

WEDNESDAY 4 NOVEMBER 2009

Present

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

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 30 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

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.

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 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 2001/2002 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.