

WEDNESDAY 16 DECEMBER 2009

Present

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

Memorandum submitted by ENISA

Witnesses: **Dr Udo Helmbrecht**, Executive Director and **Mr Jeremy Beale**, Head of Stakeholders Relations, ENISA, examined.

Q177 Chairman: Good morning Dr Helmbrecht and Mr Beale. Thank you very much for coming. You have come almost as far as any other witness that this Committee has had for a very long time and we are most obliged to you for coming all this way to help us with our inquiry. Could I begin by just explaining some of the background housekeeping situations. You realise that this session is open to the public and the webcast of the session goes out live on the audio transmission and will subsequently be accessible via the parliamentary network. A verbatim transcript will be taken of your evidence and this also will go on the parliamentary website. We shall be sending you a copy of the transcript for you to check for accuracy, and if you need to make corrections we would be most obliged if you could make them as soon as possible; that would be very helpful. Also, if after this session is over you feel you would like to amplify or explain in greater detail some of the things you have told us, again we would much welcome to have supplementary evidence from you. A final thing which I always say is that the acoustics in this room are very bad; I am rather deaf, so will you please speak up.

Perhaps now you would each like to introduce yourselves and if you would wish to make some opening remarks we would be glad to hear them.

Dr Helmbrecht: Thank you very much for this warm welcome. We very much appreciate this opportunity to talk about IT security topics in this round. My name is Udo Helmbrecht and I have been the Executive Director of ENISA since October of this year. My former position was in Germany, President of the Federal Office for Information Security, so we were involved from the management point of view during the set-up of ENISA in the last five years. So I am well aware of the topics we are discussing here. At the beginning the only remark I want to make is that if we talk about IT security today it is really a new challenge in the area of e-commerce of how we work together, how we communicate together, and therefore I think it is very important that we have this open discussion on this topic.

Mr Beale: My name is Jeremy Beale; I am the Head of Unit for Stakeholder Relations at ENISA. I have been there since April of this year so I am also relatively new. Prior to that I worked as Head of the e-Business Group at the Confederation of British Industry here in London; and prior to that I worked for a number of years at the OECD in Paris on these issues, as well as a brief bit in between at the Cabinet Office.

Q178 Chairman: Thank you very much. Perhaps I can ask the first question, which is one of those basic questions: tell us who works for ENISA; what do they do; and, most important of all, who benefits?

Dr Helmbrecht: ENISA has a staff of around 65 people currently. We have permanent posts and contract agents and we cover a whole range of skills in our Agency. This is because - if you talk about IT security in *society* - we think that we need different skills; so we have people with a technical and computer science background; we have lawyers and economists so that we can address the different perspectives of IT security. We have recruited staff from the private sector, for example, from the Commission or seconded international experts from

the Member States. A lot of people coming from the private sector have experience as a Chief Security Officer – for example, our head of the technical department – so this means that we can cover the experience from the public sector, the private sector and different skills for the work packages and work programmes we are running. The benefits: what we try to do is to provide added value for the Member States and for the Commission. So that there are two directions. One is that we provide guidance to the European Commission in the process, for example, of their legislation via European projects or research areas. On the other hand, we work together with the Member States, for example in building up CERTs and having reports which they can use in their own Member States. We try to do those things on a European level with cross-border activities or cross-border needs in this area.

Chairman: I did not say to you both that if either one of you wants to come in and supplement what the other is saying we would be delighted to hear from you. Lord Richard?

Q179 Lord Richard: Can I be fairly practical and ask you a few background details? What is the governance structure of ENISA? How does it actually work?

Dr Helmbrecht: If you look into our regulation we have some formal bodies: one is the Management Board. The Management Board is representative of each of the 27 Member States.

Q180 Lord Richard: You have 27 Member States.

Dr Helmbrecht: And three representatives from the Commission, so the Management Board has 30 members and the Management Board is responsible for approving appointment of the Executive Director.

Q181 Lord Richard: How often does it meet?

Dr Helmbrecht: It meets two times a year as a whole body. The other formal structure is the Permanent Stakeholder Group, which is appointed by the Executive Director and has members from academia and universities, and from industry; and from the citizen point of view from the, let us say, associations or businesses from the Member States representing users. So these are the formal bodies; and in addition to these we have so-called National Liaison Officers. These are representatives of national governments who act as a single point-of-contact. In addition when we are running our work programmes, we typically have experts for technical expertise; this is the basic structure. If you look at, for example, financial regulations, we have work package processes where ENISA makes proposals, which we discuss with the Permanent Stakeholder Group and the Management Board, and these proposals are then presented to the Management Board to discuss and approve; so this is the basis of our work. This means it is influenced by industry, private sector users, by governments, by the Member States, and by the Commission - and the results are also in the end presented to them; and for the annual account for the financial area I have to go to the European Parliament for them to “discharge” to use an accounting term.

Q182 Lord Richard: You have national representatives in ENISA?

Dr Helmbrecht: Yes.

Q183 Lord Richard: Do you have ENISA representatives in the individual countries?

Dr Helmbrecht: We do not have representatives of our own in countries; so this means that we with our Agency are located on Crete. For projects, for meetings we often go abroad; so this is something where the interaction is done on a project and working in them.

Q184 Lord Richard: What I do not quite understand – and I would be grateful to hear the explanation – is who decides what you actually do?

Dr Helmbrecht: It is a process. On the one hand it is the expertise of ENISA. The second step is that we discuss it with the community. This is on the one hand the Permanent Stakeholder Group, which has expertise of sectors of the private sector – such as the banking sector, the IT sector; the universities - so the representatives who say where the technology is going, for example. So this is a discussion when in the end topics and priorities are set and then because this is also discussed with the Management Board, it is then discussed with the Member States and with the Commission. So there is a picture where this whole group then says, “These are the topics we should address for the next years.” Currently we have a three-year plan, so at the beginning of the year we discuss it for the next year and by this process we try to cover all interests, all aspects from the political level to the technical level.

Mr Beale: If I may, there is a final formal written approval of the work programme and the budget by the Management Board. So there is a formal process of approval there.

Q185 Lord Richard: That is only twice a year, is it not?

Dr Helmbrecht: At the beginning of the year we start with the process; in March we have the first Management Board meeting and this is the first discussion. Then we have in the middle of the year a discussion between the Management Board and the Permanent Stakeholder Group; then in October it is the final approval of the work package and the annual budget and by this you have the process involving other people and the formal decision by the Management Board.

Q186 Lord Richard: I am sure it is my fault and I am trying to not get entangled in bureaucratic spaghetti, if you follow me, because there are an awful lot of strands in this, but really what I would like to know is who takes the actual decision as to what the work is going to be? If something is happening rather more quickly than others you cannot let it emerge from a 12-month process?

Dr Helmbrecht: Of course, as something which is my responsibility, I will say that there are certain topics I believe are important, from my experience and from my discussion with the Member States and with the industry. Of course I will try to put these issues on the table and then to discuss them and push them forward. On the other hand, if something comes up like a threat or something where we have to act in the short term, I am able in these circumstances to decide to remove resources and say that this project is done on a longer timescale and we have to do this; this is management through shifting resources. And if it affects something in detail I can always discuss it with the Chair of the Management Board and the whole Management Board. So, if it is; in the short term, it is a direct communication with the Chairman and an ongoing discussion, it is a usual management way to set varying priorities.

Q187 Lord Hannay of Chiswick: That is very helpful. So if I am right the stakeholder forum is purely advisory and has no decision-making or executive function. The Management Board, which has one representative from each Member State and three from the Commission, takes decisions but within the mandate that has been set for ENISA. How would you change that mandate? If you wished to make some really radical changes what would be the body that would change it? Secondly – and this is probably a bit more difficult really and it is not a question only to ENISA – are we not reaching a point where the management structures that involve representatives of 27 Member States and three representatives of the Commission are becoming hopelessly unwieldy? No university in this country is now allowed to have a council which is as big as that on the grounds that it is utterly ineffective when you get as big as that. I understand how the European Union has got where it has got to, but at some stage it is surely going to have to re-think these structures because they are going to become unworkable?

Dr Helmbrecht: I will first answer the question about the mandate. It is not the task of ENISA to talk about the mandate; this is a political process and a political decision. This

starts in the Commission, then as a Communication of the Commission you have the co-decision process between Council and Parliament, so this is the way the mandate can change. ENISA has a limited mandate until March 2012 and this discussion starts now and this will be starting officially in the next half year probably. So this is where there can be some informal discussion, of course, but the basic procedure is the way I have just told you.

Q188 Lord Hannay of Chiswick: The Council of Ministers – which Council would it be that would take the decision?

Dr Helmbrecht: Within the telecommunication working group?

Q189 Lord Hannay of Chiswick: Yes.

Dr Helmbrecht: If you talk about the Management Board of course it is a challenge if you have 30 people, but it is a question of how you do it in daily work. One way is that there is a close connection between the Executive Director and the Chairman; so this means that if something has to be discussed in the short term, it is no problem today to pick up the phone or to have an email or to have a discussion. Then what happens is that usually you have Member States who are interested in different topics – because the IT security level is very different in Europe – and you have other Member States who do not put so much effort into it, so in the end it usually turns out that there are some active groups and some who are just following what is the mainstream. My approach is to have discussions with the board members, get the interest of the Member States and if you do this over time you get an impression of where there is a compromise to be found or where there are some challenges to face. Then if you prepare – and I think this is important – a Management Board meeting with a tough agenda with information beforehand you can challenge this.

Q190 Lord Hodgson of Astley Abbotts: I think you said that in October of each year you came to a conclusion of what will be next year's work programme. I do not have a record – I apologise if I missed it – of what is on your programme for 2010. What are your key tasks for 2010? Perhaps at the same time what are you looking at for 2011 and 2012 since you take a three years view?

Dr Helmbrecht: If we look at 2010 we have in our work programme some tasks which I will mention in a second, which we started and will then finish, and we have some new work packages – we call it preparatory actions – which start next year. So, we have done a lot of work on the topic of network resilience. Due to the Commission Communication on Critical Infrastructure Protection – CIIP – we are also concentrating on the resilience framework within the CIIP. Then we have our support of the Member States building up CERTs; then we have our risk assessment in this area. So these are some main programmes we are running, which we will continue. And we start a new activity on identity and trust and this is to start in the next year. So these are the main topics.

Q191 Baroness Billingham: I just wondered if you have any direct links at all with the Member States of the European Parliament or do you always work through other agencies?

Dr Helmbrecht: If you talk about the European Parliament there is the so-called ITRE Committee. This is a Committee which on one hand has to approve the election of the Executive Director and on the other hand it is a committee where ENISA has a chance to present itself. I am accountable for the financial aspects to the European Parliament. On the other hand, it is on an ad hoc basis if there are any other engagements with the European Parliament.

Q192 Chairman: How often does the Chairman of the Management Committee change?

Dr Helmbrecht: I do not know this off the top of my head but currently it is Professor Posch from Austria and I think he has been doing it now for one and a half, two years and will do it until next year.

Q193 Chairman: This Committee has had problems in the past with various European organisations where the chairmanship of the management committees changes much too quickly and the person doing it hardly gets a chance to get their feet under the table. Do you find that the Chairman of the Management Committee has enough time to really get to understand the problems?

Dr Helmbrecht: I think in this case for ENISA currently we are very lucky because on the one hand the Chairman, Professor Posch, has done it for some time and does it also in this, let us say, transition phase with a new Director. Secondly, he is the Chief Information Officer of the Austrian Government so he knows his topic and this means that not only on a political level but also on a technical level there is an information exchange and because he is involved in a lot of other European topics I think for ENISA it provides for good communication with the Chairman.

Q194 Baroness Garden of Frognal: You mentioned in a reply to an earlier question that you were looking to resilience and to critical national infrastructure and we understand from previous witnesses that those used to be off limits for ENISA. So has that change been successful, incorporating those into your work, or is it too early to tell?

Dr Helmbrecht: The answer is basically yes. I think that the challenge for ENISA in the starting phase was that it was being built up in 2004; you had to recruit people and it takes some time to get familiar with the organisation before you can really work. I think this was a challenge also for the former Director. Then the question always is, if you look at the European level have you understood the interests of the Member States and also the limits of

the Member States? Then if you look at the regulation it is something where you then have to look at what are the tasks and to put the tasks in to deliver. So if you look to the general discussion about critical infrastructure over the last years in Europe there have been some discussions in the past but on the European level it took some time really to be aware of how to put this into a co-operational level in the European Union. So when the European Commission then made this communication of CIIP ENISA was prepared to take up this task and we are lucky that it fits into our skills, our work packages that we can address, and that if we do something in this area we can be successful.

Q195 Baroness Garden of Frognal: So it was not a policy decision as such; you are saying that it was a timing and administrative decision that you did not take it on initially but you then broadened your remit?

Dr Helmbrecht: Yes. I would say that sometimes when you look at this discussion it is always a question of what is in the interests of the Member States and when do you pick this up on a European level.

Mr Beale: If I may, I also think that it is a trust issue; that ENISA had reached the point where trust had been built with the member countries and the Commission. If I could just say from my past experience at the CBI when the discussions about setting up ENISA were going on we were concerned and we did not want a European agency getting involved in national security issues. That was appropriate for Member States; we did not think it was appropriate that at the European level the competence existed there. ENISA did not do that; it did not try getting into areas where it would not be helpful. So I think the fact that it was asked to take on this work in resilience was actually a compliment and showed that there was that trust, and I think that the results since then have shown that that trust was well-deserved. I hope I am not breaking a confidentiality issue but we were just at CPNI before we came here and they

said that some of those materials generated by that work they were finding very useful. So, so far so good.

Q196 Lord Harrison: I thought I would ask my own question first and go back, if I may, because I think we are touching on areas in this way. Good morning, gentlemen. I have read the written evidence that you have presented where you say that the clearest framework yet for enabling Europe to act in the case of major disruptions has been clarified, but you realise that the practical implementation of this framework has still to be identified and refined and that this area of good practice is where ENISA fits in and plays an active role. I am wondering whether you would like – and I know that you have already said, Dr Helmbrecht, that you resist commenting on the mandate that you presently have – to see ENISA tackling a wider range of issues and would you like to see a change of role perhaps involving more operational issues. It seems to me from both what you and Mr Beale have been saying that you are straining at the bit here; that there are opportunities and opportunities that whilst they may well be a matter of trust that you do not trespass into that area, nevertheless seem to be an open goal, as it were, for ENISA to become more involved, more active and to help the ultimate aims of yourselves and of what the European Union would want.

Dr Helmbrecht: When we look at the current mandate of ENISA it was written and decided in 2003. So from this time on we have two basic developments; one is that we had the enlargement, so we now have the chance to involve new Member States and help them to improve IT security in general. The other thing that we have is the Lisbon Treaty since December now, which also gives some opportunity for the future. The basic point I want to make is that when we from the ENISA side look at IT security, it is first prevention – IT security is something that is needed in society today – and how can we put IT security into e-commerce, e-government and all that we are doing here. On the other hand, this is tied to the smooth working of the European market. So what I want to say is that when I look at this

from ENISA's perspective, even with the current mandate there is enough to do. And to look at how can we improve IT security on the internet if we have electronic communication? We need a lot of awareness and education of how to be competitive in Europe with our IT industry or industry in general, looking to other areas like Asia or the United States. If you look from this industry, from the private/public sector, which affects our everyday life, this is something where we have – if we do it in the right way in the interpretation of the mandate – a lot of possibilities. It means that where we can have our priorities, that we need to be sure they really add value for us before we start the discussion of how much to extend the mandate of ENISA, which in my view should be a long term discussion. Because, if you talk about operational things, it is sometimes a little bit of interpretation. For example, the department where we do most of our formal Work Programme activity is carried out now, we call an operational department, in contrast to where we do our administrative tasks. But if you talk about operational things like doing 24 hours, seven days a week, 365 days a year, running a CERT, then you will need some other resources, for example. So, what I mean by this is IT security is so big that I want to concentrate with our limited resources on the priority, on the European Common Market.

Q197 Lord Harrison: There could come a time where you outgrow that original mandate and it could be useful by expanding that mandate, but at the moment you are curbed by resources. This area of good practice is where ENISA fits in and plays an active role – active in the sense of promoting what can be done – in promoting good practice, and then already you are beginning to change the mandate, are you not?

Dr Helmbrecht: Yes. I see it currently as a situation where for me as a Director I wear two hats. One is that I am responsible for running this Agency and with these resources for the next year, doing the best for you all. On the other hand, of course, I am someone who wants to stimulate the discussion about the future of IT security in Europe with different aspects. To

give you one example, a concrete example: currently we do not have a connection with law enforcement and I would not talk about ENISA being involved in law enforcement currently, so there is a clear red line. You had another question about NATO and it is also clear that ENISA is not involved in any NATO topics – there is a clear border. But if you, for example, look today at threats on the internet, you have different laws in different Member States and it is difficult if you have a botnet if somebody is abroad attacking some country in Europe, so we need in the future some improvement in international law and IT security. This is something where I would stimulate the discussion but for the moment I would keep ENISA out of this role to have a strict reduction to the mandate.

Q198 Lord Harrison: Before I come to the NATO question perhaps I could ask Mr Beale, who laid great emphasis on his CBI perspective when he was there that trust was of the essence that ENISA did not outgrow its role. Are you at one with Dr Helmbrecht on this, that there may have to be change to reflect changing circumstances?

Mr Beale: Yes, I think there will be and there are changes. One of the reasons why I certainly went to ENISA was because I felt that I had been working on these issues here in the UK but that a lot of the areas that needed to be addressed increasingly were at the European level; so that generated my interest and I felt that ENISA had an important role to play there. I should just say, though, that one of the things that I learned at the CBI – it is a similar thing that we are debating at ENISA – is just because there is a problem that needs to be addressed you should not try to be the ones to address all the aspects of it. It is a matter of learning to identify who the key partners are and to working with them. We had to do that at the CBI – there were many problems our members had and we had to identify who in our membership could make the difference and help them to work with others. In many cases that is what we are doing at ENISA. Dr Helmbrecht referred earlier to the way that there are certain leading Member countries. Part of my responsibility as Head of Stakeholder Relations is to identify

who in the private sector - and which countries - have the lead, have the ideas, can help set the agenda and to work with them so that they can, rather than ENISA, try to do more of what is needed than we can be ourselves. The question about the mandate comes in where, in that architecture of all actors being active, should ENISA play a role - and I think that Dr Helmbrecht outlined the key issues of concern in terms of what that debate should be about.

Q199 Lord Harrison: Dr Helmbrecht, you have partly answered the next question: do you liaise with NATO or indeed other military groups? Under the main question, do your plans involve the engagement and encouragement of defences against cyber warfare?

Dr Helmbrecht: As I said, ENISA will not be involved in NATO topics. On the other hand I want to stress that with the problem or challenge of the internet you have the same technology and the same tools that you use in the private area and in the military area. This means that from my perspective there should be approaches in the Member States and if the Member States look from their national security at how they deal with things then they have to find solutions. Then of course there must be, for example, from a NATO level also some solution for this; but, as I said before, for ENISA we can deliver best practice and we can deliver information and if you read our reports where we discuss technology evolution, impact of technology and threat analysis, these things of course can be used by other stakeholders in other areas.

Q200 Lord Hannay of Chiswick: Could I just follow that up. I understand and respect what you say about the red line and NATO but it is of course a self-imposed red line by the European Union and it does sound to me from your reply that it is a bit of an inhibition to have two organisations – the EU through ENISA and NATO – with a very big overlap in membership, and given that there is a similarity between cyber warfare manifestations originating from States and those originating from criminals or the private sector, that this red

line in the longer term is a bit of an inhibition to the sort of co-operation that there ought to be between a European institution and NATO. Is that not something that Lisbon will help to address that can be reduced as a red line, or is it absolutely un-crossable and something that is going to govern your work for the foreseeable future?

Dr Helmbrecht: I think we should look from the responsibility point of view. For example, if you talk about military threats you have national structures. Also, if you look for IT security you have a lot of Member States – let us just say the old Member States or big Member States – who have experience with this, which have agencies, and so you have established structures there. Also in other sectors you have found ways of how to work together with different sectors and government, private sector, military and so on. So if you put this on the European level the question is: what responsibility do you want to put into a European agency like ENISA? Of course I agree that if we now have the Lisbon Treaty that it must be a political question – what do you want with such an agency - and we can also participate in this discussion from the technical input. But in the end it is a question of what do you want to have here and I think that if you look at other cases, for example at telecommunication, at internet service providers, if you talk about vendors producing IT products you are talking about a huge amount of area where as a daily business what we are doing is faced with, let us say, the classical threats of the internet like botnets, Trojan horses, phishing, getting money off other people - so a lot of things which in this area are not connected to what are NATO topics. Of course, on the other hand we have to have some kind of information exchange but this can be on another level which must not be something that you put in a mandate with responsibility. If you talk about responsibility and you talk about how to run the European Market, how to have things involved also as they do it with other sectors, then it is an approach where you can keep this line and say that this is national responsibility, this is European responsibility and this we put to ENISA.

Q201 Chairman: Can I pursue the NATO side of this. I am sure you are aware that NATO is an organisation which is prepared to come to the aid of a stricken nation if they request it in the event of a major terrorist attack or a major natural disaster. Each year they have an exercise. I attended one some years ago in Croatia where they had a simulated hijack, a simulated biological attack, a simulated earthquake, a simulated major oil spill and a major transportation breakdown. They are having another one in September in Armenia. They have them each year and they are very well attended – not just military – particularly with civilian aid organisations and emergency services coming from countries right across the NATO alliance. I ought to know but I do not know whether they have ever had a simulated cyber attack, but I would be very surprised if they have not. For instance, they have had a simulated dirty bomb. I feel sure at some time they will have had or will have in the future a simulated cyber attack. Have you ever been approached or involved in taking part, even as observers, in those exercises; and, if not, do you think that it would be worthwhile if you were involved, even as observers, because there are quite a lot of observers, as I know very well.

Dr Helmbrecht: The answer is we have not been invited or involved in NATO exercises and I think what you are discussing is different when you talk about something that is part of a mandate. If NATO invited ENISA to put their experience on the table, of course this would be no problem. If we discuss this topic we are also talking about exercises in the IT security community; so from the European Commission Communication it is intended, and it is now our work programme, that there should be an exercise in 2010, so what we are preparing is how to do this. But if you talk about exercises I know that the military community has a lot of expertise in how to do exercises, so we do not have to invent the wheel again. This means that of course you can have discussion, exchange information, exchange best practice and experience, but, on the other hand – and I think this is the question that you raised – if you talk about crisis management, if something happens, how to react, this is not something

different from what we have to discuss for the future, and how do we want to deal with a civil crisis and military crisis in the future if a significant IT threat was involved. What I want to say is that there are a lot of topics which must be addressed. One is the ENISA mandate, one is our work, one is how to work together. You can use the connections in participating in conferences and exercises but we have to carefully distinguish what we are talking about at this level.

Q202 Lord Dear: Gentlemen, last week when we were taking evidence a witness suggested that in his opinion you had failed to engage with the global security groups that are operated by the internet industry. I wonder whether you would agree with what he said and whether he was right in talking about the organisation way back in the past or even currently and whether you have any plans to extend your activity and your interface with the industry?

Dr Helmbrecht: I can understand this remark because, as I said, ENISA was building up connections and, like Jeremy said, building up trust and building up this community, so what we want to improve in the future is the following. On the one hand we have the so-called Permanent Stakeholder Group; we have members coming out of Europe, so this means that we have on an expert level built up in this community. You have other organisations like the OECD or ICANN for the internet. So this means that we are starting to have a dialogue with them and this means that step by step we will improve this global network. What is also something positive for us is that we get invitations or questions from organisations from abroad, for example from Asia or even other countries, asking us if we could give a presentation of this or that, so we get invitations. This is something that will evolve in the future as ENISA works on these topics and extends its network. Does that answer your question?

Q203 Lord Dear: I am grateful to you for that but in my experience the internet itself is a very fast expanding entity and the industry that supports it has to be very fast as well – one drives the other. So we are talking about something which is changing almost on a daily basis and I wonder whether you are able to work up to a speed where you can interface at the same sort of speed or whether you are constantly, as I understand from your last answer, trying to catch up to something which is disappearing further and further into the distance?

Dr Helmbrecht: My aim is to overtake them. My approach is if you look at the current situation, for example let us take the CERT community, we had to face, as Jeremy said, building up trust so that we are accepted by European organisations like the Trans-European Research and Educational Network Association's CERT Task Force (a part of the FIRST global association) and others, so by being part of this community; and then immediately you have contacts to Asia, the United States and so on, so this is something which spreads out. Of course, on the other hand – and this is what is important for us – to be in contact with the research community and the industry community, so that, for example, I am now able to select a new PSG because it is just in a phase of changing and I am looking for people and I have a lot of applicants who are coming from industry – let us say, for example, companies like Nokia and France Telecom or British companies. So, other companies are participating here and we also have American IT companies with subsidiaries in Europe and this means that my aim is to have a close connection to them so that you can have by this an immediate response – what other technologies are taking place and what threats are coming up. This is something that starts working and so if you have these connections you are aware of their company strategies and what they are doing and thinking and what is changing.

Q204 Lord Dear: You have talked a lot about trust in your evidence so far and I appreciate that because it is the bedrock to most human relationships and organisational relationships, but as I understood you before – and you must correct me if I have got hold of the wrong end

of that stick – the trust I thought you were describing was between Member States within the EU. But I think what you are now talking about is building up trust with the security industry itself and I am surprised to hear you say that because I would have thought that they would have welcomed involvement by an organisation such as your own, representing the whole of Europe, to help them to deal with something which is a burgeoning problem. Am I not seeing the same scenario as you?

Dr Helmbrecht: Yes, but there are maybe two different approaches to what is happening and on two different levels. One is, which Jeremy addressed, that if you talk with Member States about critical infrastructure the question is what is in the interests of a Member State to have under its own responsibility and what to put on a European level? So in this discussion if you have ENISA then you have two levels: one is you have the organisational trust and do you trust that ENISA keeps information confidential and how do you share it? And the other is personal trust. If you talk about CERT topics it is a lot about personal trust, you know each other and to share information. On the other hand, if you then go to industry we did not really until now establish a public/private partnership model. So what we do currently is have projects and have experts and discuss it with them. But the question is, for example, what I want to do – I start it next year – that if we talk about the internet we have to have close co-operation with the telecom providers, with ISPs, to have also some kind of early warning system, technology and other things. So it is not that the industry comes and say, “Hi, there; it is ENISA,” it is something where you have to talk to them because the question is what is the added value from a European perspective for a global acting company. This is something where we are having some discussion and also to have this trust by the industry that they have an added value if we work together with them.

Mr Beale: If I could just add to that and, again, if I can draw from my experience at the CBI? There are a lot of agendas out there in the industry side and there is a difference between

suppliers and users and between the different communities of suppliers and what they are supplying, and I think the value added that ENISA would bring will be to be smart about its agenda and to identify which interests again can work best together and this is particularly pertinent in those public/private partnerships – or models of co-operation is maybe a better term because sometimes PPPs can be a specific legal form. The task is about identifying what the agendas are that are going to bring the actors in so that ENISA is not seen, for instance, as just representing the interests of network operators or software suppliers or business users but a forward-looking agenda which helps each of those entities or those sectors and others move forward on an information security agenda for Europe. That is where we are still, as Dr Helmbrecht has said, engaged in defining the terms in that debate and that is a maturity aspect of our development. We are still a young Agency but I think that the new Permanent Stakeholders Group will be very, very helpful to us in refining that agenda along with the advice from the Member States because the Member States will of course get that lobbying from the industry too.

Q205 Lord Dear: In about a year or two years' time do you think that your organisation will be able to work at the same speed as the internet industry?

Mr Beale: My personal experience from the two months that Dr Helmbrecht has been with ENISA is that we might have overtaken aspects of them too. He is working us very hard!

Dr Helmbrecht: I did not tell him to say that!

Lord Hannay of Chiswick: Could we look at the issue of CERTs now?

Chairman: Just for the record, Computer Emergency Response Teams.

Q206 Lord Hannay of Chiswick: It is like the *Today* programme! The Commission's Communication puts a lot of emphasis on the desirability of setting up national CERTs which would cover more than simply public sector infrastructure. That in a way is slightly different

from the approach that is being followed in this country, as you know, where we have industry-specific, sector-specific and company-specific CERTs. You are presumably doing a lot of work on this; do you regard those two approaches as being mutually inconsistent or do you think that in some countries, perhaps smaller Member States or Member States with a less mature internet industry, a national CERT makes more sense but that in others the sort of approach in the UK makes more sense? Could you perhaps give us some thoughts on that?

Dr Helmbrecht: I think both approaches in the end match together because, as you said, you have small Member States who do not have any CERTs and the question then is how to build it up, and because you have from ENISA's side this connection to the Member States, to the Management Board and other people, you can then build up governmental and national CERTs. But I would also appreciate in support if such Member States would then have academic CERTs and so on. I think it has been shown in the past that sector-specific CERTs work very well because they understand the business. It is different if you have an academic part where you have a lot of students and teachers or if you have an insurance company or a stock brokerage where you need seconds of reactions and you need other procedures of CERT interaction. So if you have sector-specific CERTs and if they interact, as I said, on this trusted communication you can improve it. So it is my approach, wherever we have a structure like a well defined and working structure in the UK, is to take this as best practice and to use it and interconnect it and support the interconnection and support smaller or new Member States to go this way; and in the end if we have CERTs – and this would be my vision – in every sector or every Member State in a trusted communication then we have really improved something.

Q207 Lord Hannay of Chiswick: If I were to take that a little further, setting up a national CERT in a small Member State that does not have a very mature internet industry might be the obvious first step but it would not preclude them subsequently having sector-specific or

company-specific CERTs as they became more sophisticated and as their involvement built up?

Dr Helmbrecht: Yes.

Q208 Lord Mackenzie of Framwellgate: Good morning, gentlemen. Lord Jopling mentioned earlier about simulated cyber attacks and of course a lot of your tasks emanate from EU Communications and large-scale cyber attacks. On the question of resources, do you think you have sufficient resources to do this work and do you expect to deliver on time?

Dr Helmbrecht: For every agency there are never enough resources. The question is if you take the topics and you take the resources how to set priorities. So it is very important to discuss these things, in our case with the Management Board and the responsible stakeholders, as to what priorities we want to put into our work programme. I can say that for 2009 we delivered all on time. Of course, we have a tough work programme for 2010 and, as was mentioned before, if something comes up it is always a management challenge then to move resources. I think if you connect it to our current situation for 2010 and 2011 this is what we can foresee, by setting the priorities and discussing this. From the Member State perspective you know what we can do and this is where we can also say that with our resources we can reach these goals. What I currently do is to optimise the processes within the Agency and to get resources from the administrative area module and operational area, but in the end it will be discussion. As I mentioned before, if you talk about this new process of the mandate it is then your decision of how much resources you give ENISA because I am well aware that in the end it is the citizens who pay taxes.

Q209 Lord Mackenzie of Framwellgate: Just to follow that up, you mentioned that it was a management challenge to move resources around but if there was a surge of demand, for

whatever reason, do you have the mechanism for actually increasing resources, even on the short term?

Dr Helmbrecht: It is limited of course but we have a part of our budget which we have for projects and which we can use for contract agents.

Q210 Lord Mackenzie of Framwellgate: Like a contingency fund of some kind.

Dr Helmbrecht: It is not in this way that there is some reserve in the Agency but it would depend on the stage of the year. If it is in the early stage of the year I can always decide and say that if there is something really urgent we can do this in this way. On the other hand, if it is at a later stage of the year I would go another way and say is there some support of some Member State or some company with resources, because also in this community sometimes it may be an advantage for somebody in the private sector where you can say, “Could you also help us on this topic?” So there may be ways out if it really gets very critical.

Q211 Lord Hodgson of Astley Abbots: You are looking at the challenges of a virtual industry – a virtual and fast moving industry, as Lord Dear reminds us. I note that in your evidence you said some very nice words about the Greek Government’s generosity in the facilities in Heraklion. Could you say something about the challenges that you have in recruiting people (a) who can be at the leading edge of the developments which were the subject of Lord Dear’s question; and (b) whether the fact that it is based in Crete assists or detracts from that ability to recruit?

Dr Helmbrecht: It is not a black and white question, of course. If you decide that European agencies are spread around Europe then it is the responsibility of the Member States to define the seat and I appreciate all that the Greek authorities do in this regard. But, of course, there are some challenges. Most of the burden is taken by the employees because it means travelling for them and travelling always means for a mission here because you can never do

it on one day. On the other hand it is currently a difficult situation for families with children because you do not have a well established European School in Heraklion, so if you have parents with children from the ages of, say, 12 to 18 it is nearly impossible currently. This means for some employees the family situation is difficult, but this does not mean that it is difficult in general because we get a lot of applications for vacancy notices – although it is not really spread around Europe on the whole. We get a lot of skills from the public and private sector, so it is not a problem if we have a vacancy notice to get somebody there. But in the end you get, as I said before, a limited social mix in such an agency.

Q212 Lord Hannay of Chiswick: Could you elaborate slightly on this? When you advertise your vacant posts are you getting the same sort of uptake that you would expect if you were, let us say, in Frankfurt or London or somewhere like that? Or are you really being inhibited by the fact of the geographical situation of the Agency? Are you achieving the retention period that you need if you are to have professional people who understand their jobs really well, or is the fact that the Agency is situated in a place where it is quite difficult to get to and from and that there is not a European School, and so on, is causing problems both of retention and of recruitment? It would be helpful to have an idea as to that. What we were struck by when we looked at the origins of ENISA was that it was rather odd that Greece was allocated ENISA but was then left to choose whereabouts in Greece it should put ENISA. The normal practice, from my own experience, is that the bid of a country for an agency like this should be accompanied by a proper analysis of the place that they were offering to put it and its ability to help on these things like recruitment and retention.

Dr Helmbrecht: If you discuss this topic there are always some points of advantages and disadvantages and in a second I can give you an advantage of the location. The basic point I want to make is that this is not only a question that challenges ENISA, it challenges also some other European agencies, but in the end if you put this Agency somewhere else in Europe you

would always have travelling and you would have this discussion. So if you go deeper into this discussion it becomes difficult because in the end you would say that every agency should be in Brussels and maybe this solution could also be questioned. So from the principal approach it has some different aspects. You have an advantage if you look at Heraklion that you have a big university campus; you have a research institute called FORTH, which is working on computer science and intelligence and other things, so this is something, from a technology point of view when you are looking where is the technology going, something which is an advantage for ENISA. The other thing is of course that if you look in the end – and this has to be discussed honestly – at somebody who has worked in London and then goes to Heraklion and he is in the situation that he has two children and a wife then it becomes a problem if the wife does not get a job there immediately because of the situation. The point I want to make is that we get staff – that is not a problem; we get enough applicants for vacancy notices that we can choose high quality; we get it from government and we get it from industry, so this is not the problem. But, in the end, if somebody says, “I want to have this one in this family situation” then it is not possible because they will not come.

Mr Beale: If I may add something here? It is also in many senses the agenda that an organisation has that attracts people. They will put up with lots of things if it is an exciting, dynamic, important place to work. I think it is over the last 18 months that three British people have joined ENISA to work there where previously there were none; and there is a reason for that. As I mentioned for myself, it was because I felt that a lot of the issues were becoming important and – and he is too modest to say – that Dr Helmbrecht, who was President of the German BSI before, has also come to work there. There is no inherent barrier where ENISA is to attracting high-calibre candidates, if I could be so bold as to put myself under that umbrella. The key thing becomes about how you work and what you do - and that is really the focus of our efforts: it is now on improving our interaction with our stakeholders

and being more at the centre of the debate. We have also opened a branch office in Athens with the support of the Greek Government so that we can hold meetings there that will make it easier for the people we interact with to come and participate and, as Dr Helmbrecht mentioned earlier I do believe, we also hold meetings in Brussels, in Vienna, in Madrid, in Paris and we have held one in London too. So we can be flexible and I think that is the more important thing – not getting trapped as a result of where we are.

Q213 Lord Hodgson of Astley Abbotts: I heard you say that of course it is people with young families where the major problem is. In my experience this is a young person's industry and it is young people, people who will have families who are going to be leading the charge on taking the industry forward; they are the people who have the mental agility and the intellect. So it does seem to me that there is quite a disadvantage if young people with families do not want to go to Heraklion for the reasons that you have identified. Could you just confirm that all the 65 of your staff are based in Heraklion? And it would really help me greatly if you could tell me how many nights the two of you spend in Crete each year?

Dr Helmbrecht: I can give you the figures, of course, but not in detail. I can give you an approximation. I can say that for young families, if it is kindergarten and the first years at school it is possible; so now it is an evaluation to say that if you have parents aged up to 35/40 years it is not a problem if the wife does not work. But then it becomes a problem if the parents are between 40 and 50 years old because then you have this family situation which makes it difficult. On the other hand, all staff live on Crete because it is a condition, if you sign your contract, that you move there. Of course you can fly back and forth when you want. What happens in some cases is that the man or the wife who works for the Agency lives on Crete and the family does not live on Crete – we have some examples of this – because of the situation, and this then makes it difficult for those parents who are let us say 45 years old. But if you want to have the figures I can give them to you in detail.

Q214 Lord Dear: Gentlemen, this is more of a statement I suppose rather than a question. I remain uncertain of the validity of what you have told us, from my perspective. Let me tell you where I am coming from. I think if we were looking into some deep-rooted problem in the motor industry we would be surprised to find if any EU Commission set up to deal with that was not located in the Ruhr or in Turin or some other centre of motor manufacturing. Similarly, this is a global problem and if it is being approached in a global way I think we would be surprised not to find the international organisation located in Silicon Valley in California or in Cambridge, UK. I speak as the Chairman of a high-tech company, which is located in Guildford, and much as it would cost us money to relocate we are seriously thinking of relocating to Cambridge because that is where the centre of excellence is for high-tech in this country, and that is quite a short move. I am surprised – and this is what I want to put on record – that we are talking about something which is as fast moving and internationalised as the cyber problem and the location that you have has been chosen in the way that it has. I would have thought that there must be a great difficulty – although you tell us that there is not – in attracting and relating on a daily basis face-to-face with the sort of people who are up to speed with the problems, and how that can be done from the fringes of the EU with no huge tradition of dealing with these sorts of problems still defeats me. That is more of a statement than anything but I wonder if you would like to respond to it.

Dr Helmbrecht: One remark to this is what we can improve in the future using the technology really in a daily way in which we are dealing with internet security. For example, if you have a video conference system, if you have some kind of tailored working this may reduce some of the difficulties in the future. On the other hand, if you are looking to the industry it is an industry where you have, at least in Europe, too much dependency on plant locations. Of course, I follow your argument that if you look around Europe where do you have the IT industry but this means in the end that it is more of a community that we are

dealing with, to say “Where do we meet?” So for us it is more an issue of saying we have this community of experts, of working programmes and we come together with the Management Board, with the PSG and we are doing our projects and we are running our exercises and we are doing this, as Jeremy said, in different countries of Europe – wherever is most appropriate for that body or project. So we meet this challenge today by saying that we look to have the right place for where we are working together at any one time or on any one issue in the Community. The other thing is what we have talked about before – the location for the staff. So it is more a challenge for the staff and not for the everyday working for the future.

Q215 Chairman: I want to move a shift on this question, from those who work for the Agency to those who have to visit it. From which European hubs can you fly to Crete, apart from Athens? I am asking where are the direct flights to Crete from European hubs, capitals if you like, besides Athens.

Dr Helmbrecht: From most European main cities you have direct flights to Greece, to Thessaloniki and Athens. In the summer you have flights to Heraklion. This is during the tourist season from about March/April to October, so you can have direct flights by the different companies which bring tourists to the island.

Q216 Chairman: Most of those will be charter flights, will they not?

Dr Helmbrecht: Yes, most of them are of course charter flights.

Q217 Chairman: Do I take it from your answer that it is only really from Athens that there are regular direct flights?

Dr Helmbrecht: Yes.

Q218 Chairman: How many flights a day are there into Crete to and from Athens?

Dr Helmbrecht: I do not know but I can give you a typical example. When we go back to Heraklion in a typical way we leave London in late evening, have a flight to Athens and stay overnight at Athens Airport and take the first flight on Thursday morning. So that is the typical way that you go from Brussels, Frankfurt, Paris or whatever in the evening and have an overnight stay. On the other hand if it is a question that you have a meeting early in the morning then it is the same the other way round; or if you have a late morning meeting sometimes you can take the first flight from Heraklion and then be here another time. So it depends a little bit on the time schedule but let us say for a one-day meeting you need to spend two nights.

Q219 Chairman: My question was how many flights a day are there regularly between Athens and Crete?

Mr Beale: I do not know the exact number but there are numerous flights during the day from which one can select to go either to or from Heraklion to Athens or back.

Dr Helmbrecht: For this afternoon there are three flights to Athens from London, for example.

Q220 Chairman: I am not interested in London to Athens – that is the normal thing. What I am concerned about is Athens to Crete.

Dr Helmbrecht: Athens to Crete, in the summer it is nearly an hourly basis; in winter time it is Olympic and Aegean so you have some flights in the morning, some flights in the afternoon and late evening, so there are a number of flights.

Q221 Chairman: Let me take this a little further. I think the Committee was not aware that you had an arrangement in Athens where you could have meetings there, but if you cannot tell us straight out could you give us supplementary evidence of, say, over the last year how many

visits have you had for meetings from outside visitors who are not employed by the Agency? It is this matter of the inconvenience of getting to Crete that we are not clear about and it would be helpful if we knew how many people a year come to visit you. Could you give us that information?

Dr Helmbrecht: I can give it – I apologise not now. The basic information is that the Athens office, which is paid for by the Greek Government, we have had since the autumn of this year. We did not have it before; so the last five years it has really meant meetings in Heraklion or meetings at other places in Europe.

Mr Beale: What you are getting at, I think – and I can point out another aspect of it - when I go to get a flight from Heraklion to Athens in the winter I only need to leave the office about half an hour to get to the airport and through to the departure gate. If I need to go to Heathrow from many places in London I need to give it an hour, and at Heathrow I may need to give a good hour to get through check in and security. There are certainly drawbacks but there are benefits of being in a quiet airport during the winter.

Q222 Chairman: What I am thinking about is the inconvenience of people visiting you for meetings and business, who have to spend probably an extra night getting to Crete and an extra night getting back. It sounds like two nights in Athens, which is highly inconvenient and expensive, and what I am trying to get at is how big is this problem? And one can only assess how big the problem is if we get some sort of an idea how many people are affected by this, because it seems that the most highly inconvenient way of setting up an agency is if people have to spend a night on the way back. But if you could give us some idea of your experience since you set up the Athens office – was that July?

Mr Beale: That was this autumn. In fact, literally about a month ago, two months ago it was first opened. We have not had any major meetings since then in there; we have had meetings of various expert groups in the Athens office – two so far since it opened – but next year we

will be holding the Management Board meeting there, and possibly the Permanent Stakeholders Group meeting there, twice-yearly for both of those.

Chairman: That sounds a good start.

Lord Hannay of Chiswick: Presumably – it is perhaps a little unfair to say this – the actual decision to open the Athens office simply validates all the questions that the Chairman has been putting to you.

Chairman: Exactly.

Q223 Lord Hannay of Chiswick: Because under normal circumstances it would not be a very useful application of resources to have an office in Athens which is simply there in order to provide meeting rooms. But clearly the pressure from people who do not particularly like spending the two nights that going to Heraklion necessitates has led to this decision. So it is a kind of sticking plaster decision to what I can only suggest was a somewhat hasty decision in the first place as to the siting of the Agency.

Dr Helmbrecht: If I can make a remark. We tried to avoid this problem in the past by having meetings somewhere else in Europe.

Q224 Lord Hannay of Chiswick: But then that is inconvenient for the staff of the Agency because they have to be absent for substantial amounts of time.

Dr Helmbrecht: Then it is some kind of customer orientation to say that we take the burden.

Q225 Lord Hodgson of Astley Abbots: I think this point has been largely covered but it is not only the time wasted of visitors, it is the time wasted of valuable senior staff going to Athens or going somewhere else. When you give the additional evidence could you tell us what time would you would have to leave your office in Heraklion to attend the meeting at 10

o'clock this morning, if you had flown straight from Heraklion? You would obviously have to overnight somewhere but what was the latest time you could have left your office?

Dr Helmbrecht: I have to think because I came from Paris last night. As Jeremy said, it is a very short way to the airport; it is very easy to board; it is a 50-minute flight. So sometimes if you take the time to go there, if you have a big city and you have to go through the traffic, it can take longer in the end. I can tell you the other way around because I know that when I leave this evening I will be in the office tomorrow at about 10 o'clock.

Q226 Chairman: I think we have covered the ground and made the point. Thank you very much for coming; you have come a very long way.

Mr Beale: It was no problem!

Chairman: We very much appreciate the evidence you have given us and, as I said at the beginning, if you wish to expand upon it we would be most obliged if you would let us know as soon as possible. Thank you very much, that concludes the meeting.