

WEDNESDAY 2 DECEMBER 2009

Present

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

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

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

Mr Servida: That helped.

Q109 Chairman: Welcome. May I just give you a few background notes? You will know that this session is open to the public, although there is no member of the public present at the moment. A webcast of the session will go out live and as an audio transmission and is subsequently accessible on the parliamentary website. You will be sent a copy of the transcript of your evidence; this also will go on the parliamentary website. If, after the session, you want to clarify or amplify any of the points you have made, we would very much welcome that but could you let us have it as early as possible. You will hopefully check it for accuracy and, again, let us know as soon as possible, if you feel there are things which need to be changed. The acoustics in this room are particularly bad. I am rather deaf so if you would be kind enough to speak up that too would be most welcome. Perhaps you would be good

enough to introduce yourself to begin with to the Committee and for the record and then we will start our questioning.

Mr Servida: Thank you very much. My name is Andrea Servida. I am Deputy Head of Unit on network information security, internet and “.eu” within the Directorate General Information Society and Media of the European Commission. I feel honoured to be here in front of you today.

Q110 Chairman: Thank you. That is admirably brief.

Mr Servida: If you want to know more, I am Italian and can speak for much longer.

Q111 Chairman: Could you tell us why you believe that internet resilience is an appropriate topic for the European Union to be tackling? Surely this is really a matter for individual Member States. What is the added value that the EU and the Commission in particular will bring to this whole issue?

Mr Servida: I will start with the political dimension and then the more urgent dimension, which is the nature of the problem with which we are confronted. In terms of the political dimension, I must recall the request by the Council in 2004, after the bombing attacks in Madrid, to the Commission to come forward with a programme to help Member States work together to coordinate their activities better in order to face terrorists and the possible risk to the critical infrastructure. This led to a number of statements by the Commission. I must also recall that the Council requested the Commission to develop a programme, in cooperation with the other institutional bodies, in particular the High Representative for Common Foreign and Security Policy, that is the Second Pillar dimension, as well as the Member States, which are important, and the European Parliament. That led to a number of activities which materialised towards the end of 2006 in a communication from the Commission, as a response to the request by the Council, putting forward a programme to engage the Member States in

coordinated activities in respect of their responsibility to work together in order to address and take on the challenges relating to the protection of critical infrastructures. Then there was a proposal for a directive which somehow was meant to provide the framework for Member States to identify on what they would like to work together and to exchange practices and good policy measures. This directive was adopted towards the end of 2008; it is the directive on the identification and designation of the European critical infrastructures and under this directive two sectors, transport and energy, were identified as critical ones to which the directive provisions had to be applied immediately. The next in line was somehow identified to be the ICT (Information and Communication Technology) sector. Why was this approach coming forward in the directive? Because, very much in the way that had been adopted by other countries, particularly the US which I think had opened the way back in 1997 with the PCCIP (President's Commission on Critical Infrastructure Protection) report on critical infrastructure protection in the context of the reflection on how to deal with the Y2K vulnerability, the Commission proposed to go about engaging the Member States and stakeholders in protecting the critical infrastructures via sector specific approaches which means designing policy that would somehow address the specific vulnerabilities, including the interdependencies which had been identified in 2006 as one of the horizontal sectors, to engage the stakeholders to look at the specific sectors of transport, energy, food, utilities and all the rest. In this respect the political dimension to the urgency to look at security and resilience comes from the fact that the policy statement, policy proposal, which was put on the table in March by the Commission, tried to articulate in anticipation of what would be the implementation of the directive and anything that may come as a result of the implementation of the directive, which could only happen after 2011. Then, in anticipation of all this, we came forward with a set of measures we considered important and which were to some extent alluded to in the preparatory activities that the Commission have carried out since 2006 on

how society, in general, should prepare itself in order to be able to withstand disruption. I am talking about disruptions because I think what it is important to highlight here is that the proposal that is on the table, which was adopted by the directive, is to some extent instantiating, in terms of immediate measures that it would be worth considering and pursuing, as they address at the European level the specificities of the IT sector for what it means in terms of critical sector for society. This is where indeed we have to frame this proposal and we have to frame this proposal from the perspective of how society should act in order to make the work of law enforcement, police, judicial systems more effective and simpler when dealing with possible threats due to criminal activities or terrorist activities and other possible realisations of malicious intentions that may exist in society. Why did we take this approach? Because we believe that if we want to make our society more secure, safer for everybody, everybody should pick up his or her own responsibility. Security and resilience are conducive to the message that everybody should act. We cannot just think that the protection of other critical electronic communication networks, our information infrastructures, whatever you like to call them, could be delegated just to law enforcement, defence or any other national agency or even international endeavour of national agency or governmental agency. Why? It is so pervasive throughout our society that we have to take a measure as a stakeholder. It is of course not only up to the end user to do something. That is the weak ring in the chain. It is up to everybody, but in particular the private sector. Why? Because, as a result of the liberalisation of the electronic communication network and service market, the owners and the operators of networks are in the private sector. We do not have any more monopoly type situation where it is easy for governments to act and to maintain a grip on these critical resources. The private sector is acting; we are favouring the development of new markets. This leads, particularly in this sector, to a globalised market to globalisation and new opportunities for society. However, everybody should somehow take a

step and understand that we are not just talking about commodity services, we are not just talking about new gadgets and new opportunities for business growth, we are more and more relying on these services, products or resources, as if they were really the nervous system of society. In this respect everybody should take responsibility. This is why we put the focus on security and resilience and this is why, as we said in the communication, this policy proposal is complementary to everything that is ongoing and which is in the pipeline in terms of European initiatives, intergovernmental initiatives, in the area of coordinating and making the cooperation between the police and the judicial system more effective and efficient. This proposal is not just what would be sufficient to protect the critical infrastructure; it is to some extent developing the societal, the business dimension which is needed to understand and to take the citizen into account in order to make us as Europeans able to withstand the problem.

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

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

for any government and for any administration, including the European Union, to set the framework conditions which on the one hand would help society to develop and the internet to bring all the innovation which is needed but at the same time would ensure that we look at the way in which our digital society is developing in such a way that we will retain in the way in which the society is developing type of safeguard, whether technological, legislative or other, which would help everybody to benefit from these developments. This is why we need to stimulate everybody to understand that they have a role to play and to find incentives. This is why the policy that we have there does not rely on the Commission to do much, to be honest; it is more for the Member States, it is more for the private sector to engage with Member States. I must say that I am here speaking before you in a country which is a leader in this area worldwide for a number of reasons but across Europe we are not all running at the same speed. The pace of development, in particular in terms of our security policy is really varied. Just to give you an example, there are countries where the first ever policies in the area of network information security were developed during the course of 2007, a couple of years ago. If that is the case, what could the understanding be in those countries with respect to the nature of the issue, how to engage resources, in particular the business and private sector resources? That is where Europe is trying to support. The Commission and the European Union are trying to stimulate the Member States to act, building on the good experience and the understanding that have been developed in those countries who have done more in this area and therefore they are leading. Of course, we also have to look at the whole picture. Just doing more yourself domestically does not make you safer because you are interconnected; you have interdependencies with other countries, with other regions. Unless we are somehow making sure there is no vulnerability or risk getting to you because other regions are not considering the measures which have to be taken, then you will never be able to be safe. Nor, I suspect, and we can build on the experience of the US in this area, no

individual country could sensibly consider itself to be in a position to take on all the risks, all the threats alone just because we are so interconnected, so global and it is so easy to cause damage across the world. Something should be done to put in place without fencing, those measures which would help to keep the environment a little more secure, more resilient.

Lord Mawson: And a bit about your background.

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

Mr Servida: Yes, I am; indeed.

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

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

Q115 Chairman: Thank you; that is very helpful.

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

Chairman: It is helpful that the Committee knows that.

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

Mr Servida: Absolutely; yes. This is to some extent in the spirit. The policy statement is in the framework of the EPCIP (European Programme for Protection of Critical Infrastructure) directive and the directive sets, as the first step, full cooperation at the level of Member States and the identification of European critical infrastructures, in this case for the ICT sector. We are not there and we will not be there until after 2011. Two options: we can stay away and in the meantime pursue the development of the sector-specific criteria which are needed in order to implement the directive when the directive applies to the ICT sector, which is indeed the legal framework in which we operate. Of course this is a decision by the Member States because the Directive was adopted by the Council in 2008. Or, we try to anticipate, in relation to what might come, the self-evident or the undeniable facts we are confronted with, we can start looking at how we need to prepare ourselves to deal with whatever would be then identified to be the European critical infrastructure or not for the ICT sector. This is why, for the international dimension, we jump ahead. If you do not know what the European critical infrastructures are for the ICT sector, how can you go international? On the other hand, it seems established, and I think this is common knowledge, that the internet, whatever type of understanding we may have of it, whether physical infrastructure or a platform for supplying services for access communication, whatever, the internet itself is global and, even more

importantly, it has been developed in order to be resilient. In itself, genetically if I may put it that way, the internet was built to be resilient, to be resilient to nuclear bombing, as I understand it. I was not there at the time. That was the original need which led to the development of ARPANET (advanced Research Projects Agency Network). Because the internet is global, we need indeed to start thinking of how Europe would be more influential in the way in which the internet is developed. Let me give an example. You mentioned China. China is introducing a number of regulatory measures which are extremely difficult to understand in terms of what would be the effect with respect to the overall security of the internet. On the other hand, all these regulatory developments are pursued in the name of national security. The Chinese Government is there to protect the Chinese citizen and these aims are legitimate. We cannot say they are not. However, the big picture is not there so China is pursuing this development and is introducing a number of trade issues, trade barriers, which are extremely bad. To answer you – and this is my personal understanding and understanding that I have gathered from discussion around the world - we need to make sure that this does not happen, because fencing the internet is not going to help anybody. This is why one of the pillars, within the limited responsibility we have for information activities, we are proposing Member States come forward with their priorities and our priorities as a region. One of the questions is whether we can really bring down the internet. Perhaps we may not bring down the internet as a whole system but of course regionally we may be disrupted. We are seeing cases due either to attacks or to failures of technological systems like submarine cable breaks in 2008 and before. There we thought, indeed the Commission thought, that in order to be influential we really needed to gather more information and we needed to engage ourselves more with other regions but we cannot do it via 27 bilateral discussions because that will not help and will lead to fragmentation. This is actually what we see in certain international arenas where the different perception of what is critical in the internet, whether it

is the service provision or the cables and the wires or other things, is making the position of Member of States a bit contradictory one to the other. This is why, we have put there a seed for what could be the development in the area of the internet via the establishment of priorities, establishment of what the guidance could be that you, Member States, at the European level could agree would be important to secure the resilience and stability of the internet and to promote this inter nation via the strategic alliance. This is why in the declaration of the EU/US summit which took place on 3 November in Washington there is actually one clear reference to the effect that the US and the EU agreed to strengthen the cooperation on cyber security resilience and trustworthiness of the communication networks and the internet. We need to go via a strategic alliance - and I think personally but these are views to some extent shared in Brussels - that if the EU and the US can do it together the others will follow because there will be sufficient power and weight in the way in which the two regions would act together to make the others follow. This would also possibly embrace in the discussion those regions which in a way feel themselves isolated and therefore they feel they have legitimate grounds to think of the internet as a kind of private garden and to plant whatever flowers they want in their garden without thinking that perhaps this might not be good for everybody. This is very worrying because we see a regulatory development but we also see technological development. I learnt when I was in the US just before the summit at the end of October that indeed there is a proposal coming from China, at the ITU (International Telecommunications Union), to modify the BGP (Border Gateway Protocol) protocol, which is an IETF (Internet Engineering Task Force) protocol not an ITU standard to introduce counting methods and controls possibly for anybody to monitor and count the flow of packets to introduce possibly a remuneration mechanism and to make everybody pay for the flow. This is a technological development. But, what is behind it is the policy assumption that if you put in more technological controls in certain critical resources of the internet we

may of course do something, which might not perhaps be so evident in what is declared to be the very purpose of such a development but which could be easily done if there is an hidden agenda.

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

Q117 Chairman: May I just say that this Committee over the last year or so has been very concerned indeed about the lack of cooperation and coordination between the EU and NATO. We have put this in reports and I have also, with another hat on altogether, drawn attention to this lamentable relationship between the EU and NATO. If you could put that together with the question from Lord Hannay of Chiswick, I should be obliged.

Mr Servida: I will try to do so. I do not know whether you have seen the report that the NATO Centre of Excellence in Estonia completed on the case in Georgia. It concerns the legal analysis of whether the attacks could actually be considered as leading to all the elements which would trigger article 4 and 5 of the NATO Treaty. The analysis is not conclusive of course. When it comes to cyber warfare it is very difficult to establish the chain of command as being the head of a government and saying “Do this, this and this”. Even if that were the case, there are issues about the way in which you can ensure traceability of what

is happening and understand what is indeed the actual target that was aimed at. In terms of cyber warfare, for national governments this is to be one of the areas to be looked at for sure and that is the primary responsibility of national governments and it should stay so. We as the Commission have no mandate to do anything in this area. The relationship of the institution with NATO is mostly with Solana, the Office of External Relations and I must say that, in preparation of the policy proposal that is on the table today, Commissioner Reding, actually met the Secretary-General of NATO at that time to address a very specific aspect, that is the aspect of how to work with the private sector. NATO also has initiatives to engage the private sector because at the end of the day even Estonia has shown that top-down intervention does not really fit the timescale and the pace of development and the type of cooperation and resources that you need to have readily at hand and to make them work in the scenario like the attacks which were carried out on Estonian networks. We had these discussion with NATO to see how, at least when addressing the private sector, which to some extent has owns the resources, the electronic communication networks and operates them, how we could make sure that cooperation would cover all the aspects, those aspects which are closed and related to defence needs and capability, because at the end of the day NATO will have to interact with them. Why? Because cyber warfare is not considered to be just addressing the critical governmental resources as such but a will impact society, internet banks. We have seen what happened in Estonia with attacks on banks and we should not forget the attacks on Estonia lasted for three weeks. Even in those three weeks the cooperation which was put in place was not mandated top-down from the military and a defence perspective. Of course there was a joint effort with law enforcement but really the people on the ground were mainly those who were really cooperating at the level of CERTs, governmental CERTs, international CERTs and others, telecom operators and all the rest. In short, cyber warfare activity is a national priority. There is need to look into it and to see how

that could be tackled. I think the only case we could gain some understanding on cyber attacks combined with an act of war was indeed the case of Georgia; it was clear that was a coordinated effort. But, coming back to Estonia, the analysis of today is really very elusive, not conclusive and it would still be very difficult to act on it. Of course we and national governments will have to take into account that, because of the pervasiveness of the technology and services which might be subject to attacks, the realisation that a cyber warfare type of scenario would primarily impact on society and there is where, as I understand from the analysis that I have read, everything becomes more complicated because to decide whether it is an act of war or not might indeed take longer than for the attacks to impact on society and possibly be fought and mitigated.

Q118 Lord Hannay of Chiswick: Presumably the entry into force of the Lisbon Treaty yesterday will to some extent simplify a bit the divisions between the Commission on the one hand and the Council Secretariat on the other because you will presumably be trying to produce a unified approach to these matters in the future. I am still missing slightly an answer to the question which has been put to us quite often by witnesses and others as to why it is that the EU should be involved when so many of its members are members of NATO and there is clearly quite a lot of ongoing work being done in NATO.

Mr Servida: If I may, I think that the purpose of the policy as spelled out by the Commission is to bring forward and to raise awareness of the fact that because of the nature of the problems that we are confronted with we cannot just delegate defence to do it or a national security agency to do it. If we don't have the civilian society, in particular the private sector, but not only the private sector, the users, even the public administration to take up some sort of responsibility for making the environment a bit more secure, more resilient, to be able to withstand more the potential disruption, whether from attacks or technical failure or natural hazard does not really matter but we have to raise more awareness that we are not isolated. It

is not that by connecting ourselves to the net without any protection we possibly only bring harm to ourselves only, but that our resources could be exploited to carry out attacks on others and we do not even see it. There is where we try to intervene. Of course on the more cyber defence-related issue, the Lisbon Treaty would facilitate but I am not sure whether on the war-related aspect there would be any difference. I am ignorant in this respect whether we do gain any further competence, I am not sure we do. This has always been outside the scope of the Treaty.

Q119 Lord Richard: I wonder whether I might just follow this up briefly. Several times you have said that the object of the negotiations was to produce a unified way by the individual Member States, to assess regional priorities, to present those regional priorities to the United States if they have different ones, though frankly it is very difficult to see what different ones there could be. What I am wondering is what sort of structure you see within the EU to try to deal with this. Do you see a new kind of organisational structure, a director-generalship, a DG? How?

Mr Servida: My personal reflection is that we do not need a European structure in place. Member States have the primary responsibility, the democratic safeguards that have to be there to ensure that any action that governments take to fight possible disruption is to be theirs and we have seen it with Estonia. When things happened people did not turn their face to the ISPs but to government. Why? When you are disrupted in your daily life of course you turn to the government. I think that is where any and every European citizen would indeed be looking. In the UK people would turn to face your government, in Germany it would be the same.

Q120 Lord Richard: Given that, which I entirely agree with, what is the role of the EU there except a coordinating role almost an intellectual coordinator as opposed to a practical coordinator?

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

Q121 Chairman: Let me put a practical suggestion to you. You say to provide a platform to help States who are being affected. I am sure you will know that NATO, to use a dreadful acronym, have something called EADRCC, which is the body which NATO have to go to the aid of a stricken state which has been affected by a terrorist attack or a natural disaster. Each year they have an exercise. I attended one some years ago in Croatia where 17 nations participated; they had simulated hijack, biological attack, earthquake, chemical crisis and so on. This year in September their exercise will be in Armenia. If that exercise included a simulated cyber attack and if NATO, EADRCC, gave you an invitation to attend, to observe and to participate would you be keen or would you be anxious to go or have a representative from the EU go? If you were to go, I should be delighted to entertain you for dinner.

Mr Servida: What can I say? Perhaps I may say that personally of course it would be a huge opportunity to learn because nobody has a solution here. I must say that personally I would be delighted, provided that there is no problem with security clearance or whatever, because that is the other side of the picture when you have this type of exercise. Apart from this, our interest is to learn and how to put the framework in place for things to happen. When I was in the US and I was talking with DHS (Department of Homeland Security), they were actually considering inviting the Commission as observers for Cyber Storm III because they now have an extended programme of observing countries. Of course, we are not a government but nevertheless they see the opportunity to engage with us in a way that would be up to the US to decide. As I said, I felt honoured and interested. For us the participation would possibly be instrumental in designing or possibly supporting Member States on how to work together. Indeed in that respect, in view of the fact that Member States had requested the ENISA agency to help them plan and organise the first pan-European cyber security exercise, I might say that it would be even better for them to be there to observe and learn than for us. I think that this type of event is always very enriching because they help to deepen the understanding

of how complicated the issues are and, more importantly, who has been forgotten outside the room. That is what I learn at least by talking to the experts from those countries who have already conducted this type of exercise.

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

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

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

interests. It is not just that a little local or regional intervention would make sure that the internet would stay up and running; on the contrary.

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

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

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

Mr Servida: Yes; absolutely that is an easy target. However, the analysis of Estonia showed that taking down media websites was actually more alarming to people than not having transactions done digitally. We should not forget that one of the systemic vulnerabilities of Estonia was actually due to its strength of having nearly, if I am not mistaken, 95 per cent or 96 per cent of payment transactions done digitally. When they became independent they decided to develop the information society in a way that perhaps was not very much considering the resilience or the redundancy issues but that led to digital cash being the common means of transactions. The fact that the media were not up and running was even more alarming. Again, we can easily think what the vital services are for what we understand

as society today, electricity, banking, communication but it is only really by testing and seeing how the scenarios develop - I hope that we shall not go through it - only by analysing incidents and attacks that we can really understand what is worrying and what is vital and for what purpose it is vital. That is where we come back to the issue of making sure that we learn from what is happening and we learn also from near misses, those events which perhaps do not reach the front page of a newspaper fortunately but nevertheless they are instrumental to understand the picture and how things may go wrong. That is why we, in the policy proposed at the European level, invited the Member States to equip themselves with those bodies which would make them able to learn from the process as well as to act. Of course there is not much to be taught to a country which is already well equipped, but nevertheless drawing attention to the fact that there is a need to cooperate beyond the national boundaries, which in this country would be like preaching to the converted, is a message because it shows what the responsibilities are. It not just for a little country "A" which may be self confident that it is done everything for its citizens may be deferred to or whatever. If they do not do it, they are at risk of making others vulnerable.

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

Mr Servida: Absolutely.

Q126 Lord Mawson: How do you intend to involve the internet industry in your plans and indeed in your thinking in a serious way? My experience, not in the EU but in this country, is that the world of entrepreneurs in the business and social sector and the world of government are like two worlds actually passing in the night. We may be using similar words but in terms

of communicating and understanding there is quite a gap. How do you intend to involve the internet industry, if that is true, in your plans?

Mr Servida: We have to, everybody has to. In particular at the national level the internet industry, whatever it is embracing, should be involved in the discussions. There are two main reasons. First, there might not be the same understanding or there might be a communication problem, or there might be a problem of how to share the objectives, how to understand each other's objectives. Business is there to make money, to grow, to be in business, to compete globally and that is where it is important that we understand any possible consequence of a regulatory framework that in the name of other possible legitimate and important objectives could somehow put industry in a difficult position to compete globally. At the same time industry should also understand that security is not an option. We need to understand the economics behind this, what the incentives are needed. The market really does not seem to be leading to overall security. Let us take an example. If we look at the old telecom, the German telecom and the British telecom, of course they come from monopolies where there is a culture of security, of reliability which you do not find when you move to ISPs. A realisation of this, just without saying what is bad or what is good, in our discussion we try to involve all European industry across the food chain and when we talk to ISPs of course for them security is a cost. Why? Because for them the service is a mere conduit which is indeed important but at the same time there is no incentive to act. This is well represented in the way that the European organisation of ISPs, which regionally has some good practices, comes from a certain area in Europe, is unable to promote good practices in terms of security, is unable to promote this as good practice for the whole sector across Europe. Why? Because they are so diverse; we have small ISPs, the big ones coming from the monopoly, so the culture is not there. We need really to engage everyone, but we need to engage everyone in order to understand from the governmental side what the business model is, what the industry

is already doing, because a lot of what major industries, in particular the ones coming from the old monopolies, are doing is not highly visible, not visible enough I believe to make everybody confident that indeed they are doing something. At the same time the sector has to react and to be engaged. That is where the difficulty lies. At the European level we think that by bringing into the picture the economic, the business, the market dimension to the way in which public policy objectives, which are legitimate and should be understood by industry, could be articulated, to the way that a baseline approach could be developed, that might be the way for industry to find a gain.

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

Mr Servida: Absolutely.

Q128 Lord Mawson: What are you doing practically to try to make those interconnections between entrepreneurs and the EU?

Mr Servida: The very pillar for intervention is the European public/private partnership for resilience for which we have launched the idea. We have started a process to engage at the European level with private sector and public bodies in Member States in order to see how to establish it. By the end of this year we will come forward with the road map and the plan is to launch it by mid 2010. It is not easy and it is not easy because indeed we need to marry at the same time sharing the public policy objectives and sharing priorities on operational measures and the operational measures stay where the private sector stays. We need to make sure that there is an economy of scale so what is decided in the UK will not be different from what is

decided in Spain. I suspect there are several players acting in Spain and in the UK and they may find it difficult and costly to have to fulfil or to meet requirements which are defined top-down without any understanding of the very systemic issues there and for the industry this will be a cost, will be a way to be less competitive in the global market. That is where people like to get. How to mount it is the challenge and this is why we are talking to the private sector but, even more importantly, to Member States. The partnership should first of all be national. You are lucky enough here to have public/private partnership initiatives, the CPNI is working well and that is a pillar but we need to draw from that in order possibly to address in the European pillar those global issues which are not just UK based. We had a discussion on the public policy aspect of vulnerability disclosure and in CPNI I understand that there is a process there which is replicated by the same players in Finland in Sweden and in Germany. Is this effective or does it bring a cost? Is it not the case that there is some sort of baseline that if it works in the UK it works also in Spain, in Italy, in Sweden and in Denmark? Having the discussion once and for all and having everybody agreeing on it in terms not of regulation but in terms of voluntary commitment to what would be the practice to be followed, which is stemming from shared public policy objectives and shared understanding of the economic dimension, the market dimension, the competition dimension, we think will help industry to compete but at the same time to meet up their responsibilities. Otherwise it might become a requirement should something go wrong. We always catch the train. Estonia happened; unfortunately we did not have regulations put in place. Should something happen again, then politicians will need to introduce something and if that is introduced top-down might stifle innovation. This is what we believe and this is where we would like to get the internet industry, not only at the European level but globally though if you do it at the European level you have the voice, the weight, to pursue a similar discussion across the world. This is why in contacts that we had with the US we will talk to government but also to the private sector.

DoC, the Department of Commerce, is extremely interested to see how we can align the way in which we can indeed bring the incentives forward to the private sector to make a global policy because there is an economy of scale to be gained.

Q129 Lord Mawson: You only learn about that by doing it.

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

Q130 Lord Richard: This question may not actually be for you and if it is for you, I think you have probably answered it quite a lot already. In your view is the internet safe at the moment for consumers to use?

Mr Servida: That goes beyond my remit but we contribute a bit of course in terms of defining the point. What is safe?

Q131 Lord Richard: Usable, works, does not break down, is not attacked, that sort of thing.

Mr Servida: It depends for which purpose you use the net. When searching for information, if you just look at what information is posted there or where the information comes from, whether it is quality we do not know. Let me put it this way. I think the internet should be safer and should be safer because the user is the very weak ring in the chain, not in terms of being the one who does not understand anything about security or whatever else, but he is the one most exposed and we see this happening all the time. There are business models which

push for more and more profiling and once your personal data have gone off, they have gone off for ever. In addition the user may not really fully understand what is exposed so there is an asymmetric imbalance between those who have actually retained information, because they are providing the service, and the one who is possibly benefiting from services who sees perhaps the screen or whatever or might have difficulty understanding what it is that is happening beyond the screen. That is where it should be much safer and in particular because this is a tool which is not only for computer science PhDs but for children more and more and elderly people; anybody who may not have the understanding or the knowledge to master all the technological issues and concerns and risks that there are. This is where, coming back to the private sector, I think that the private sector has a huge role to play. In our communication which preceded the one of 2009 we invited the private sector to consider the value of going for more security in services and products and to look at the way in which they train their people as a way to bring good practices and knowledge to society. We all work in a way and we all use these means in our daily activities. If you were helped and if you trained and before that you were trained in our curriculum - but this more for the Member States - then there is the possibility for us to build an understanding and culture because it is a cultural issue not a technological issue. There is no technology, at least from what I see, that could solve all the problems. It has to do with the process, with the way in which we understand and we actually relate to this environment. So it is a culture. This is why to some extent the kids are more exposed but they are more cunning in a way in dealing with certain issues. This needs to be considered as a priority and this is why we said in the communication that one of the key elements is that trust is not just security of procedures but security of resilience; trust is more process, knowledge, culture. We need to behave. We need to understand that if you are trespassing into certain areas it is like throwing stones at the windows in the street. This understanding is not there yet.

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

Mr Servida: As I tried to explain right at the beginning of my evidence, the policy which was put forward in this communication in March was not addressing how to go about terrorism. On the contrary. It takes for granted that Europe is engaging, is understanding how to deal with, how to fight terrorism, how to fight cybercrime, how to improve the cooperation between law enforcement agencies and the police and that is happening. Until the end of last month it was under the Third Pillar; there are several initiatives in which the Member States have engaged themselves and the Commission is helping in terms of exchanging information, reinforcing the investigation capabilities in Member States and all the rest of it. This is to happen and that would address exactly your aspect. What is on the table here is in addition to it. We should not forget that there is no civil defence capability in any country that would be able to intervene in a crisis in the country unless we have a good engineering code for buildings construction. If these will not withstand or are not designed and built to withstand the weight and the risk, whatever the risk – not the nuclear bomb risk because there is a risk trade-off there - but will withstand the wind, the snow whatever, without this type of

cooperation between society and civilian resources and an understanding of that risk and the public bodies which have to intervene in the area of fighting cybercrime and cyberterrorism, if we don't have the understanding that we need to do both, not just going after terrorists but also to make sure that we have a more secure and resilient and safer society in which we have to prevent terrorists doing whatever they want to do whether locally or internationally, unless we do this we will not be able to make our society safer. It is like pretending in the civil defence we have to go after any crisis without having an engineering code deployed by society on the way in which buildings, bridges, railways and infrastructures are built. That is where we intervene. This is why we look at preparedness, we look at resilience, we look at the way in which civilian resources, the private sector, should take up responsibility to make the overall environment more secure, to make it more possible for law enforcement, judicial system, intelligence, to do everything that should be done in order to prevent and fight and go after terrorists and cyber criminals. This is why we say it is complementary; it is not replacing. On the contrary, the type of issue that you are raising, issues where - I do not have any understanding because I do not deal with terrorists-, of course terrorists are using resources for communication, they even bring destruction; they do. If you are disrupting society, it is one way of upsetting the order of society, to upset it even more now that you are interconnected, economic systems, the financial system. Disruption in a country is tremendous. Everybody looked at what happened because of the attacks on the Twin Towers, the financial losses. Why? Because there is a reverberation globally. It is not like in the good old days where there was a dampening effect of time, geography, distance. No, no, I plug in, whether I am in New Zealand or in Bristol, to me it is all the same, we are on the same timescale.

Q133 Lord Naseby: What I am trying to get at and the one area I do know quite a lot about is the Tamil Tigers. The Tamil Tigers have websites in the UK and France, Germany, US,

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

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

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

Mr Servida: Business is business. The last count that was done, the inventory that is available from the web of ENISA, says that in Europe we have more than 130 CERTs,

industry, academia, governmental, national, you name them. This is growing, in particular the work between the private sector and academics. In view of what the needs are, the business model, the provision of new services, what we were addressing there was building on the experience that we see internationally, first in Europe but also internationally, how Member States should consider putting in place very basic services which are needed on top of which they may articulate not just policy in the area of protection of critical information infrastructure, but, even more importantly, which can engage this society to be more responsive in order to prevent, fight, mitigate and recover possibly from disruption. What might our Member States need to consider in terms of having an operational capability, which is essential. If we look at the analysis of Georgia and Estonia, NATO did not intervene, nor the ministry. We had a CERT, a CERT in France in the UK in Finland, Georgia, the CERT in Estonia, so those capabilities are there and they will always have a responsibility to manage the networks but at the governmental level, it is important that governments realise that they need to have some operational capability in place. How do you organise it, whether it is just a national one or, the model which is in the UK, different ones, is really up to the Member States. This is why we say National/Governmental CERTs. This is to us a basic component which is operationally needed in order to make each country capable of cooperating with other countries at the European level but, even more importantly, to make their policy effective at the national level because it is only via these operations with people on the ground, those who actually have the problems and own the networks that indeed you can really work out a solution. These CERTs, computer emergency response teams, are those who are in contact with the private sector and those who manage the network. This is why we said it is not just a need for Member States to establish whatever they like, but they need to have it and they need to have this resource not just as an operational resource, but to become a key element, key tool in the public policy development which is needed to engage again the

private sector and the other stakeholders in enhancing the level of security resilience nationally and the European and then the international. It is a more a plea to the Member States to understand that it is important and this is built on the realisation that, despite what we see in the paper, the cooperation at the pan-European level is very limited; we have seven or eight countries where these capabilities are working together. What about all the others? Is this good? We do not think that this good because if we need to react as a region, it would be good to know to whom country A could indeed relate and how to relate. It is not just via the highest political level that a relationship should be established; here we are talking about events which happen at the speed of light so we need to be there in the field and know with whom to engage. This is where the experience in the UK, in Finland, in Sweden and in Estonia now, who did not have much capability, shows that is the way in which you can really be operational and effective.

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

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

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

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

like to do, it would be much better, but even with the current regulation, with the current level of resources, there is quite a lot that ENISA could be doing and to some extent is trying to be doing now with the new management. Even with the new work programme structure which has somehow been put in place since 2008 with a programme with the focus on resilience, for instance, they have done an interesting stock-taking exercise on the security and resilience regimes in Member States. That was important for us to have at our disposal in order to articulate where to intervene. We need to have data on which to act and in order to have this data we need to have a body like ENISA but this whole focus should be the good one ENISA should not position itself to do everything that covers every possible topic. It should really try to focus on where it could make the difference because it is there to help Member States and the private sector.

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

Mr Servida: I look forward to that.

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