HOUSE OF COMMONS

Home Affairs Committee

Oral evidence: Counter-terrorism in Europe, HC 933

Tuesday 13 January 2015

Ordered by the House of Commons to be published on 13 January 2015.

Watch the meeting

Members present: Keith Vaz (Chair); Nicola Blackwood, Mr James Clappison, Michael Ellis, Paul Flynn, Dr Julian Huppert, Tim Loughton, Mr David Winnick.

Questions 1 – 44

Witness: **Rob Wainwright**, Director General, Europol, gave evidence.

Q1 Chair: Could I welcome to the dais Rob Wainright, the Director of Europol? Thank you, Mr Wainright, for coming at short notice to talk to the Committee. This is part of the Committee's ongoing scrutiny of Government policy as far as counter-terrorism is concerned. The appalling attacks in Paris last week have highlighted the necessity to look at issues concerning counter-terrorism. I have visited Europol and other members of the Committee may have done so, but perhaps it would be helpful if you could set out briefly Europol's role in dealing with counter-terrorism issues because one of the things the Committee has noted, especially in our last report, is the lack of an international platform to deal with counter-terrorism.

> ***Rob Wainwright***: Thank you, Mr Chairman, for inviting me here today. As you will have seen from your visit to Europol we have some unique capabilities to help police security services around Europe to deal with a range of security threats relating to organised crime and cybercrime but also terrorism. In recent years, accelerated perhaps in recent months and certainly by the events of Paris last week, we are seeking to maximise those capabilities to help in regard to countering terrorism. These are principally about maintaining unique intelligence exchange capabilities, databases that can manage sensitive intelligence on a cross-European basis in order that we can identify important intelligence links between suspects as they move around Europe and, indeed, beyond Europe; and counter-terrorist experts who can interrogate that data, make sense of it and help national agencies to deal with the operational follow-up. We have experts on terrorist financing. We have experts who monitor the internet, jihadist websites in particular, and can allow us therefore to track potential alarming developments and so on. Europol is a hub for intelligence exchange and operational co-ordination across 28 member states and, indeed, many more that are now actively members of our organisation.

Q2 Chair: We appreciate the work that you and members of your team do. For those of us who went to see how you actually operate, it was very impressive. The threat at the moment to the United Kingdom is set at severe, one less than critical, which means an attack is highly likely. There are different threat levels in different countries. Does Europol have any role to play in looking at the overall threat to Europe, or is this still something done by national Governments? Do you have any input into a much wider canvass than, for example, the UK Government?

Rob Wainwright: We do not have a formal role in helping each member state to set its threat level but we inform the assessment that goes into setting those levels. In particular, we use our unique intelligence capabilities to help to paint a picture of what the threat looks like across Europe.

Q3 Chair: If you were defining a threat to Europe as a whole, what would it be?

Rob Wainwright: I hesitate to use any particular terminology because it could be misleading but to put it into context it is certainly the most serious terrorist threat Europe has faced since 9/11, for example. It is important that in the period since that major attack there have been significant developments in both the scale and variation of that threat away from what we had at the time—a network perhaps directed by an al-Qaeda core leadership—to something now that is much more diffuse in nature, a decentralised network of thousands of independent and semi-independent actors, many of whom have been radicalised on the internet and by engagement in conflict in Syria and Iraq. Many of those are European nationals who have since returned to their home countries to pose a latent threat there.

Q4 Chair: Indeed. In respect of that, I think some of us were surprised. This is all newspaper articles so if I am wrong, please do not hesitate to correct me. The two brothers involved, the Kouachi brothers, were apparently on a no-fly list that the Americans had. Would that information automatically go to the French Government? Would Europol be aware of it? Do you do any tracking of individuals who enter the European Union as opposed to the tracking of individuals in particular countries?

Rob Wainwright: We are aware of some of the intelligence antecedents of the members of that organisation from our participation with the French authorities over the last 10 years. We are not automatically informed, for example, by the US authorities of those on the no-fly list.

Q5 Chair: Would you like to be? Would Europol like to have the capability of knowing who is on a no-fly list?

Rob Wainwright: I think, Mr Chairman, the point is that the scale of this threat, dealing with multiple thousands, and the way in which it involves so many different countries, means that we have to, to a certain extent, have some centralised intelligence capability to help the national authorities.

Chair: Yes.

Rob Wainwright: So, yes, it makes sense for certain capabilities that are maintained by the UK, the United States and other friendly countries to be shared and systematically interrogated through the databases that we have so that we can help to identify those intelligence capabilities.

Q6 Chair: One aspect of the attack on *Charlie Hebdo* was that two of the people concerned had travelled to Yemen where they had received training. I have just spoken to the Yemeni ambassador because I wanted to know whether there was a way in which the Yemeni authorities could alert the British authorities or, indeed, the French authorities, because all European nationals need a visa to go to Yemen. That is the way they get into the country. Although there are no direct flights from London to Sana'a, they go via Dubai or some other place. He told me that last year 3,200 British nationals travelled to Yemen. It must be quite easy to get that kind of information given by the Yemeni authorities, who are on our side, back to people like yourselves and national Governments. It is not big ask, is it, when people travel to Yemen and you do not know what they are doing there?

Rob Wainwright: It should be possible. In that case we would expect the UK or another EU member state to channel that information to Europol. We would not get it directly from Yemen necessarily, but it should not be difficult, I agree with you.

It is an interesting point you raise because it illustrates the fact that the problem that we are dealing with these days is not just about Syria and Iraq; it is also about other conflict zones and other terrorist networks around the world—in Africa and the Arab peninsular, for example—that have franchise movements of the Al-Qaeda brand, if I can call it that. While, quite rightly, security services around Europe have indeed been prioritising their work in dealing with the foreign fighters who are returned from Syria and Iraq, what the events in Paris last week show is that there is also a threat, clearly, from sleeping networks, dormant networks, that suddenly can reawaken.

Q7 Chair: What would you put those figures at? We know the foreign fighters going from the UK was 500. It is 1,000 in France. What would you put the numbers of people at roughly? We know you cannot be specific on a particular figure but roughly what are we talking about?

Rob Wainwright: I think we are talking about 3,000 to 5,000 EU nationals.

Q8 Chair: Who are a threat in some way.

Rob Wainwright: Potentially, yes. We have to be very careful about characterising all of them in that way but clearly we are dealing with a large body of mainly young men that have the potential or the intent, if not the capability, to carry out the attacks that we have seen in Paris last week. Because of that, one of the things that Europol has been focused on since April last year is developing a dedicated intelligence database to deal with this phenomenon of foreign fighters. So far we have collected approximately 2,500 names of suspects from our member states and indeed our other co-operation partners around the world.

Q9 Chair: A final question from me on the internet. When I went to see Europol I was very impressed by the monitoring of internet sites by your officials, who do so in different languages. This is their oxygen of publicity, is it not? This is when they make a threat of seeking to behead someone, as we heard in the internet chatter in our country; whether or not that is something that is correct or not, we do not know. Do you think the internet companies need to do much more at taking down these sites before we ask them to take them down?

Rob Wainwright: I think we all have to do a lot more, frankly, to deal with the cyber dimensions of this and related threats. One of the important evolutions that we are seeing right now in the current terrorist threat is the way in which the internet is used, clearly, much more aggressively and much more imaginatively by the networks. Social media is a recruitment tool and a propaganda tool. I think therefore, yes, you are right; it means that we need to have a closer, more productive relationship between law enforcement and the technological firms, and also the right legislation in place to allow the security authorities to monitor suspected terrorist activity online.

Q10 Mr Winnick: Internet companies are causing much concern, as the Chair has said. One wonders how soon there will be more effective action because if a terrorist used the print media we would know what the outcome and the outcry would be. Do you have much optimism that the need will be recognised by the internet companies if thugs are using them to promote mass murder?

Rob Wainwright: I think many of these tech firms have responded enthusiastically to calls by the British Parliament and other countries and are now working perhaps on a much better level, but the scale of the problem is enormous. The darknet area of the internet, which is home to so much of this criminal and terrorist activity that is being planned, is a huge endeavour to monitor. There has been little appreciation about the scale of the difficulty involved. One of the obvious concerns is that if we effectively invite or expect technological firms to do the work of monitoring rather than doing it ourselves directly, they are working to fundamentally a different imperative—a commercial imperative—which is not necessarily always the same as those that we have in the police community, for example. This is a complex threat and one that so far I do not think has been addressed in the best way in terms of the arrangements between the police and these technological firms.

Q11 Mr Winnick: Mr Wainright, what surprises a lot of people is that the murderers in Paris last week were known to the authorities. They were certainly not law-abiding citizens who have never committed a crime. We know their background. We know that the security authorities in France had taken appropriate action in noting that they were a danger. Then they were taken off the radar, rather like in the case in Britain of 7/7 where they are known to the security authorities and no further action was taken. Are there lessons to be learned, or is it simply impossible, given the numbers involved, for the security authorities to keep a tab on these people?

Rob Wainwright: I think it is really difficult. I would not say impossible. I think it is exceptionally difficult given the scale of the problem right now and the numbers involved for the security authorities to monitor all potential threats. That is the very painful reality that the attacks in Paris show. Do not forget that the French authorities are among the finest and the most well-equipped in countering terrorism. It shows just how difficult it is.

Q12 Mr Winnick: Do you think there are particular racial groups who are most at risk now, be it in France or in Britain? One knows that once the murders were carried out in the magazine offices, where the 12 were slaughtered, an undoubtedly co-ordinated cell decided to go to a Jewish market. Would that have come as any surprise to you?

Rob Wainwright: Well, no.

Mr Winnick: Automatically going to the Jewish market in order to bring about further casualties.

Rob Wainwright: I think the fact that these terrorists sought to target Jewish people and Jewish landmarks, for example, is no great surprise. The last significant attack we had in Europe of a similar nature was against a Jewish centre in Brussels. It is clear that certain sections of the public, and certain places and businesses, are more vulnerable than others. I think that is well accepted by the security authorities around Europe.

Q13 Mr Winnick: There has been a unanimous response, as one would expect, from all decent people regardless of whether they are Muslims, Jews, Christians or anyone else—a loathing and hatred of the mass-murderers. But controversy has occurred yet again despite all that because MI5 quickly came back with the view, which they have expressed many times before, for greater access to communications, what is known as the Snoopers' Charter and the rest of it. Do you feel much purpose is served by bringing up that sort of issue, which is bound to cause controversy but is not likely to be brought about, certainly in this Parliament, as far as Britain is concerned?

Rob Wainwright: I think the security authorities have every right to tell the public and the legislators what they think they need in operational terms effectively to combat the threat. It is for Parliament to decide what the nature of that capability should be. I do, however, think there is a particular challenge that we face in terms of adequately monitoring communications online. There is certainly a significant difference between police capability to lawfully intercept telephone communications and intercepting communications online. I am not sure what the arguments are in following such an inconsistent public policy position.

Mr Winnick: That was not, of course, what the head of MI5 has said; he did not make that distinction that you have just made. Be that as it may.

Q14 Michael Ellis: Mr Wainwright, may I join others in thanking you and your team for the work that you do? *Associated Press* is reporting in the last hour that the police are saying in France that the arms that were used, the automatic AK-47s, came from abroad and they are seeking the source of the funding, which they are describing as outside funding. Is your organisation, Europol, front and centre in assisting the French authorities in ascertaining where the funding came from and the source of those automatic weapons?

Rob Wainwright: I am not sure we are front and centre for a number of reasons. I think the actual engagement that counter-terrorism authorities have with us can still be exploited to a greater extent. Having said that, in response to your specific question, we have been particularly helpful towards the French authorities on the question of terrorist funding in this case. We helped to run a very specific, very helpful programme that allows access to terrorist financing information through co-operation with the United States authorities. In this case, after five urgent requests between us and the US authorities, we were able to give the French authorities about 60 urgent intelligence leads in this case, which has proven to be of help.

Q15 Michael Ellis: This is following the incident.

Rob Wainwright: Indeed.

Michael Ellis: In the hours immediately following the incident.

Rob Wainwright: Indeed.

Q16 Michael Ellis: You are saying that Europol made repeated requests to the United States authorities for information.

Rob Wainwright: Yes.

Q17 Michael Ellis: Were you granted that information?

Rob Wainwright: Yes.

Q18 Michael Ellis: How long did it take before you received that information from New York?

Rob Wainwright: A matter of hours. I think we were able to turn them around in under 24 hours and pass that on to the French authorities.

Q19 Michael Ellis: Having received that information, was it in relation to financing or potential financing?

> ***Rob Wainwright***: That is still to be analysed fully by the French authorities but they were intelligence leads certainly worth exploring further. The full outcome of that I am not aware of yet.

Q20 Michael Ellis: The United States authorities are clearly assisting in providing information where they have it in respect of this inquiry.

> ***Rob Wainwright***: Yes, and I am sure not only in the way that I have described.

Q21 Michael Ellis: As far as communications data is concerned, it has clearly been said repeatedly now by the security and intelligence community that the mechanisms available to the law enforcement authorities in this country have to keep up with technology. At the moment we have a division between the powers available to law enforcement for traditional forms of communication—landline telephones, mobile telephones and post, for example—and more modern forms of communication. To further that point, do you agree with those in the security and intelligence community, and with me for that matter, that we do need to advance our legislation in this area so that we can properly protect ourselves from what you have called the dark places on the internet that terrorists and criminals are using?

> ***Rob Wainwright***: It is reasonable, from my experience, to point out that there is certainly a deficient police capability to monitor communications of serious criminals and terrorists online. We have run now for two years the European Cybercrime Centre that monitors a whole range of significant security threats online, and from the dozens, if not over a hundred, major operations that we have helped to co-ordinate since that time it is quite clear that we have a pressing and, indeed, rising challenge to deal with highly encrypted communications online that are managed through the space of the darknet, which are effectively out of reach of law enforcement authorities—not in every case, but in an increasing proportion of those cases. It is fair to say that the scope that the police have to monitor communications in the offline world is greater than it is in the online world. Given that a majority of those communications run by these networks are moving online, there is a security gap there. To what extent it should be plugged by the right and balanced legislation is for others to judge but I do think it is one of the most pressing problems that police face across Europe.

Q22 Michael Ellis: But you agree that there is a gap.

> ***Rob Wainwright***: Yes.

Q23 Michael Ellis: You are saying it is for others to decide whether that gap should be filled but you, as the Director of Europol, are saying that there is a gap.

Rob Wainwright: Yes. A capability gap certainly.

Q24 Michael Ellis: Thank you. Just finally from me, how many arrests would you say have resulted following Europol's work in the counter-terrorism sphere? Can you say in any degree of approximation?

Rob Wainwright: I can't, I'm afraid. I'm sorry; it is difficult to do that off top of my head. We have been engaged in a number of important counter-terrorism investigations, although maybe not as many as you might think, given the reticence of some counter-terrorism authorities to always fully engage Europol. To put an exact number on that is difficult, I am afraid, at this stage.

Q25 Michael Ellis: Sorry, can I just go further on that because that is quite important if there is a gap between the counter-terrorism authorities of various countries' willingness to communicate with Europol in this sphere. Why is there such a problem? Why is there such a lacuna?

Rob Wainwright: I think the reticence comes in part for very good reasons actually. National authorities are dealing with issues of national security, and often very sensitive intelligence that is better exploited in bilateral, known and trusted intelligence channels. That said, I think we have worked very hard at Europol to develop very strong and effective security protocols and given the globalised nature of the threat now, I think we take a bigger risk not interrogating the databases that we have. We are in a stage of evolution where I am trying to convince the intelligence community—

Michael Ellis: That you are not going to leak.

Rob Wainwright: —to place greater trust in Europol in order to use our databases to good effect.

Q26 Michael Ellis: But they are worried about you leaking, in short. Is that it?

Rob Wainwright: I don't think they are worried about us leaking. I think they are more used to dealing in a different way of exchanging intelligence. I am saying there is a way that you can do that that can complement that as well.

Chair: Thank you. The Committee, in our last report, was very clear that there ought to be a platform of some kind in that way.

Q27 Dr Huppert: Can I pick up two issues that you have talked about?

Rob Wainwright: Sure.

Dr Huppert: The first of these was that you were pressed by the Chair about taking down content online.

Rob Wainwright: Yes.

Q28 Dr Huppert: This Committee has been to see YouTube and its extensive programmes to take things down. It is very keen to talk about promoting counter-speech—rather than trying to silence as many things as possible, which will never work because people can just put things back up, trying to get other messages out there. A lot of other NGOs are talking about that. Is that something that you are trying to promote?

Rob Wainwright: Yes. We are part of a wider agenda. At the EU level, there is something called the Radicalisation Awareness Network that has many, many different forms, and it does just what you say, actually. It tries to promote an effective countermeasure and also to develop a range of other prevention tools to make sure that the right education is happening in schools and universities, for example. But it is also that we have perhaps more effective community policing so that police officers in the communities can deal with some of the disaffected members of those communities who might be swayed towards following this path.

Q29 Dr Huppert: Do you find that countries across Europe understand the benefits of counter-speech? Rather than going for the simplistic option, do they understand why it has benefits?

Rob Wainwright: I think most of them do, if not all of them. There are some such as Belgium and the Netherlands that are particularly advanced in how they are working those agendas at the moment, but generally, yes, I think it is now commonly accepted as a key part of the counter-terrorism strategy across Europe.

Q30 Dr Huppert: Then can I turn to the other thing that was raised by Mr Winnick to do with the Snoopers' Charter, as it became known? It certainly seems slightly odd that we would give away our privacy in order to defend our way of life. You were talking about dark areas where people cannot monitor what is happening. The Prime Minister spoke about not wanting anything that cannot be accessed with a warrant. As you know, bank communications are encrypted. Do you think it would be important for police to be able to break the encryption on every bank communication?

Rob Wainwright: In terms of that there are—

Dr Huppert: Sorry, Mr Ellis, were you saying yes?

Chair: Sorry, we did not hear that.

Michael Ellis: I am quite happy to give evidence myself in due course.

Chair: That will not be necessary. We have a perfectly suitable witness.

Rob Wainwright: There are other well-developed capabilities and, indeed, pieces of legislation that put on the financial institutions an obligation to report suspicious financial transactions. So there are well-functioning elements that give the police the opportunity to be made aware of such transactions.

Q31 Dr Huppert: Indeed. There is a big difference between reporting suspicious things, which I think does happen on quite a widespread level, and giving the police access. I think many of us would be concerned about breaking that security because other people would wish to break it as well. Would you go with what the Prime Minister said—I do not know if he meant it—about trying to say that, for example, iMessage, an Apple messaging system, should not be allowed because it is encrypted, and that Snapchat should be banned? Would you go that far?

Rob Wainwright: Depending on the national legislation in each case, under the right judicial parliamentary or ministerial supervision, all communications potentially, yes, should be available to be intercepted by the police authorities—if there is due cause, of course.

Q32 Dr Huppert: But I think the problem is a technological one, given how easy encryption is to do—Pretty Good Privacy has been around for a long time. People can very easily set up an encrypted messaging system and the law can respond only by making it illegal to encrypt a message, which would seem like a fairly draconian response. I cannot think what else there could be that would make it a legal requirement for any encrypted messages to be decryptable.

Rob Wainwright: I think it is a fair point, Dr Huppert. This is not just about legislation. You are right; this is also a very significant technological challenge that we face. The point that I am making here is that we are facing those challenges and there is a capability gap. Whether or not it is caused by deficient legislation, deficient technology or a combination of the two, the fact of the matter is that the reality today is that the security authorities do not have the necessary capability to protect society fully from these kind of threats.

Q33 Dr Huppert: The estimated cost for the Communications Data Bill, when the draft was published, was £1.4 billion. Do you think that for this country to spend £1.4 billion on that, with other countries presumably spending similar amounts, would be the best way of spending that money to keep us safe?

Rob Wainwright: I should not answer that question. I prefer not to, thank you.

Q34 Tim Loughton: Mr Wainwright, can I come back to an answer you gave to Mr Winnick earlier about social media technology firms? You said something to the effect that they are working to different commercial priorities than the police. Your preference is for the police to have oversight of looking for dangerous stuff on the internet or communications through social media. Is that right? Because if you look at the vast social media firms we have now, the market capitalisation of some of which is more than the economies of some of the countries where some of these terrorists are originating, do they not have a duty to use all their technological nouse to proactively track down some of the things that Government and police authorities would wish them to do? If they are not operating to the same priorities as the police, should they be?

Rob Wainwright: That is a different point. What I was trying to say, Mr Loughton, is that in the end these tech firms are working to commercial imperatives driven by what they think their consumers want from them. I think the impact of Snowden, for example, is important here, because in particular some firms have perhaps reacted to Snowden by thinking that the public now would like the next generation of telephones, for example, to have greater in-built privacy to prevent the state from so-called snooping on them. That has been a very important impact on at least the perception of these firms in terms of what they think the public want and therefore what drives their commercial imperative.

You have the FBI director therefore very publically and strongly denouncing the fact that Apple, for example, is now specifically developing tools that are unbreakable, effectively, even under a judicial warrant. If the commercial imperative doesn't happen to accord, for whatever reason, with the requirements of the state to protect the citizens in this case, we have problem. I am not saying that in this case any of these firms, frankly, don't have either a commercial imperative or, indeed, an honest intention to help the state authorities to deal with the considerable threats from terrorism. I am certainly not saying that, but there is a challenge there, I think, that we face in government and in terms of our co-operation with industry.

Tim Loughton: But there is a bigger issue here, which we could probably argue about—*[Interruption.]* But now we have a Division, so we cannot.

Chair: We have a Division, so we will need to suspend the Committee briefly and then we will return. I know you have a time constraint, which we will stick to as much as we can.

Rob Wainwright: Okay. Thank you, Mr Chairman.

Sitting suspended for a Division in the House

On resuming—

Chair: We are quorate so we will make progress.

Q35 Mr Clappison: I have two points I want to put to you, one of which arises out of the questions that have been asked. I put this as perhaps not the most technological person in all the world. There are very good reasons for putting special scrutiny on measures that are proposed immediately after a terrible event has taken place—the so-called knee-jerk reaction.

On the other hand, do you not agree that many members of the public would find it strange if the police did have due cause for suspecting that something was amiss and that some active terrorism was being prepared, but they did not take steps to investigate it by way of carrying out whatever surveillance was necessary.

Rob Wainwright: Yes, of course, and one would expect that counter-terrorist authorities, wherever they are in the world, are making the right decisions around which priority targets to follow. I think the events in Paris showed, however, that there is a potential threat even from networks that were quite probably correctly assessed to be dormant. Sometimes it is difficult to get the necessary piece of intelligence to tell you to prioritise a target, which might be one that has been sleeping for some time.

Q36 Mr Clappison: That would tend to suggest that the challenge that you face is perhaps even greater than one might have originally imagined.

Rob Wainwright: I think it is in the sense that it has become, as I said in my introduction, a network of potential terrorists that are much more diffuse in nature, operating in a very decentralised way very often through people who have never come to the attention of the authorities, so it is more difficult and much more complex than dealing with the problem that we had with a core leadership of al-Qaeda 10 or 15 years ago. It really is a challenge for security authorities here in Britain, France and many, many other European countries.

Q37 Chair: Were you surprised to hear of the hacking of the US Twitter account? Given all your capabilities in cybercrime, hearing that the United States of America’s Twitter account had been hacked by people supporting ISIS must have come as a surprise to you.

Rob Wainwright: It may be an embarrassment, but let’s be clear that it is not the same as these terrorists accessing the confidential information held by the US authorities. This is an outward facing public external e-mail system that is not connected to the internal intelligence system. The actual damage caused is very small, although perhaps it is a bit of a blow tp reputation. But, no, I am not surprised, Mr Chairman, because I can see how capable certain cyber-criminals are at carrying out such hacking attacks. This was not a particularly well developed hacking attack, actually. The real issue is the extent to which IS in Syria and its apparent network has an apparently greater internet-based capability, and to what extent that might develop in the future towards something that would be much more dangerous to us in terms of any attacks that are conducted across the internet.

Q38 Chair: Your message to these companies—to Google, Facebook and all these other outlets—is not just, “You must do more,” because everyone must do more, including ourselves. Is it a harder message that you are sending out to them?

Rob Wainwright: No, I don’t think so, necessarily. I have seen that they have responded very well to calls for them to do more. The level of engagement is much better now than it was. I just think that, yes, we all have to do more, and I know that sounds very vague, but the nature of the threat is such that there are many, many different dimensions here that all require some urgent attention.

Q39 Chair: As far as terrorists are concerned, I do not know whether you saw the article by Robert Fisk in *The Independent* basically saying that terror lists were meaningless because people were on these lists and it did not mean very much. Presumably the two who perpetrated the attack in France were on a list of some kind, yet they were not prevented and could not be stopped from doing what they were doing.

Rob Wainwright: No, because it is not always possible to do that. That is not to say, of course, that one particular counter-terrorist instrument is worthless. I think there is some operation value from placing suspects on, for example, a no-fly list or a terrorist financing list. There is some value in doing that in a systematic and reasonable way.

Q40 Chair: You still cannot tell the Committee where this funding has come from? Do you not know? You have experts there in The Hague but it is still difficult to know who is funding these organisations?

Rob Wainwright: Yes. I can't tell you that. I don't know that. That intelligence assessment is being done principally by the French authorities in relation to that case.

Q41 Chair: Not in respect of this attack but generally speaking, is it still too complex to find out who is funding these groups?

Rob Wainwright: We know that IS itself is very well funded from different sources. The extent to which any of that funding is being channelled directly to people in the EU is more difficult to confirm, but it is certainly an area of very specific investigation assisted by Europol at the moment.

Chair: Last quick question from Mr Loughton.

Q42 Tim Loughton: Just to finish off the point from before, without going into the whole big thing about privacy and everything, do you not think, though, that there are greater responsibilities that these social media companies should be following? If one takes the analogy of paedophiles and child sex abuse on the internet, and the tools that a company like Google is now developing, which are very sophisticated, there are no qualms over privacy because they are tailored to rooting out these evil acts and passing on the details so that people can be prosecuted by the police. Why should it be any different if we are asking them to be vigilant and to develop their technological know-how to root out the crime that is being promoted through terrorism? Why are the two things different?

Rob Wainwright: They shouldn't be different. We should be asking for the same level of service and co-operation, and we should be expecting to have the same response.

Q43 Tim Loughton: That was not what you said earlier, though. I am glad you have given that answer, because you were suggesting that they have different commercial priorities and then you came into the whole privacy argument. But, as far as you are concerned, they should be no less tenacious, proactive and co-operative in hunting down people who would perpetrate and promote terrorism through social media than those who would perpetrate sexual acts against children.

Rob Wainwright: No. It certainly wasn’t my intention to suggest there should be different levels of priority attached to different security threats. That was not my point at all, no, so I agree with the premise that you made.

Q44 Chair: After what has happened in Paris, the fact that the authorities knew about the existence of these individuals and the fact that the terrorist threat is now severe, how soundly in our beds should the British people sleep?

Rob Wainwright: The British people can be assured, at least, that here in the United Kingdom we have some of the most well-developed and effective counter-terrorist arrangements anywhere in the world. That is certainly how I would read it from my experience right across Europe. That said, the threat is here and it clearly affects the United Kingdom at least as much as many other countries across Europe, and it is a real threat, Mr Chairman. It is something that we have to deal with, very much so. At Europol we are committed to developing our intelligence capabilities so that we can provide the best possible support to the national authorities here in the UK and across Europe in fighting these problems.

Chair: Mr Wainwright, thank you very much for coming to give evidence today and for all the work that you and your team do. Please pass on our best wishes to them.

Rob Wainwright: I will. Thank you, Mr Chairman.