.

8. There is a need to identify the modalities of operation, build trust in the ICTs as well as trust in the means by which data is collected, stored, transmitted and handled.

9. There is a need to revisit the technical tools of trust (such as hard and soft biometrics) which are easily presented to stakeholders and citizens as tools to guarantee their identity, security and privacy and therefore justify them trusting the ICTs and the way in which they are used by public and private sectors, and trusting their "governance".

10. The future of the internet in the context of ambient intelligence, nano-robots and RFIDS offers therapeutic opportunities for society. Dependence on them is also potentially risky in the event of cyber attacks at the smallest most personal level (as on today's PCs and phones) or at local, regional or state levels.

11. The most vulnerable in society might benefit the most from such technologies if there are sufficient resources to provide them with them. Equally, if access to them depends on financial wherewithal, they could be at risk themselves from not being able to access or use those technologies. Certain sectors of society could be doubly disadvantaged, dependent on human interaction but unable to access, in the event of cyber attacks, able citizens whose working mode has been disabled by the attack. What backup and practices need to be developed?

12. What are the implications of a convergence between the real world and the virtual world where some reliance is placed on humanoid robots for a variety of therapeutic or security purposes?

13. There is a need to focus on human security and not just homeland security if the EU and its component states are to be able to respond effectively. What might be a realistic role for citizens to help in preventing, predicting, responding to and combating such cyber risks?

14. Other questions that need to be addressed concern: the requirements placed on industry regarding what it develops (sometimes with public money), what it sells to citizens, and what it outsources? Should outsourcing itself be regulated in the light of foreseeable threats and risks? How is human dignity and privacy to be secured and protected in the e-health, e-education, e-commerce, e-leisure and e-citizen arenas?

15. There is a need to be vigilant of creeping steps to privatise accountability, to put data subjects—including minors—in the position of being responsible for data they handle in an environment that will be increasingly wire-free, populated by ubiquitous sensors, reliant on machine-to-machine interaction without human mediation, and where the lure of convenience presented by ambient intelligent environments could be manipulated for ill and/or in arbitrary and discriminatory ways.

13 November 2009

Memorandum by Ofcom

1.1. We welcome the opportunity to provide evidence to the House of Lords' Select Committee inquiry into EU policy on protecting Europe from large-scale cyber attacks.

Ofcom's role and duties

1.2. Ofcom is the regulator and competition authority for the UK's converged communications industry, with responsibilities covering television, radio, telecommunications and the management of the radio spectrum. Ofcom's primary statutory duty is to further the interests of citizens and consumers in communications matters, where appropriate by promoting competition, as set-out in the Communications Act 2003, Section 3(1). Section 4(j) of the Act[92] requires that, in pursuit of its duties, Ofcom should have regard to the desirability of preventing crime and disorder. Ofcom's regulatory principles, which guide our day-to-day work, require Ofcom to research markets constantly, and to remain at the forefront of understanding technology developments that drive the communications industry that Ofcom regulates.

1.3 From Ofcom's own research into the development of the UK communications market,[93] we know that communications services, increasingly conveyed over the Internet, are becoming an essential part of the daily lives of many UK citizens and consumers: for example, nearly two-thirds (65%) of UK households had a fixed-line broadband connection in Q1 2009, and UK consumers are now (May 2009) spending an average of 25 minutes per day using the Internet. By Q1 2009, more than eight million people in the UK (16% of adults)

[92] Communications Act 2003
[93] Ofcom: The Communications Market Research Report, 6 August 2009

had at some point used their mobile phone to access the Internet (up by 42% on last year), and more consumers (46%, up 7% on last year) are now buying communications services in "bundles" (fixed/mobile phone, fixed/mobile broadband, and/or TV). Communications industry revenues in 2008 were ~£52 billion.

1.4 Allied with this heightened awareness of the importance of communications, are growing concerns about the underlying communications networks infrastructure in terms of their coverage (in population and geographic terms), the availability and quality of the services delivered over them, and the resilience of the infrastructure to a wide range of commercial and/or technical failures in general, and specifically in relation to the vulnerabilities of networks infrastructure to large-scale cyber attacks.

UK Developments in Cyber Security

1.5 While the responsibility for protecting UK networks against cyber attacks is shared between Government, various Government agencies, and private sector network operators, Ofcom, as the economic regulator and competition authority for the UK's communications sector, has been playing a full part in recent developments, culminating in the publication of a number of influential reports over the summer of 2009:

1.6 In June 2009, the Government published an update to the National Security Strategy of the UK (*Security for the Next Generation*),[94] first published in 2008. This update reflects changes to threats around the world, and puts much greater emphasis on communications and cyber security. Alongside the update, the Government published the first-ever UK Cyber Security Strategy (*Safety, Security and Resilience in Cyber Space*),[95] creating a UK Office of Cyber Security (OCS) in the Cabinet Office, and a multi-agency UK Cyber Security Operations Centre (CSOC) at Cheltenham. As they become established, we would expect OCS to lead on the national policy response to the threat of cyber attacks, while CSOC will lead on the real time national response to large-scale cyber attacks.

1.7 The Council for Science and Technology (CST), the UK Prime Minister's top-level advisory board on science and technology policy issues, also published a report in June 2009 on "A National Infrastructure for the 21st Century".[96] The CST report focused on the inter-connectedness between the four main sectors of the national infrastructure[97] (ICT (ie communications), energy, transport and water), and the dependence of the other sectors on communications. It also highlighted the highly fragmented delivery and governance structure of the national infrastructure, its weakening resilience through a combination of ageing components, the infrastructure nearing its capacity, and greater complexity, and pointed to the significant challenges posed by climate change.[98] The CST's main recommendation was for the Government to appoint a lead body to deliver a clear and consistent vision for the future of the national infrastructure. The Government has responded by announcing (in *Building Britain's Future*[99]) the setting-up of Infrastructure UK.

1.8 The Institute for Public Policy Research (IPPR) also published a report in June 2009 of an all-party commission (led by Lord (George) Robertson and Lord (Paddy) Ashdown) on its national security strategy for the UK. The report is a comprehensive study into all aspects of the UK's national security strategy, taking two years to complete, and producing 108 recommendations. The main thrusts of the report were the need to:

- think strategically, prepare for the worst, and to ruthlessly target resources
- co-ordinate Government efforts on security (including the idea of a single security (cf defence) budget)
- push power and responsibility for security up to multilateral institutions (particularly in Europe, as part of a more equal NATO relationship between Europe and the US)
- promote resilience of national infrastructure, and devolving resilience down and out from central Government to local governments, businesses, communities and citizens
- ensure legitimacy (operating with the rule of law at home, and consistently with human rights and international law abroad).

1.9 Of particular relevance for Ofcom in this context, the Digital Britain report,[100] also published in June 2009, proposed a number of extensions to Ofcom's current duties in the areas of network investment and network infrastructure reporting. On network investment, the Government is proposing that Ofcom should have an

[94] Cabinet Office: The National Security Strategy of the United Kingdom: Update 2009 – Security for the Next Generation, June 2009
[95] Cabinet Office: Cyber Security Strategy of the United Kingdom – Safety, Security and Resilience in Cyber Space, June 2009
[96] Council for Science and Technology: A National Infrastructure for the 21st Century, June 2009
[97] The four key infrastructure sectors of the UK critical national infrastructure (CNI) are: communications, energy, transport and water, which are referred to as the network infrastructures. The other five sectors of the UK's CNI are: finance, food, government and public services, and health and emergency services, which are referred to as the social and economic infrastructures.
[98] The Government's Department for Environment, Food and Rural Affairs (DEFRA) also published a consultation in June 2009 on the use of the Adaptation Reporting Power in the Climate Change Act 2008, including on how the power should be applied to the electronic communications sector
[99] HM Government: Building Britain's Future, June 2009
[100] HM Government: Digital Britain, June 2009

explicit general duty to encourage investment as a means of furthering the interests of consumers, alongside its duty to promote competition where appropriate. Digital Britain also recommended that Ofcom be given a duty to alert the Government to any significant deficiencies in the coverage, capability and resilience of the UK's communications infrastructure and to report every two years on the state of that infrastructure. We expect these recommendations to be given effect in the forthcoming Digital Economy Bill (expected to be published in November 2009).

1.10 Ofcom has also been working closely with Government (the Department for Business, Innovation and Skills) and communications providers (CPs) to establish a set of minimum security standards (based on International Standards ISO 27002/11 on Security Management Systems, and their application to Telecommunications) for interconnection between CPs in shared access facilities (eg Local Loop Unbundling (LLU) operators in BT exchanges) to mitigate the risks of any security weaknesses of one operator impacting the ability of other interconnected operators to provide secure services. The adoption of these minimum security standards will establish a baseline of protection to help to mitigate risks from cyber attacks.

International Dimension

1.11 However, as the Internet is a global phenomenon and cyber security is an international risk, it is essential that the policy response to the threat from large-scale cyber attacks has a strong international dimension.

1.12 Within Europe, while matters of national security are reserved for Member States, there is clearly a significant opportunity for, and potential major advantages in, the sharing of information and best practice among Member States on network resilience and building-in to the design and implementation of networks measures to protect against cyber attacks, as well as in the co-ordination of the rapid real-time response to cyber attacks occurring on an international scale.

1.13 We welcome the recent statements from the European Commissioner for the Information Society, Viviane Reding, which have raised the profile of the issue of cyber security across Europe and started a debate about how the EU should respond.

1.14 Given the increasing threat of large-scale cyber attacks, we believe it to be appropriate to review the arrangements currently in place across Europe for information sharing and co-ordination on network security issues (including the role of the European Network and Information Security Exchange (ENISA)).

1.15 We are of the view that there could be some merit in establishing the role of an EU Cyber Security Tzar to act as a catalyst to review present arrangements and to foster co-operation on cyber security among the Commission and Member States.

12 November 2009

Memorandum by Payments Council

The Payments Council is pleased to provide evidence to the Select Committee to aid its inquiry into this critical area. The Payments Council is the organisation that sets strategy for UK payments. It has been established to ensure that UK payment systems and services meet the needs of users, payment service providers and the wider economy. A complete list of our members may be seen in the Annex at the rear of this document.

One of our core objectives is to ensure the operational efficiency, effectiveness and integrity of payment services in the UK. This has led us to taking on a central industry role with respect to gaining a deep understanding of threats to payment services and to developing tactical and strategic responses to these threats.

Further information about the Payments Council may be found on our web site: www.paymentscouncil.org.uk

1. Importance of the Internet to Payment Systems

The provision of payment services has become increasingly reliant upon the internet and on internet technologies.

Financial institutions, payment service providers, payment processors and others engaged in this space have all sought to leverage the advantages of internet technologies to increase efficiency, reduce cost and to deliver enhanced services to customers who are increasingly demanding integration with the internet. This trend is almost certain to continue, with older proprietary interfaces increasingly being replaced by ones using internet technologies.

It is important to point out that while inter-bank payment systems, services and schemes such as Bacs, CHAPS, Faster Payments (these three being the predominant automated payment schemes in the UK), credit & debit cards, cheque payments, ATMs and so on are increasingly using internet technologies, they mainly do so using closed networks that are insulated from the wider internet. This makes them much less vulnerable to attacks than the wider internet infrastructure. The Payments Council and its members take the security of payment services very seriously, and take proactive measures to protect customers and systems to a very high level of effectiveness. We are not aware of any instances of the UK's core payment systems having being breached in any significant manner due to internet hacking attempts.

Where payment services become customer-facing—for example logging into internet banking services—they are potentially at risk from attack .Even here though it is important to put the scale of the threat in context. For example over 22 million people now bank online in the UK, but the number of bank accounts that have been compromised due to attacks such as phishing and malware is a tiny fraction of one percent of the total, and losses to the banking industry through online banking fraud are likewise a small fraction of other fraud losses such as credit card fraud. Another industry body, Financial Fraud Action UK (and its predecessor APACS) has been instrumental in co-ordinating the industry's efforts to understand and combat all forms of payment fraud. This includes introducing measures to harden payment systems and services against fraud, such as rolling out Chip & PIN and developing an interoperable standard for two-factor authentication for online banking.

1.1 *The Committee's questions*

Given our role, we will be responding to the Committee's questions from our own specific point of view as appropriate, and we have not attempted to answer all the questions posed as we expect that others will be better placed to respond.

Threat Analysis

Q. *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

A. Those organisations currently responsible for ensuring the resilience of the internet are working hard to keep it that way. It can be argued however that they are each limited to specific aspects of the internet that fall within their remit, and in many cases there is relatively little in the way of effective co-ordination between them. That there is no body with an over-arching role of ensuring integrity has been seen by many as a negative factor, but we would view a centralised regulation-based structure as being overly cumbersome given the complexity and scale of the internet.

The internet is not a fixed or stable medium—it evolves quickly, in patchwork form and across multiple jurisdictions. This necessitates a highly flexible and dynamic approach to ensuring stability and security, and argues against regulatory intervention that results in a more inflexible approach. Regulatory intervention at local level, including EU level, is also unlikely to be sufficiently broad in scope to address any fundamental issues as these are highly likely to apply at global levels.

Recent efforts by the Internet Corporation for Assigned Names and Numbers (ICANN) and others to enhance the integrity of the Domain Name System (DNS) are a positive example of what can be achieved by taking a focused self-regulatory approach. ICANN is taking seriously the lessons of previous attacks on—and failures of—DNS to ensure that the proposed new Top Level Domains will be introduced based on secure principles and practices, with a view to eventually extending these practices to the rest of the DNS. This is beginning to have an impact at more local levels—for example in the UK Nominet are to sign the root for the UK domain early in 2010.

There are a number of areas where performance can be improved. Internet Service Providers (ISPs) should be able to undertake more effective traffic monitoring to identify, for example, customer computers that are compromised with malware and to prevent them from infecting other machines or causing actual harm to the infected customer by providing alerts and advice. In practice few ISPs choose this path for reasons that include concern over the possible erosion of their "mere conduit" status, operational cost and fear that customers may react negatively to well-intentioned actions. The broader regulatory and business environment within which ISPs work can therefore be said to be having a negative impact on their ability and willingness to be more proactive, and in such circumstances there may be justification for action to be taken at national and EU level to provide legal clarity and a well-understood level playing field.

Q. *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

A. The nature of the specific attacks mentioned remains controversial, and we need to be clear that one must keep an open mind about the nature of past nationally directed cyber-attacks. The difficulty is one of attribution of attacks to certain actors, and intent from both public and covert sources; it is likely that most of these attacks, but not all, are caused by independent "concerned" citizens with access to tools such as botnets. Whatever the ultimate truth, they do demonstrate that the potential capability to affect a nation's internet-based services exists and that it is technically possible for future conflicts and wars to include disruptive attacks against Internet infrastructure. Another side effect of the attacks is that it clearly demonstrates that nations heavily reliant upon the internet for service delivery, such as Estonia, are that much more vulnerable to wide-ranging disruption.

Payment systems are one possible target of a nationally directed attack. It is relatively simple to understand the likely motivations for such an attack, including a desire to disrupt normal economic activity either in a nation as a whole or through focused attempts to harm the finances of certain organisations. To date however we have not seen any examples of such behaviour, beyond limited examples of criminally-motivated denial of service type attacks which do not affect underlying payment systems and are relatively simple to recover from.

Q. *The events in Estonia led to a more public involvement by NATO in cyber protection issues. Should the military be more involved in protecting the Internet?*

A. We do not believe that military involvement is an appropriate way to mitigate problems largely affecting the civil and private sectors. The vast majority of malicious behaviour on the internet is as a result of criminal activity and should be dealt with through properly constituted and resourced law enforcement, and ably supported by national Computer Emergency Response Teams (CERTs) acting with a "common good" remit.

Q. *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

A. Botnets are the weapon of choice for internet criminals, particularly organised crime syndicates. The payments industry has been one of the main targets of botnet-aided crime for a number of years we have gained much experience in combating botnets and their creators. We consider them to be a significant threat in that they facilitate fraud, identity theft and other crimes.

It is almost depressingly easy for a criminally-minded individual of even limited technical knowledge to create, maintain and exploit botnets, as many are now sold on underground markets in kit form complete with support arrangements. These kits enable botnet operators to easily configure them to carry out various tasks in real-time. Botnets often enter the public consciousness by virtue of their size, for example the Conficker worm is estimated to have compromised several million computers worldwide. However, in our experience smaller botnets can be even more damaging as they tend to draw less attention despite the fact that they are just as sophisticated.

Against payments targets, botnets tend to be used in a number of ways including:

- Hosting phishing sites, including fast-flux
- Transmitting phishing spam
- Stealing data from infected computers
- Handling data stolen from other computers
- Acting as proxies to enable criminals to access secure services while disguising their true locations
- Attempting further infections of other computers (for example via using so-called "drive by" infection techniques)
- Facilitating distributed denial of service attacks.

The payments industry, including the Payments Council and its members, take active steps to combat the risk from botnets, including providing evidence to law enforcement, ISPs and others to identify and shut down botnet command and control systems; and to identify and track down the perpetrators.

As botnets tend to be global in nature, action against botnets tends to occur at a global level through strong co-operative efforts, such as the Conficker Working Group that was set up specifically to deal with the Conficker worm outbreak. Nevertheless there is a good case for taking stronger action at national and EU level to make our local environment as safe and secure as possible. This is particularly important with respect to computers that are targeted because they belong to customers who are located in regions where particular

financial institutions operate. For example malware such as Zeus (aka Z-bot) is designed to target customers of financial institutions. In these circumstances it is likely that action at national level would be most effective. However there is also a strong case for countries demonstrating "best practice" approaches to be used as models by the rest of the EU.

We also need to maintain a balanced and objective view of the nature of the threat. The Centre for the Protection of National Infrastructure's (CPNI) assessments currently regard the threat of cyber attacks intended to disrupt or harm from nations or terrorist groups as being low. The threat from criminal groups is much greater and is largely aided and abetted by botnets.

International Responses

Q. *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies? The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

A. Many aspects of the payments industry are highly multinational in nature and benefit from a unified approach, particularly in providing secure payment infrastructures that extend across borders (eg the Single European Payment Area —SEPA). The provision of retail payment services however remains highly localised, and national level approaches become more important. It is important to note that although payment services may appear on the surface to be fairly generic, in reality the manner in which they are delivered differs widely from country to country, increasing the need for country-level response strategies. Further layers of pan-European organisations are unlikely to add much more value.

The Payments Council and its members engage in a wide range of partnerships on national, EU and global levels with respect to cyber security. We engage with our peers across Europe and elsewhere, and also with other relevant parties including law enforcement, academic researchers and information security organisations. Our strategy is to engage at a global level wherever possible, so the case for specific EU-level initiatives would be seen as potentially limited in scope.

Q. *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

A. We regard CPNI's work in this field as being a good example of what can be achieved at a focused national level. Establishing the close contacts needed for effective information sharing and planning is not a simple matter and requires a great deal of trust and understanding on all sides, a state of affairs which is easier to achieve at national level. CPNI for example operates the FSIE (Financial Services Information Exchange) in partnership with financial institutions and ourselves, which has provide to be an effective tool in the fight against threats to the financial sector. A pan-European approach may broaden the extent of available data and lead to a more widespread common approach, but in practice will be much more difficult to achieve to the depth and breadth required. A case-by-case approach is required—payments are already catered for by the G10 oversight of SWIFT.

Q. *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

A. Government CERTs such as CPNI are valuable as they provide the structures to bring sensitive intelligence and advice to CNI sectors and participants. They are not the only type of CERT needed however and it is important that national-level CERTs do not just restrict themselves to addressing issues directly affecting national security to the exclusion of dealing with the private sector.

What is desperately needed are so-called "common good" CERTs that have close ties to governments and national security infrastructures, but which also interact with the private sector and law enforcement. For example the payments industry in the UK has established excellent relationships with CERTs elsewhere in the world, particularly in Australia and the US (AusCERT and CERT/CC) as they are prepared to engage with banks and others to combat online threats against banking and payments. In many senses however this is a highly unsatisfactory situation, as there is no viable equivalent closer to hand in the UK.

Q. *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements? Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

A. We are of the opinion that structures emerge to fit national needs and process. Attempting to retrofit a boilerplate universal model is likely to create more problems than it solves. In our opinion it is vital that cyber crime strategy at the highest level is formulated with a global view in mind. A pan-European approach may add value, but run the risk of adding unnecessary layers of complication and replication of effort.

ENISA

Q. *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work? Is ENISA being effective in its role, or does it need reform?*

A. We are highly supportive of ENISA and believe that it has the potential to be a powerful force for good in promoting the development of CERTs in Europe, but it can be awkward in its execution. Its potential appears to be limited by two factors:

— Its place within the pillar structures appears to be hampering its scope for action, although the Lisbon Treaty may improve matters.

— Geographically, ENISA is not conveniently placed. Even in the internet world personal contacts are important, particularly in the security field. Its location is also likely to affect its access to the resources and skills that it requires in order to be effective.

We recommend that ENISA be provided with the wider mandate it needs to be effective, and that consideration be given to reviewing whether its current location is a help or hindrance to its future success.

Timescales

Q. *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

A. We appreciate the desire for a speedy response, but this is an enduring problem that will require a well thought-through strategic response and it will therefore not be feasible to implement this by the end of 2010. Existing structures have taken many years to evolve and become effective following a process of trial and effort and numerous false starts. We recommend that the Commission takes this opportunity to adopt a more flexible approach that takes a longer term view, and that builds on existing successes rather than attempt to create too much that is new.

Annex

PAYMENTS COUNCIL MEMBERS

Full members:

— Abbey
— American Express Services Europe
— Bank Machine Ltd
— Bank of America
— Bank of England
— Bank of Ireland
— The Bank of New York Mellon
— Bank of Scotland (The Governor and Company of)
— Bank of Tokyo-Mitsubishi UFJ
— Barclays Bank
— Cardpoint Services
— Citibank
— Clydesdale Bank
— Co-operative Bank

— Danske Bank
— Deutsche Bank
— HSBC
— JPMorgan Chase Bank
— Lloyds TSB Bank
— Nationwide Building Society
— Northern Rock
— PayPal (Europe)
— Post Office Limited
— Royal Bank of Scotland
— Standard Chartered
— Wachovia

10 November 2009

Memorandum by Serious Organised Crime Agency (SOCA)

The Serious Organised Crime Agency is an intelligence-led agency with law enforcement powers and harm reduction responsibilities. Many of the questions posed by the House of Lords Inquiry are outside the SOCA remit and this submission will focus on evidence confined to the areas of SOCA expertise and/or experience.

1. Threat Analysis

1b. *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

Current Government position favours a co-operative regulatory framework between Government and Industry. Industry favours self-regulation rather than Government imposed regulation and sanction.

Criminal legal statute is sufficient to allow law enforcement to effectively challenge Internet based bodies who operate in a way which is not conducive to promoting a trusted Internet space and who provide services to criminal groups. These industry bodies are few in number and generally any abuse of the Internet, in particular the abuse of Domain Name System (DNS) is carried out without the complicit knowledge of Internet Service Providers (ISPs), Backbone providers or Domain Name Registrars.

This legal framework is however, somewhat undermined by legal articles within the European Union, for example Section 19 of the EU e-Commerce Directive. The Directive states that as long as a service provider acting as an ISP did not initiate the transmission, select the receiver, or modify the information in transmission then it is said to be a "mere conduit" . This gives ISPs protection from liability for the content of their traffic. The ISP is therefore under no obligation to monitor its traffic and more importantly, it is not required to act over reported malicious traffic crossing its network even when made aware of the criminal nature of the traffic. Australia, in comparison, has a system where ISPs are required to produce a code of conduct to monitor their traffic and take corrective measures if malicious traffic is detected.

SOCA would invite this Committee to consider that the UK Internet space cannot be viewed as a national issue alone. The internet is a global phenomenon and the concept of national borders, law and accountability do not translate well to a commodity which transcends national borders.

Globally there is a huge disparity between the levels of responsibility shown by Domain Name Registrars, ISPs and other areas of Internet connectivity and functionality. There are some fine examples of best practice which are quoted, for example Public Interest Registry's due diligence and compliance processes. However this best practice is not replicated across industry and this leads to opportunities for criminal groups and other bad actors to exploit the lack of audit and compliance within many industry groups. This lack of due diligence is mainly due to market forces and competition, although SOCA has seen examples of criminal enterprise using the lack of checks and balances to establish themselves both as criminal domain registrars, for example ESTDOMAINS in Estonia and criminal ISPs, for example the Russian Business Network.

Criminal abuse of the Domain Name System is at the root of all the current major criminal attack systems including the Rockphish and Torpig Malware versions and the Avalanche Botnets, which according to the Anti-Phishing Working Group Annual Report 2009, are believed to be responsible for 24% of global phishing attacks. All these attack vectors purchase domain names in bulk from either legitimate or criminal domain registrars. These domain names are used to host the attacks and are rotated every few minutes to frustrate law

enforcement and industry efforts to take them down by utilising Fastflux methodology. Enhanced global due diligence in the sale and management of Domain Names and swift removal of criminally registered domains would have a significant impact on this type of crime.

SOCA is working closely with a cross section of the global law enforcement community to lobby and effect change within ICANN (Internet Corporation for Assisted Names and Numbers) to enable a self regulatory system, run by ICANN, which would incorporate best practice models into a mandatory regulatory framework, implemented and administered by the Industry itself.

This type of mandatory global regulation has the capacity to make a significant impact on the capability of criminal groups to use the Internet for a range of criminality. The model could work equally well with Regional Internet Registrars who also have a global remit and range. Between these six bodies (five Regional Internet Registrars and ICANN) a global regulatory system could be implemented swiftly and effectively thereby imposing considerable control over Domain Registrars and Registries and Local Internet Registries and Internet Service Providers.

SOCA would invite this Inquiry to consider the Government's current multi-stakeholder approach to industry to be the correct one and the best model for effective regulation whilst ensuring sustainable economic growth and stability. However, self-regulation by industry is only effective if the provisions of such regulation are applicable to all industry and do not have an opt-out option for any levels. Such regulation is not regulation as such but merely best practice. Criminal groups and bad actors on the Internet will not comply with self-regulation.

There are examples of good practice within the Internet community, a prime example being the model of cooperative working between the sector and the Internet Watch Foundation to prevent access to child abuse sites. This model works well for URLs (although the growth of criminal ISPs in the unregulated sector allows the constant moving of sites within the same ISP) but could be extended to addressing other areas of serious criminality which are developing.

1e. *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

Botnets are networks of compromised computers (bots) that have been infected and are now under the control of one party. These networks sometimes comprise tens of thousands or even millions of machines, all of which await commands from the controller. They are very difficult to trace, particularly where they employ peer-to-peer technology, and offer criminals a widespread and virtually untraceable platform from which to launch attacks or engage in further activity.

They can be used for a variety of purposes including phishing and malicious software (malware) attacks, dissemination of spam, providing proxy services to hide the locations of criminals and to conduct Distributed Denial of Service (DDoS) attacks that bring down systems and websites.

Significant harm is caused by bots both within and outside the UK. Large numbers of UK home users and corporate PCs and servers are infected and form part of these botnets. Criminal activity and attacks against UK users and businesses are often propagated by bots outside the UK, which presents enormous challenges to both law enforcement investigations and industry responses. UK bots are also attractive to criminals targeting the UK, both for committing crime, for example stealing the user's online banking credentials and for facilitating crime, for example providing a UK computer behind which the criminal can hide.

The total extent of compromised bots within the UK is unknown, largely due to the fact that there is no national reporting body or CERT that is compiling this data, but industry reports indicate that the problem is extensive. There is no common standard or requirements setting out what action should be taken by Internet Service Providers (ISPs) in the UK, and there is certainly a disparity between the level of monitoring and response that they provide.

As ISPs control the networks that customers use to connect to the Internet, they are also best placed to monitor the traffic for malicious or criminal activity and to ensure that compromised machines are "cleaned". Globally, and specifically within the EU (Germany) some ISPs have successfully provided "walled garden" services, where they will monitor for infected bots, and then isolate them in quarantined networks with access to Anti-virus and other tools required to clean their systems. They will only allow customers to re-access the Internet when their systems are cleaned up. There are various technical options for monitoring and taking action on botnet activity, but we have seen no evidence of a consistent approach being applied by ISPs in the UK to deal with this problem.

International Responses

2e. *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

The use of the CERT network in dealing with Internet related incidents is very important. The UK has several CERT bodies which address different sectors. In the absence of a national CERT, it is critical that these bodies work together and that their remits are coordinated to ensure that all areas have adequate response and coverage.

The importance of a joined up CERT network will increase in the light of any implementation of either industry-led or Government regulation due to the need for clarity surrounding the level of information required to activate the actions required by any such regulation. This will be crucial in allowing industry to have a trusted single point of contact through which requests and responses can be routed. This is a particular complaint from industry that they are "harassed" by requests from self interested parties seeking take downs and interventions which are not covered by law.

2g. *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

As previously described, the imposition of boundaries within Internet Governance is a difficult if not futile issue. Certainly policy and process can be developed nationally or within a European framework but any regulatory control will be limited by the extent to which the offending infrastructure actually sits within such regulation.

SOCA's projects are globally focussed and engagement with the Council of Europe and the European Commission are important, as there is some conflict between European Law and that of the USA, the latter being where much of the internet infrastructure is based.

EU privacy laws are a prime example of this and mean that the processing of personal information is limited to certain explicit purposes. For example private individuals registering domain names for use on the Internet can have their details hidden. Interpretation of this law within the Internet community is polarised with resellers of US based registries finding difficulties in aligning the open WHOIS policy of their parent registry with EU restrictions. The continued open source nature of the WHOIS is still threatened by EU privacy laws and their interpretation.

The best solution is a global one but any interaction and policy making must be as wide as it can be but with due regard to the implications beyond the jurisdiction in which it is made.

12 November 2009

Memorandum by Mr Tim Stevens

1. My name is Tim Stevens, and I am a doctoral researcher in the Department of War Studies, King's College London. I am also an Associate Fellow of the International Centre for the Study of Radicalisation and Political Violence (ICSR) and an Associate of the Centre for Science and Security Studies (CSSS). I write and consult on a range of issues relating to cyberspace and conflict, although my principal foci are what might be termed "cyber strategy", and organisational responses to "cyber threats".

2. Although there are many issues of great interest and importance under the purview of the Committee, I shall restrict my comments and observations to two issues: the nature of cyber attacks; and the role of the military in protecting the internet.

3. Summary. *On cyber attacks:* the EU should be concerned about cyber attacks in the mould of Estonia and Georgia but should be mindful of the different types and effects of offensive cyber actions. *On military protection of the internet:* given the private ownership of most information infrastructure and the problems of attribution the role of the military in protection should be limited in peacetime. Their principal role should be as a principal facilitator of information sharing, training and rapid response as required. The submission *concludes* by broadly supporting the EU's intentions in these areas.

Cyber Attacks

4. The Committee notes the concern held by the EU about cyber attacks, noting the historical events involving Estonia in Spring 2007 and Georgia in August 2008, and asks whether this concern is justified. The answer is a qualified "yes".

5. The derivation, intent and effect of the Estonia and Georgia events were quite different, but were similarly characterised by one key aspect: vulnerabilities. It is a truism that an "attack" is contingent upon the use of "arms" at some level but its efficacy and effects depend upon the nature of the vulnerabilities inherent in the systems one is attacking. The discourse of "attacks" has served principally to put the onus of responsibility on the aggressive party rather than on those charged with securing networks satisfactorily. One unfortunate by-product of this attitude has been a bias towards viewing all "attacks" as inherently strategic, whereas they are in reality more often operational or tactical. Many, of course, are also automated and unpredictable in their outcomes.

6. This is not to say, however, that there are not serious concerns about the use of offensive cyber capabilities to degrade, disrupt or even destroy the networked functionality of a modern state. We must distinguish between the first-, second-, and third-order effects of such cyber attacks.

7. *Destruction*. The potential destruction of physical assets as the primary aim or outcome of an attack is vastly over-inflated. At present, whilst it is possible to overload network hardware such that they are rendered physically inoperable, it is extremely unlikely under most conditions. Rumours suggest that during the Estonia attacks a single server was "melted", although this is, to my knowledge, unsubstantiated. Whilst I would be cautious in denying this as a possible outcome, I would adjudge it improbable at present or in the short-to mid-term future. The intended first-order effects of cyber attacks are not physical at all: cyber conflicts are, at the pragmatic level, about the "contestability of connectivity",[101] and this is the confrontation they aim to dominate or control. A distributed denial-of-service attack (DDoS), facilitated by a botnet perhaps, aims only to restrict access to a given internet-mediated resource, such that the normal functionality on which people and services are reliant is disrupted. Most "attacks" result in embarrassment or inconvenience, rather than anything more serious, although we should not underestimate the impact these *can* have.

8. *Stasis*. The second-order effects of restricted or disabled network assets can be more serious. In the Estonian example, government communications networks were reduced to radio for a limited period, financial operations were severely compromised, and the ordinary functionality of a highly-networked state degraded for periods of minutes to days. Under such circumstances there are fears that critical national infrastructures (CNI)—energy, security, emergency services, etc—can be rendered inoperable by attacks on the critical information infrastructures (CII) on which they rely. Although many commentators exaggerate these fears there are definitely grounds for concern. Although personally I am very cautious about the use of cataclysmic epithets to describe potential scenarios—"cybergeddon", "digital 9/11", "cyber Katrina", etc—horizon-scanning demands that our response frameworks take account of the worst-cases imaginable. A state's inability to communicate with its own organs and agencies must be of very grave concern.

9. *Demise/breakdown*. The third-order effects are, really, where public concerns are situated; that is, in the impact on society attendant on disruptions to critical infrastructure. Principally, these include the inability to distribute food, energy, water and emergency services in effective and timely fashion. It is notable that in the wake of Hurricane Katrina, even President Bush admitted that the administration had lost situational awareness in New Orleans as a direct result of degraded communications infrastructure. As the Federal Emergency Management Agency (FEMA) struggled even to know where to direct their resources, the media provided mobile intelligence, and it was left to entities such as Wal-Mart to ensure that survivors' basic needs were met. Since 2005, FEMA has reviewed and revised its operations procedures and organisational structure, and the US has more generally elevated "resilience" up the domestic security agenda. Katrina was a natural event however and physical destruction accounted for much of the administration's relative blindness; as stated in paragraph 7 above it is unlikely that a purely cyber attack (ie one not facilitating a kinetic second strike) would have the same effect in physical terms. Mass civilian casualties—including through deprivation of water and food—are unlikely, as are serious breakdowns in social order. We should remember that the oft-deployed historical analogies of 9/11 and Pearl Harbor served more to bolster civil, political and military resolve than they did to degrade it.

10. In summary, the European Union is right to be concerned about the effects of cyber attacks, but should focus its efforts on maintaining the functioning of critical information infrastructures, rather than on too much speculation about what happens when they go wrong. Domestic and inter-state resilience strategies should account for the effects of attacks on CII/CNI, and there may be a need for review of these procedures and safety nets in some member states. The key point is that attacks succeed because of vulnerabilities in the systems they

[101] Richard J Harknett, "Information Warfare and Deterrence", *Parameters*, Vol 26, No 3 (Autumn 1996), pp 93–107.

seek to exploit, not because the attacks are *a priori* so sophisticated or of such scale that they are destined to be effective. Much more could be written about defensive strategies in this context, and I have not addressed the nature of the offensive actors in this space, and I would be happy to provide the Sub-Committee with more information should this be required. To conclude this section, the potential of serious cyber attacks has been demonstrated but a nuanced assessment of the threat environment is required in order to allocate resources and efforts effectively.

Military Involvement in Protection of the Internet

11. The Estonian example led to calls for NATO to use their Article 5 collective military force provision against Russia. Given the problems of attribution, and the still unproven charges against the Russian Federation, it is right that NATO did not respond in this way. However, NATO have been very active in terms of cyber strategy since. In April 2008, they launched their Policy on Cyber-Defense, which allows for extended cyber defence if requested from NATO member states. It does not allow for pre-emptive operations, which may disappoint some, but reflects an understanding that militarised cyberwar is inherently escalatory. Through its Cyber Defence Management Authority (CDMA), established by the Policy, NATO has the authority to respond immediately to cyber attacks on member states, deploy support teams, and holds annual "red team" exercises aimed at engendering co-operation and awareness across the NATO community. NATO evidently hopes that its operations can provide a model of "best practice" that can filter down to national levels.

12. However, there are a host of other questions that arise when asked the question, "should the military be more involved in protecting the Internet?" For the sake of argument, I will assume that 'the Internet' is here intended to refer to CIIs in general. Such questions include, but are not restricted to:

- protection from whom?
- protection of what?
- what are the thresholds for response?
- what responses are legitimate? and legal?
- is a militarised cyberspace, in whole or in part, desirable or justifiable?
- which military?
- which command-and-control structures?

I will address briefly some of these in turn, and submit that each might be more effectively dealt with through further discussions.

13. Protection from whom? Cyber attacks derive broadly from four sources, all of whom are currently human: states, criminals, hackers, and ideologically/religiously motivated groups of individuals. The last three categories are considered non-state actors for the purposes of international law, and must be considered as qualitatively different from states. It follows that responses to actions by each of these four types must be tailored to their source. Unfortunately, definitive attribution of known attacks to specific actors can be extremely difficult. This presents a major challenge to the ability of states and their security services to react swiftly in the event of a critical incident. In July 2009, DDoS attacks against US and South Korean websites affected commercial and information services in those two countries. As they occurred so soon after North Korea's test-firing of missiles assumed to be nuclear-capable, many observers assumed that North Korea (DPRK) was inevitably the source, particularly as the attacks seemed designed to coincide with US Independence Day. Shortly thereafter, some US administrators called for retaliatory attacks against DPRK, much as some did for counter-strikes against Russia after Estonia 2007. The actual source of these attacks has yet to be discerned; South Korea continues to blame DPRK, although most analysts suggest that the attacks came from elsewhere. One wonders at the effects a US military cyber response might have had on DPRK. They could have been crippling, or they could have had little effect on a country less wired than most. Either way, the response would have been wrong. On the other hand, had the attacks been attributed to a non-state actor, what then would have been the response of the US administration? As criminal acts, law enforcement agencies should surely have taken charge. Or if terrorists such as an al-Qaeda affiliate had been held responsible would this have been the green light for a combined counterterrorism operation, probably including multiple intelligence and military agencies? We do not know but it does suggest that knowing who is actually responsible for attacks is a prerequisite for determining responses. Critics of this view state that since we only have milliseconds to respond it does not really matter who does so; as the most potent "cyber force", the military is therefore often charged with responsibility in this area. Leaving aside the fact that many data breaches, systems disruptions, etc, are often "inside jobs", the attack vectors utilised by all actors are essentially the same: they exploit the same vulnerabilities with the same technologies and the same effects. The

converse is not true: reactions can have unexpected and unwanted effects, not least of which is a tacit declaration of hostilities against the wrong party. This is at the root of the inherent escalatory nature of cyber conflict and we need to be sure against whom we are protecting our networks before we endow militaries with responsibility for them.

14. Protection of what? A hacker attempting to subvert network functionality, or a criminal running a phishing site or botnet, is not necessarily impacting upon national security. His acts are more likely to be technically criminal than they are open acts of hostility. Is the military really to be responsible for the assets of corporations and businesses that hackers and criminals might wish to exploit? The answer is "no". On the other hand, if networks essential for security and governance are under threat, does the military have a role in protecting them? The answer is probably "yes". As mentioned above in the discussion of "cyber attacks", there are many degrees of effect. It is absurd to expect militaries to protect corporate assets as varied as a large multi-national network or social networking site, particularly as the overwhelming majority of public networks are owned by private companies. Military should of course have responsibility for their own networks, and should be prepared to protect all networks in time of war, but in peacetime it simply doesn't stack up. However, it does not pay to be too rigid in one's views on this issue. We can imagine that the military might afford critical infrastructures *physical* protection under hostile conditions precisely because national networks rely on privately owned hardware. In organisational terms, we cannot expect responsibilities for such infrastructure to switch from party to party too much, which speaks again to the discussions over multi-stakeholder approaches with which this Inquiry is largely concerned. The military's principal role should probably be as a uniquely-positioned actor in the principal "action triad" of military, intelligence and industry, sharing information and providing resources where and when required, and occasionally muscle too.

15. Is a militarised cyberspace, in whole or in part, desirable or justifiable? This is a question that greatly exercises activists, technologists and ethicists of many different stripes when it arises. It is a valid concern although its terms of reference tend to be blown out of proportion to reality. Most European states are content with the current separation of the military from political and civil spheres, an arrangement that has served well in most countries whilst not at war or in times of revolution, and none of the three parties would be content to change this. I raise this issue because of recent debate in the US over the proposed Rockefeller-Snowe Cybersecurity Bill (S.773) which was interpreted as allowing the President control of the internet during periods of "cyber emergency". In effect, this was an updating of extant legislation such as the War Powers Act (1973), a point missed by those internet users whose howls of anger drowned out much of the rational debate on the issue. The EU is not proposing that cyberspace/the internet/the web come under military control in peacetime, either in whole, or in part. It is suggesting that if the conditions are amenable to it, and such a response is necessary, that militaries have a major role to play in either repulsing attacks, or in neutralising their sources. This is a sensible policy.

16. Which military? Within the EU, no member state's militaries act in complete isolation; most are either members of NATO, party to the European Security and Development Policy, or both. Due to the transnational and distributed nature of cyberspace, it makes sense to strengthen European and international cooperation and knowledge transfer with respect to cyber issues. NATO has already begun this type of activity, as noted above (para 11), and these networks and exchange programs should be encouraged, broadened and deepened. Under such arrangements, states would be able to draw upon the expertise and experience of all EU militaries should they need to do so. This is currently the case for kinetic actions. Although there are many problems with collective security frameworks, there is little reason to propose that an effective system cannot or should not be built. It may actually be a lot easier and productive than traditional collective military operations, due to fewer demands on matériel, although intelligence-sharing may be problematic and complex. The success of these endeavours is likely to be predicated on the ability to parse the threat environment satisfactorily, to prioritise threats according to their impacts and effects, and to delegate resources sensibly as a result.

Conclusion

17. I apologise to the Committee members for the length of this submission. My observations are neither complete but nor should they be considered in isolation from the other issues raised in your Call for Evidence. All comments are based on public open sources, although specific references can be provided if necessary.

18. The emphasis of the EU Policy is on protecting member states from large-scale cyber attacks, and the EU is correct to assert that defence is the key to success in this field. There are many approaches that can be used to combat or counter the sources of cyber attacks but getting one's own house in order is a first step to thwarting attacks on one's own systems, at local, national and transnational levels. This calls for a communal defensive strategy that relies on all stakeholders for success. I have focused on the military but the private sector is likely to be the most important in this debate. The Committee's Call asks a final question, whether the Commission's plans can be put into practice by the end of 2010. As these principally deal with

"frameworks" and "roadmaps", and the definition of "criteria" and "priorities", there should be no substantial obstacles to doing so. Meeting these targets will depend on the willingness of member states to work together to achieve these goals. The UK is in an excellent position to play a significant role in this process and I hope it takes the opportunity to do so.

3 November 2009

Memorandum by XS4ALL Internet

I am writing in regards to your recent request for input on EU documents "Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience" (COM(2009)149 final, Council document 8375/09) and the "Impact Assessment" (COM(2009)399 and 400, Council document 8375/09 ADD 1–4). I understand that you are soliciting input on these documents as well as the overall proposal being put forward.

For context of my input: I am the Chief Security Officer of XS4ALL Internet B.V., the longest-established Internet Service Provider in The Netherlands, and part of the Koninklijke PTT Nederland (KPN) corporation. I also serve as one of the five kernel Security Officers for KPN-CERT, the computer emergency response team for the entire KPN organisation. Further, I sit on the board of directors and steering committee of the Forum of Incident Response and Security Teams, an international non-profit made up of over two hundred IT incident response organisations from education to multinational to governments and beyond.

This feedback is based on my role in the IT security industry for over 20 years, and is not a specific statement on behalf of any of the above listed organisations.

Threat analysis

— *How vulnerable is the Internet to wide-spread technical failures? To what extent is it likely to be affected by natural disasters?*

The Internet was, and is, built to be resilient at multiple levels. Wide-spread technical failure is extremely rare, and in many cases can be prevented through the use of "best-practice" guidelines. Unfortunately, as the popularity of the Internet has increased and expanded into regions where such guidelines are not followed carefully, the potential for limited disruption has increased. In reality, these disruptions are noticed quickly by the international community and usually rectified with all due haste and professionalism.

Natural disasters pose increased risks where reliance on physical architecture elements has created points of focus for Internet traffic. An example would be fibre-optic cables damaged due to earthquakes, without appropriate levels of redundancy. However, this risk is actually greater in many metropolitan areas where several communications companies "bundle" their physical infrastructure together in the same underground piping/ditches/etc. Internet outages caused by backhoe or a shovel far outnumber those caused by natural disaster.

In many cases, the vulnerability can be mitigated through current technology and procedures, but that often comes at a financial cost. Two fibres on different physical paths costs more to deploy than one.

— *Is the Internet industry doing enough to ensure the resilience and stability of the Internet, or is regulatory intervention unavoidable? What are the cost implications if the industry volunteers, or is forced, to do more?*

Yes, it is doing enough. More regulatory intervention is not necessary. If anything, it could well do more harm than good.

— *The Commission is particularly concerned about cyber-attacks, and draws attention to events in Estonia in Spring 2007 and Georgia in August 2008. Is this concern justified?*

No. These events were in many ways atypical for the "damage" they caused due to the relative unfamiliarity with standard Internet security practice for some of the Internet providers involved. Involvement of their "network neighbours" has brought about a wealth of knowledge, awareness, information exchange and experience.

— *The events in Estonia led to a more public involvement by NATO in cyber-protection issues. Should the military be more involved in protecting the Internet?*

Absolutely not.

— *How concerned should we be about criminally operated "botnets"? What evidence do we have that shows the scale of this problem, and the extent to which it can be tackled at the European level?*

You should be aware, but not overly concerned. Governments and the EU should focus on making sure that those of us who operate in the Operational Security realm receive the support we need to do the job for which we are trained and responsible. We are happy to provide high-level information and risk assessments, and your awareness of what these risks are (and understanding their proportionality as compared to the perfectly normal and valid Internet use) is warranted, but, as they say, "Don't Panic".

International responses

— *The Commission believes that a pan-European approach is needed to identify and designate European Critical Infrastructures, and that national responses will be fragmented and inefficient. Is this analysis correct? Would multi-national companies be especially in favour of multi-national policies?*

It's not that simple. The Internet does not care about borders and nations. Its popularity and use is driven, and governed, by this principle. The Commission is right to be focussed on the preparedness of a specific member nation's IT and IT security infrastructure, and any "National Approach" is doomed to failure, but indeed the true success of IT security and CERT activity for over 20 years has been in the private organisation and multi-national co-operative approach.

— *The Commission draws attention to the emergence of "public-private partnerships" as the reference model for governance issues relating to critical infrastructure protection. However, they see no such partnerships at the European level and wish to encourage them. Are the Commission correct in this aim?*

Yes, but they're wrong about the partnerships. There are a vast number of them. Not all make headlines. The partnerships are about solving specific problems and the fact that they are simply getting on with the task and accomplishing real results behind the scenes is a testament to their results driven success.

— *Are there indeed market failures occurring so that there is inadequate preparation for high impact, low probability events? And if so, how should they be addressed?*

No.

— *The Commission supports the European Information Sharing and Alert System (EISAS). Is it appropriate to develop this type of pan-European early warning and incident response capability?*

No. The Industry has such efforts already, and the Internet does not care about "Europe" per se—decades of practical experience has proven this. Many (most) large scale network operators have participated in such early warning and incident awareness networks for many years. Creating more initiatives creates more duplication of effort and content.

— *Are Government operated Computer Emergency Response Teams (CERTs) an appropriate mechanism for dealing with Internet incidents?*

No, absolutely not. A Government operated CERT should focus on being the computer security response organisation for a given government's IT infrastructure only. Their obligation is to their residents and citizens and the infrastructure the government itself provides and uses. Most governments are woefully unprepared for their own IT infrastructure and need considerable time to get "their own house in order"—at the end of the day they are merely one player in a large world of response teams—one voice in the CERT choir.

— *Will the UK's existing approaches to this policy area be adversely affected by fitting in with a European-wide system—or will this lead to improvements?*

— *Is it sensible to develop European-centric approaches at all, or should there be much more emphasis on a worldwide approach? In particular, are US policies consistent with the proposed European approach to the problem?*

Worldwide. The worldwide approach is precisely how operational computer security response organisations have functioned for decades, with phenomenal success.

European Network and Information Security Agency (ENISA)

— *The Commission sees a major role for ENISA in developing national CERTs, and in assessing the development and deployment of EISAS. Is ENISA an appropriate body for this work?*

The problem is with the concept of a "National CERT"—as already mentioned, this concept is fundamentally flawed. Adding more layers to incident response work in the form of National CERTs only serves to slow down the process, add bureaucracy, muddle incident details and, inevitably, lead to finger pointing and inaccurate feelings of incident resolution.

For example, it is far more efficient for a telco or provider or organisation to know how to reach out to my CERT team directly when an incident arises involving our organisations. By introducing additional links in the incident handling chain, the chance of data going missing, misunderstood or simply delayed, increases exponentially.

On a regular basis I receive incident reports directly from telcos/providers in other countries. Usually within minutes of the incident starting. That same incident is sometimes shared with national CERTs—and the data that eventually (weeks later) arrives has been modified to be almost unrecognisable from the source format.

There may be a limited role for ENISA to help Governmental CERTs. The response team specifically focussed on the IT infrastructure for a government itself.

— *Is ENISA being effective in its role, or does it need reform?*

Timescales

— *Most of the Commission's plans are to be put into practice by the end of 2010. Is this timescale realistic?*

No. Much of this work is tremendous duplication from existing efforts that have been in place for years or decades, the rest may very well be addressing the wrong problem.

I apologise for the time it took to get this feedback to you; I understand that you are already underway with inquiries in the House of Lords (a colleague of mine from the Forum of Incident Response and Security Teams is presenting to the Lords on 25 November), but I think it is critical that you take these points on board.

Those of us who spend our days helping defend the IT infrastructures of millions of citizens throughout not just Europe, but the world, who consider the Internet a daily utility have a wealth of hands-on experience and knowledge, and we are always happy to help educate and inform others as to the realistic threats and risks.

In closing I'd like to summarise a topical computer security incident involving CERT teams and global co-operation which took place this past weekend.

Last week I discovered a new iPhone worm which had the potential to harvest data from compromised phones, interfere with internet banking, and spread to hundreds of devices (likely thousands) in only a few hours. As soon as I realised what I had found, I shared the details with the operational Internet service provider communities, including the Forum of Incident Response and Security Teams.

Within minutes anti-virus firms and IT security press were publishing updates, fixes and details. My reverse engineering of the malicious software and the responsible disclosure I made to organisations who could help deal with the problem resulted in a spontaneous and instantaneous response of experts from around the world (from Australia to Japan to the United States to many European nations)—the right people know how to find each other. Enhancing our ability to do our jobs, without the encumbrances of unnecessary legislation is how the Commission should seek to assist global IT security events.

Our calm, rational, experienced response is here to help.

The sky, as they say, is not falling.

24 November 2009

Printed in the United Kingdom by The Stationery Office Limited
3/2010 441925/1312 19585