

WEDNESDAY 9 DECEMBER 2009

---

Present

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

---

**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 per cent 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 per cent 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 per cent, 30 per cent, 40 per cent 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 malware 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 per cent 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 Chantzios:* 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 Chantzios:* 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 Chantzios said, address their own needs in a very sector-specific way.

*Mr Chantzios:* 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 Chantzios:* 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 Chantzios and not as Ilias Chantzios, 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 Chantzios:* 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.