CHATHAM HOUSE

Chatham House, 10 St James's Square, London SW1Y 4LE
T: +44 (0)20 7957 5700 E: contact@chathamhouse.org
F: +44 (0)20 7957 5710 www.chathamhouse.org
Charity Registration Number: 208223

Transcript

Protecting National Infrastructure against Cyber Threats

Matthew Kirk

Group External Affairs Director, Vodafone

Erik Akerboom

National Coordinator Counter Terrorism and Security, Netherlands

Harry van Dorenmalen

CEO Europe IBM and member of Cyber Security Council, Netherlands

Simon Riggs

Senior Vice-President of Information Security, Bank of America/Merrill Lynch

Ahmed Ashour

Managing Director and Founder of Al Jazeera Talk, Al Jazeera

Chair: Dr Robin Niblett

Director, Chatham House

2 November 2011

Robin Niblett:

Ladies and gentlemen, welcome to this second day of the conference. I'm delighted to have the opportunity to chair this session. Chatham House is also very pleased to be a partner, or one of the partners, with the Foreign Office on this event. My colleagues in our international security programme have been working on the cyber security issue extensively over recent years including putting three reports out over the last three years, the last one being on 'Cyber Security and UK National Infrastructure'. And that is very much the topic of the day – protecting national infrastructure against cyber threats. Obviously these are challenges that are pervasive, that touch the world over and most interestingly and in common with a lot of the other themes that we have been covering in this conference to date.

This is a topic that really challenges the combination of coordination between the private sector and government in particular. Given the fact that probably the bulk of cyber infrastructure is in the hands of the private sector, whether it is controlling energy and water supplies, transport networks, the financial sector, the emergency services, telecoms and, as we'll also hear from our last speaker, affecting the capacity for the media to communicate and be able to serve either as a communicator for its own ends but also as a communicator for government as well in the case of any particular emergency moments.

So this is a topic that I think is probably in the heart of these cyber conversations that have been held over these days and I am delighted that we have a group of speakers here that I think will be able to tackle this topic from a very interesting perspective. What I will do is I will introduce each of them as they head up and invite each of them to make some remarks of seven to eight, maybe a maximum of ten minutes, so that we can have also the maximum amount of time for conversation among the panellists and also with you being able to draw in your insights. I think also that we will be able to get some broader questions drawn in from the audiences that are keeping up with this conference and with this event today online.

Thank you very much for coming. Thank you for being part of this first session. What I am going to do first is introduce Matthew Kirk who is the Group External Affairs Director with Vodafone, this is the position he took up in 2009, although he has been in Vodafone since 2006. Matthew brings that important combination of both having worked in the private sector but also in government. Having served for the beginning of his career with the Foreign Office, he also ran the FCOs investment in ITs and telecom for three years, served as ambassador to Finland and therefore I think will be aware of the

very critical role Vodafone plays in the telecoms infrastructure. It's great to have him as the kick-off speaker. So Matthew, you're our first speaker and I will introduce the other speakers as we go along.

Matthew Kirk:

Thank you very much Robin. Good morning. The title of this session was changed a couple of days ago and I was rather relieved when it changed because it had been about protecting the critical national infrastructure and critical national infrastructure is one of those phrases that is used a great deal and not very often defined. When you look for definitions of it you often find rather different ones or rather general ones. There is one, for example, in the US Patriot Act. It doesn't particularly tell you what you're talking about.

As Robin says, it is a number of facets, a number of assets that are critical to the functioning of our society, like: energy, water, food chain, health, transport, financial services, emergency services and defence forces. In fact when you start listing them out you start to wonder about what isn't critical national infrastructure rather than what is. Interesting question perhaps, critical national infrastructure today is defined very much by minsters of government. It would be interesting to go and ask the twenty year olds in tents in front of St Pauls whether their view about what is critical to the functioning of society is the same as the government.

But narrowing the session down to the cyber threat to national infrastructure is really helpful, partly because it is an issue I feel I can talk about with a little bit more knowledge but party also because it is a more containable subject. One of the things that link all of the elements of the critical national infrastructure together is that they rely on networks to make them work. And so the cyber threat to national infrastructure is the threat that comes across networks and through the systems which people are using across those networks and are delivered by them. When you think about the protection of this national infrastructure as one of the core responsibilities of government, one of the striking things when you look at the cyber threats that are coming across those networks is that most of those networks are not directly controlled by government. Some are run by parastatal companies but many such as the one that my company runs are run by private sector operators and sold into the other elements of the critical national infrastructure from one part of the private sector to another. So clearly the relationship between government and the private sector in protecting the national infrastructure from cyber threats is absolutely fundamental.

A quick word on the threat. I think there was a fair amount of discussion on this yesterday, I don't want to go into it in detail, but certainly what we see is threats that come apparently from governments, from organised crimes, from the hacker community, from insiders within your own business occasionally and from the gifted amateur who is just after a bit of fun. And the purpose of such attacks is not always very clear. Sometimes you can see a denial of service attempt or the theft of data as a clear motive of the attack. But sometimes rather as George Mallory, who died on the top of Everest in the 1920s on his third attempt, said when he was asked why he kept trying to climb Everest, his answer was, 'because it's there.' And the numbers of people who attack networks and attack infrastructure through networks are clearly doing so because it's there. Some of those have a malicious purpose to them; some are actually trying to expose what they see as vulnerabilities in order that those vulnerabilities are closed up. Whatever the motives are, there is a huge growth in these attacks that are happening at the moment. The target can be the company itself, the network provider, it can be the customer, a private individual, major corporation, a government or it could be elements of the critical national infrastructure, attacked through that.

A quick word on the role of government I think. Others on the panel are much better placed to talk about the role of government, but it follows from what I said that collaboration with the private sector is a fundamental part of what government needs to do. And the willingness to build trust-based systems which allow the government and the private sector to exchange information about the threat is of fundamental importance. And this can be difficult to do. For companies it involves disclosing information to competitors and to others including the company's own customers in some cases, which are revealing of potential vulnerabilities in the company's ability to provide a service. And for government it is often the most sensitive, the most secret parts of government who need to be involved.

Another very important responsibility of government, which I'll come back to, is the ability to investigate and prosecute any wrong-doing. And this raises a question which was quite a theme of the discussions yesterday; the question of digital jurisdiction. How you make it possible to enforce the rules that operate in our society normally, including in cyber space. In the private sector there is obviously a particular responsibility for those who provide cyber services, again the same trio: company, the customer and the critical infrastructure that you are underpinning. And trust is already, but is going to be an increasingly important element in the adoption, spread and promotion of the cyber based business promise. So I think that the ability of the private

sector provider to demonstrate awareness of the importance of the service being provided and the ability to protect and prevent attacks and damage to a customer's interest will be evermore important as we go forward. But some parts of the private sector, not those that are more centrally involved in the cyber space business, some parts of the private sector undoubtedly need to realise the extent of the threat that exists at the moment. So there is a bit of a wake-up call, a bit of education that needs to happen there.

I think also there is quite an important role for the private citizen. The way that networks connect, the way the particularly mobile devices connect now opens up all sorts of vulnerabilities in networks. And there is a certain amount of acceptance. Again this was a theme of yesterday's discussion. There needs to be a certain amount of acceptance on the part of the private citizen that governments do at times need to do things, need to direct networks to behave in certain ways for their own protection.

There is an example on the 7 July 2009 here in London when terrorists attacked the public transport system on the way into work in the morning. The government directed the mobile network providers to reserve a certain amount of bandwidth for the emergency services. This caused significant disruption to everyone else's ability to communicate at a time of critical tension and desire on the part of people, a very natural desire, to communicate. But the government explained afterwards why it had done what it had done and I think that it was broadly accepted that allowing the emergency services to save as many lives as possible and allowing the law enforcement agencies to track down as quickly as they could whether there were more terrorists out there and whether there was more danger out there was a very important function and a very natural exercise of the government's powers.

I want to say finally a quick word about the international dimension because one of the features of the title is the word 'national' and there is a great sense, particularly in the way government approaches this question, that is to think of critical national infrastructure as a national thing which the nation state can do on its own. But the networks that are underpinning this national infrastructure are themselves increasingly international. And I don't think therefore it's possible to look at cyber security any more in a purely national context. Many aspects of the system that we are all using, the databases that underpin it, the domain name, address registries and so forth are distributed. Now that in itself creates strength and resilience within the system which is very important but it also means that this purely national approach on its own cannot survive. The other aspect is that the threat itself is clearly highly international and highly mobile. So this information sharing, this trust based approach which I spoke

about earlier, it itself needs to become international as well as national. There are some steps in that direction, initiatives for example in the UK, Netherlands and Italy, and some important work being done at the moment by the East-West Institute to try and build a community of trust in which this can happen.

And finally to return to the point I said I'd return to, this point of judicial jurisdiction. If we cannot find an answer to how to create the enforcement capability, the key to prevention of threat is where an offence is being committed and a certain jurisdiction over the perpetrator. As Robin said, I used to be a diplomat so I ought to be able to tell you how it is done. Fortunately for me, I am now a businessman and I can leave that to others. Thank you.

Robin Niblett:

Thank you Matthew. We might not let you off the hook when it comes to your Q and A. You have offered up your private sector experience there, but I would like to turn next to Erik Akerboom who is the National Coordinator for Counter Terrorism and Security in the Dutch Ministry of Security and Justice. He is also co-chair of the National Cyber Security Centre there. He has spent a long time in the police service and the government and is well situated to bring a government perspective on this topic. Erik over to you.

Erik Akerboom:

Thank you very much. Ladies and gentlemen, defending the critical national infrastructure from cyber threats has moved very quickly to the top of international policy agendas. I would like to take the opportunity to discuss a recent incident that we had in the Netherlands and the lessons that we learned from it. Earlier this year a hacker stole digital security certificates issued by the Dutch Certificate Authority. This incident clearly illustrates the potential of cyber-attacks to disrupt society. It also shows that in combatting them international and public/private cooperation is essential, and to describe this crisis our ministers and cabinet have been in crisis structure for ten days.

First of all, digital information exchange has become crucial to the functioning of our society for both businesses and government transactions of course. It has to be reliable and digital certificates are crucial to reliable information exchange. They enable websites to prove their identity to browsers and to other websites, and to use digital signatures. There are around six hundred certificate authorities around the world. The certificates they issue are trusted

by all the major browsers, like: Internet Explorer, Firefox, Chrome and Safari. In its term, this global certificate system is based on trust.

In late August 2011, a few months ago, it became known that DigiNotar, a certificate authority established in the Netherlands, had been hacked. DigiNotar, that's the name of the company, issued certificates for both government and other parties including a lot of law firms in the Netherlands. The hacking resulted in around 530 fake certificates. We have evidence that at least one of them has been used. The reliability of both the certificate authority and its certificates came under serious threat. The Dutch government revoked all certificates from DigiNotar and took over the operational control of the company. Browser companies also took action by rejecting the certificates. Now every certificate had to be replaced as soon as possible. Controlled migration of course was essential. There were many, many unknown factors and we had some interesting questions to be answered, like: how reliable was the firm issuing the new certificates; were its security systems in order; were the certificates in use; who could replace the certificates; and how long would migration take? Finally, should the digital exchange be suspended for some time?

The hacker stated publicly when he was interviewed anonymously that he hacked Comodo, Star.com, Globalsign and other companies and which was most probably true.

Because browser companies had already started taking action to reject the certificates we had to move very quickly and about 60,000 certificates had been issued already. A total ban would mean every website using them would be either wholly or partially offline. A Dutch newspaper talked about a potential government service blackout. At the explicit request of the Dutch government, Microsoft finally delayed a deployment of an update for one week, giving the government more time to replace all of its certificates. Thanks to all efforts of many organisations from both public and private sectors, serious problems could be prevented. But the hack illustrated quite well, I think, the potential for cyber-attacks to disrupt society.

Now, the lessons learned. This was the first real cyber crisis to occur in the Netherlands at the national level. The DigiNotar incident was a real wake-up call for the Netherlands and it underlined the importance of measures that we were already planning. The crisis was not only about security but it was mainly about trust, public trust. In particular it showed that the global certification system has serious weaknesses, it is open to abuse. This even surprised the insiders but we don't yet have an alternative. Dealing structurally with these

weaknesses would be an extremely complex operation calling for worldwide exchange of the certificate system.

The other lesson we took is that we need a worldwide response of course. The internet is an open system and watertight security is impossible to achieve. We shouldn't even be attempting it. What we should be doing is ensuring that we can give an adequate response when needed. In the event of security breaches, transparency is a key requirement because then we can take immediate action and communicate about it.

Another lesson is that we need the expertise to understand our own IT systems. It took some time before government and the business sector discovered which certificates were in use. Having a clear overview of your own IT systems also implies that incidents will be reported, especially if they could impact on your critical processes in society. In reporting of IT systems, it is also very important that we are now looking into a compulsory yet confidential reporting of IT incidents so that companies or government authorities under threat are informed in time and can take action in time. However, we are not keen on regulation. We want to keep the internet open and innovative. And what's more, regulations in this field are likely to be outdated before the ink is dry. The aim in the Netherlands is for self-regulation where possible and regulation where needed.

Another lesson is that we only managed to cope with this incident because we worked closely with the private sector, which owns much of the required knowledge and much of the infrastructure. Public/private cooperation is the key to our national cyber security strategy. Last June we set up the National Cyber Security Council. Its members are representative of the business community, academia and the government and whose members include Harry van Dorenmalen, who is in the forum, and myself. The Council advises the government and society on cyber security in strategic issues; a role fulfilled also in this DigiNotar incident.

In January 2012 we will also launch the National Cyber Security Centre. I think we will need it. In this centre, public and private parties, universities and researcher centre will contribute, share and analyse information on cyber security, identify new developments tracks and trends, advise on these issues and where needed send the alert and act.

Ladies and gentlemen, I would like to conclude that the DigiNotar incident was a wakeup call for the Dutch government but also for private enterprises. The national infrastructure is not only vulnerable from cyber-attacks it can really be

hit as we noticed. Yet we have no fool proof way of preventing an attack, the incident taught us a few lessons. At least a few things are clear now. First, as a single country you can achieve very little. After all, the internet is global and it is not owned by anyone. And second, public and private parties need each other. Each has its own role, responsibility and knowledge. It is important to us to keep the internet open and innovative. Conferences like this, like today are a big help for us and I am very pleased to have the opportunity to talk with you today. Thank you very much.

Robin Niblett:

Erik thanks for those comments and for bringing your experience of a real recent crisis to bear on this conversation. I think it will help a lot with the questions, bring in issues of standards, distinctions between self-regulation and more formal regulation, etcetera, and obviously the public/private partnerships that are needed here.

Our next speaker is Harry van Dorenmalen who is Chairman of IBM Europe, a position he took in October of last year. He has been a long term employee of IBM and has held a number of positions within there, including vice-president of IBM's industrial sector business unit EMEA and a number of partnerships with other key companies such as Royal Philips Electronics. He is also in his capacity as chairman, as I can tell from his CV, the person responsible for big problems in terms of the company for everything from corporate citizenship, environmental standards and I presume cyber security as well. If I could just make sure that our technicians have Harry's tie microphone on because although he's going to be speaking from the middle here, he is going to be roving a little bit more than standing behind the stand here. Harry over to you.

Harry van Dorenmalen:

Good morning everybody. Look, this is a great conference and I hope you really feel safe this morning. So I will use nine minutes as the clock is here but I would like to touch with you on three points basically. First, I would like to share a few words on the playing field we at IBM see it. Secondly, I would like to elude a little bit on the Cyber Security Council in Holland and see how it works in reality so that it might be useful for you. And three, I will conclude with three points that I believe are essential in us moving forward in cyber security.

So first the playing field. We at IBM believe we are in an interconnected world; we are in an instrumented world. We have all the devices. We know in a minute what is happening in Singapore. So the beauty comes when we can use all our creativity to go to work on an intelligent world, smart if you will. And in a huge part of the world they are hungry for that change, they have the desire for that change and most of all they need that change because at a certain moment when we don't have energy anymore, when we don't have water anymore etcetera, we have to act.

So you see a lot of proof points as well. Only seven years ago, the mayor of Stockholm, a public institution, took the initiative of saying, 'I want mobility in my city fixed and I want it fixed forever.' They mobilised 31 partners from the public, private, academic world etcetera and they fixed the issue over there. Surely they had data issues and their cross-border items and their payments systems but the fact of the matter is they did it, they fixed it, they found a way. Already six years in a row, the Stockholm community is benefiting from less traffic, improved food traffic and less carbon emissions etcetera, they have done it. Another example: crime in New York. The mayor said, 'It's over, I'm going to do something about it.' He mobilised partners like IBM and others. He put FBI files and those of New York police together. He equipped constables with PDA devices and he used all the data and analytics to attack crime. Not only to be reactive but also to be proactive. And also here there were data issues and there were security issues.

The point I want to make here is that in the world not only in Europe but in Asia and all over the place we have seen examples where strong leaders made a change, they made it happen. They had their 'to dos' as well but they found a solution for that. So that is the movement that is going on. Challenges we have enough. In the European environment we have enough challenges in policy making, in data protection, in cross border management, etcetera. In my view we have fewer problems than we had before, only the problems that we have are more complex, more complicated technically at times and certainly global. So the only way you can fix these things is by using everybody on a global scale, is my fundamental belief in that area.

And the final thing I think is a challenge, is never compromise on innovation, research and development and technology. These are the words that I did not hear yesterday. Our fundamental belief is that technology, we are sure, is the future. If you don't invest in it, you are losing part of the future. At IBM we keep investing six billion dollars in research and development. We have the largest number of patents in the world and we also give back intellectual property to the world in the areas of ICT and healthcare. In security we mobilise over

15,000 people by now who are experts in security. We have nine security operational centres in the world, managing 4,000 clients and managing more than a few billion threats per year. So we think we have a few threats. Ladies and gentlemen, let me take you out of the dream; we have many threats.

This summer I was at Wimbledon, at the tournament and I went down into the basement and our people who are protecting the Wimbledon site from threats. They said, 'Guess how many threats we get per day?' I said, 'maybe five, ten... one good one or whatever.' A few hundred, and it is only meant for disruption, it is not mean for financial gain, only for disruption. Can you imagine that?

So evolution, we have challenges to our work, never compromise on research and development and in the end there is only one way; we need to fix it. In my view it is global cooperation, it is bringing the academic, public and private world together and if it's easy on paper because we say work together but we know in reality it is hard work because people need to start respecting each other and start talking the same language. It's a matter of definition. Researchers at IBM in the beginning didn't have respect for sales people at IBM because they don't know what they talk about. So we need to work on putting that on the same line. That's the first point.

The second point. The head of the Cyber Security Council is Erik Akerboom. In our country we vent for doing it and five things were important. Number one, there was a leader, like the mayor in Stockholm who took a decision, so the minister of justice said, 'it's enough, I want to attack cyber security well.' So he took a decision. Secondly, he wrote a charter, a vision paper – and was this good enough, I don't know, maybe it was AD 20 – but at least it got something going and gave people something to moan about, 'oh you forgot this, you forgot that,' fine. We put a team together; people from public, from private sectors and not the obvious people who were out of this role. No, we selected people who had the skills and the knowledge and the experience to bring something to the table, that's the difference.

We made a plan and focussed on the people and on the stakeholders. Be open in what you are doing. Don't assume that people don't understand what is cooking. Take them along and be transparent with what you do and work on their trustworthiness as the first speaker mentioned as well. And what we learn well in this Cyber Security Council that is running and we are inviting countries to join us to work on this initiative, and we learnt a few things. In the beginning people are always focussing on this one in a reactive way. So there is an attack, let's fix that attack – it's managed. There is a threat, let's fix the

threat, and it's managed. Cyber security certificates are down, let's manage it you know. But really the fundamental thing is let's get proactive. We don't know what we don't know. Here global knowledge should come together, data should come together, we need to apply business analytics because we cannot oversee that anymore and work on the proactiveness. And I bet you that in the world we see today that if we bring all of this knowledge together we will know much more than we know today. Analyse it and use it to our benefit.

So that is what we learn in the Cyber Security Council, in the national outreach because Singapore, Denmark, Estonia of all places, they are all starting to work on cyber security so let's share, share on what we are doing. These councils are great but we will only have fixed issues here so hopefully we will make new friends during these councils that you can work with in the future. So that is what the Cyber Security Council is doing in Holland and as someone in the private sector, as an example, I put a lot time myself into it to help the Dutch government with our insides, with our connections with our global references, etcetera, to do something in a most positive way (sic).

To conclude, I learnt over time that in this game of cyber security, the playing field you should oversee is really to get into some actual things like step into a Cyber Security Council, go into a board, do something, don't talk about it, do something. And we learnt in the end about three words that are important. Number one, it is about *open*. If you don't have an open mindset, open innovation, open collaboration, open data, open standards, you cannot play along. The word is open so test it yourself if you are in that profile.

The second word is *innovation*. Really innovate and research. We all expect that we have these computers these days that can handle all of these complexities but trust me many people are working today on technology roadmaps to make these computers ready when we need them, so innovation is the second word.

And the final word is *collaboration*, really meaningful collaboration. The two final words are there. Let's really use the talent we have in the world, let's listen to younger generations because my two young teenage daughters tell me the way the world works today. They are an asset for me. So let's use this talent in the world and think about the people in the end and the users, citizens – patients, if you will – who are going to benefit from this. If you do the full circle I think we can make huge steps forward.

So that will be my contribution, ladies and gentlemen. I think it's a great conference here today. Hopefully you get a lot of insights and hopefully when you fly back that you have some ideas that you can apply in your own environment. If you like the Dutch Cyber Security Council, as a country, Erik is here, you're welcome. Thank you so much.

Robin Niblett:

Thank you very much Harry, and thanks for raising a very important topic. I think it is implicit in some of the other presentations in being proactive, this business of getting ahead of the curve in terms of being proactive. I think there is a sense – in a way – that we are constantly playing catch up. How can one be creative when we think about being proactive? Maybe we can come back to this in the discussion.

I'm going to turn now to Simon Riggs who is Senior Vice-President of Information Security for Bank of America Merrill Lynch. Simon strikes me as being a specialist in information security. Before joining Bank of America Merrill Lynch in 2011 he was the head of IT security at Thompson Reuters so he can really cut us across two different business sectors in that sense. Simon I look forward very much to your comments.

Simon Riggs:

Thank you Robin. I am delighted to be here on behalf of Bank of America Merrill Lynch today and to contribute to such an essential conference. I smiled as I heard the member of the last session; I thought I was a member of the younger generation as well but those days are rapidly leaving me now.

Let me open with some context if I may. So Bank of America Merrill Lynch is one of the largest financial institutions in the world, we have operations in 40 countries. And clearly as a consequence of that we depend absolutely in that global financial system on a vast network of information and communications technology. And across that network runs literally trillions of dollars of transactions every single day. So clearly the potential to disrupt those flows makes the financial services sector an incredible target for all sorts of threats. While the motives of those cyber-attacks may vary, many of the techniques used are absolutely the same and we see a broad range of sophistication that we and other financial services organisations face. Those are from individuals who as we heard earlier simply want to make a name for themselves, they want to create mischief, through to, well, more organised groups who are

clearly driven just to make money through an underground economy, to nation-states who may be motivated to steal sensitive or strategic information that you really want to remain very private. And as a consequence of all of that we absolutely believe at Bank of America Merrill Lynch and certainly I can speak for colleagues of mine in other financial services companies that it is our collective responsibility to firstly ensure the smooth and uninterrupted running of those services, wherever we do business in the world. And as we heard from Vodafone this is an international issue, it is not limited to any one country in isolation.

We clearly have to secure the data and networks that support that infrastructure and we need to absolutely prevent any unauthorised access to the data and services that we offer to customers and our stakeholders in an effort to prevent fraud, identity leakage, data loss or any service disruption which will cause all of us massive harm. So let me be very clear. As a bank, Bank of America Merrill Lynch, and like most other financial services organisations, we are laser like focussed on our cyber security initiatives, 24 hours a day, seven days a week. We are hugely responsible with what we do and we maintain constant vigilance with monitoring and assessing the threats and clearly those threats change by the day. I am astounded by the rate of change with what we need to keep up with and plan for ahead. Fundamentally our cyber security program is based around that triangle of people, processes and technology. But while we employ experts in these fields, we operate rigorous information security policies, we regularly train our staff, we consider the weakest link, and we constantly innovate. We feel very proud with the patents we produce and create internally to be forthright in this area.

The bottom line is that no one entity, no one organisation has that information. And that takes us to the core of today's theme really, that it takes teamwork to bring all of those pieces together to complete that picture. We absolutely recognise that a critical element of a mature cyber security program is an investment in partnerships and to collaborate. At Bank of America Merrill Lynch we are bolstering our partnerships and collaboration for two key reasons. Firstly, we want to benefit from gaining the broadest possible view of the threat landscape and innovative solutions that could help us and help our partners. And secondly, we want to share information, we want to share best practice so that collectively we can get smarter and better at protecting our assets and critical information. We absolutely treat every partnership as a golden opportunity to either improve our internal security practices or an opportunity to improve our expertise and insight with that same agenda.

I guess it's fair to describe the way that we reach out and work with our partners as twofold. Firstly, we work industry to industry. For anyone who works in cyber security space there is a great sense of collaboration, a sense of helpfulness and sharing between similar, like-minded organisations to help one another. Clearly, after all, we face exactly the same challenges and we should be helping one another to try and get ahead of that curve with… and be as professional as we can when dealing with those.

Secondly, we also deal with industry to government. Bank of America Merrill Lynch places great value on our engagement and partnerships with government bodies to address vulnerabilities in the critical national infrastructure. Now those relationships are most mature in the US today where we are a member of a range of 'great forums', including: the Financial Services Sector Coordinating Council and also the FS-ISAC, a great coordinating body that helps everybody to keep on top of their stuff.

But we also have hugely strong relationships internationally. Here in the UK we have an excellent relationship with the CPNI, which I'm sure you have heard about yesterday and probably more today and other specialist law enforcement agencies but it's not limited to the UK. On the international stage we also have a very promising emerging set of relationships with other organisations and government certs across the globe. And as an international player we absolutely recognise we need to act and think globally in those relationships. But while we have come a long way as an institution and as a sector more widely there is clearly no room for complacency on this agenda. We have much more work to do because the threats that we face will constantly evolve.

We constantly seek new ways in building trust relationships and information sharing relationships with government. The seats should transcend the security classification problem. After all information that other people hold that may be of some use to us is frankly, when not shared, just useless information. We certainly need to find a way to continually evolve with government and law enforcement partners to protocol where we can share information in an appropriate fashion on a bilateral basis but certainly in a way that allows us to act upon that information and make use of it because without doing so we may as well not have bothered collecting the information in the first place.

So in summary, we are developing structures with FS-ISAC and our relationship with CPNI here in the UK, they allow us to facilitate threat information sharing and best practice and effectively real time instant

response. The more we do that the better and more secure I know we can help our own financial institutions and the economies stand well on the future threats to come (sic). Thank you very much.

Robin Niblett:

Thank you very much Simon. I turn now to Ahmed Ashour. If I could let everyone know that he will be speaking – at least his opening presentation – in Arabic. You all have your headphones down there. English is on channel one, Chinese on channel two, French on channel three, Russian on four, Spanish on five and Arabic on six.

Ahmed is Managing Director of Al Jazeera Talk. He joined Al Jazeera media in 2004. He is a new media journalist and New Media Coordinator of the Al-Jazeera channel. He produces the weekly 'Minbar Al Jazeera', an open forum for people to voice their opinions, but most importantly he is one of the founders of Al Jazeera Talk, founded in 2006, which is a new site that uses exclusively citizen generated news. I think it really brings into… the concept of information and news as a critical infrastructure, as a resource, or at least as a national infrastructure resource. Thank you Ahmed, we look forward to your comments.

Ahmed Ashour:

Good morning, ladies and gentlemen. I have come from the heart of Al Jazeera in order to submit to you our experience in this new world of technology, in this new world of media. I remember in 2006 when certain intelligence was available in an Arab country when this intelligence went to a friend of mine, the authorities took their computer. They took only his screen and left the computer but they took my friend along with the screen. Now I'm going to talk to you about a completely different subject and I want to share this experience with you.

In the Arab world we do not use the internet in order to give expressions for ourselves. No, in the Arab world we use it to have freedom and cause change. What is 'Al Jazeera Talk'? 'Al Jazeera Talk' is a combination of young and mad Arabs who have voted for freedom and yes who have created their own media, who have changed their physical environment using the internet. So the main idea – in spite of it being called Al Jazeera, but it is completely distinguished from Al Jazeera; only Al Jazeera's name was used so that we can have inspiration in other words (sic) – we wanted to imitate Al Jazeera

because indeed Al Jazeera was one of the primary innovators in the media that was available in the Arab world.

I learnt in the school of the internet that we have to go through this belt that is imposed on us by governments, by NSI but we want complete freedom. This was our call. We started in 2006 and we started by using the internet and also by using the cyber world. We remembered that this world is not secure and this world is dangerous and we have to be very careful with dealing with it. I refuse absolutely this word, of this 'cyber world'. The virtual world has proved that it is the real world and I still have arguments. I can talk with my Chinese colleagues, to my Italian colleagues; we can speak with freedom, with transparency. And so I have come to you from the centre of Al Jazeera, I am saying to you that what you're going to face is the Asian people, not governments. Even if the governments flirt with us and tell us that it is for our benefit us (sic). No, it is the age of the people, of the populous even in the Arab world, even in the world that is pertinent to us. The government have tried to flirt with the people, they have tried to affect the internet and then they show us that this is a free world.

We saw what happened on Wall Street. We saw what happened in London. So people use the internet to give expression to their thoughts. We do not encourage people to be rowdy but to behave properly. We want people to be able to communicate with absolutely no barriers, without precepts. So in this communication we mustn't look at other people as if they are enemies, as if they belong to different standards: you belong to the first strain whereas I belong to the third. We always talk about this racism that has been planted by government. So we want to get rid of those barriers that have been planted or imposed by governments on people. We want to act as people.

Of course you are all aware what happened on Wall Street when people demonstrated. The internet is the basic instrument of change that we can have with us in the Arab world. It is not the only means in the Arab world. You saw what happened in Egypt when the government put a ban on the internet and any means of communication, even mobiles. This went on for about ten days and we also – Al Jazeera – used to get those pictures and we used to spread those pictures so governments have to cooperate with their people. People are intelligent, people are pure, and people want to operate with no barriers, no racism and with no distinctions.

So our world, the world of the internet, is the real world and the false world is the government's world. So I hope that the welcome is going to be popular. People are causing change, not their governments. The west of course has

given us this wonderful present called the internet. The internet was the method and the way which is most important and the most beneficial but this way is not enough. We have to talk to the world in how we use it: how we use Facebook, how we use Twitter, how we use Wikipedia and all of this information together. Of course all of this has changed and must change in order to have a better reality for the Arab World.

Also I would like to remind you that the future, the near future, is one for the people and I am reiterating this. Governments, if they want to support the internet in the Arab world, if they want to support the future of the internet, all they have to do is leave us alone. This is the only solution and this is the ideal solution. People know what is good for them. They have proved that they are intelligent. They have proved that they are capable of change and therefore if the western governments want to champion the internet in the Arab world you have to champion our people with their clear spirits, with their noble spirits. Of course we cannot make a distinction between one Arab and another, between an Arab and another nationality like Chinese for example.

Therefore on this podium I welcome this opportunity to join you in dealing with the cyber space. We, the Arab youth, did not have this cyber platform. We are talking about a new Arab world. You have to understand it is a new generation which is totally different from our rulers. What puts this culture between you and us? We are talking about this intelligent generation, which is talking about a nationality with no borders. This is the new Arab World.

The Arab revolutions have proved that we are one body. Egypt was affected by Tunis, Yemen was affected by Tunisia, everyone is affected just like a contagion but all of this is caused by new, innovative ways. So change is coming. We have to have every faith that the next generation is going to be a generation of people, not governments. So this is an invitation from 'Al Jazeera Talk' to all of you to say that governments should deal with the Arab countries in a better way. Support freedoms. The only thing that we need is freedom and after revolution there is evolution. Yes, we want to have this evolution so that we can benefit from using this system.

Also this is in invitation to all of the internet companies like Google, Facebook, whatever... that they should hold strong to their opinions. It should not divulge information to governments in the Arab homeland exactly as we saw in Asia. If we do not find security, if we do not find absolute freedom when using the internet, than we are going to use other systems and it's going to be our own media, our own systems. We are capable of doing that in the Arab world.

Therefore I remind you that what we're going to reiterate is that the internet has made it obvious to us that there is only one way forward: it is the freedom that we have gained. Yes, there are many victims; there has been a lot of blood spilled [by] all of those that have sacrificed their lives in order to have this change, in order to have a better world. This world which is changing so rapidly and I would say again that very soon… that we're going to witness this change.

I would like to thank you all for giving me this invitation to be here with you. Thank you very much for listening to me and if what I said is perhaps a little bit different to the atmosphere of this conference I would like to tell you that we have gone through this explanation at Al Jazeera. Again thank you very much ladies and gentlemen.

Robin Niblett:

Thank you very much Ahmed. Reminding us that the virtual world is the real world and that maybe the government's world is the fake world, is the way that you were putting it there and I think a very interesting kind of warning, well I took it at least as a warning, you know Google and Facebook, how they interact with governments becomes determined in part about how people interact with those technologies, with those service providers in the future as well.

We have a huge range of topics on the table. We have almost exactly half an hour to be able to engage in conversation. I wanted to just throw a couple of questions first of all to our panel just to pick up on one or two of themes that were there and then we will turn to you in the audience, to ask questions as well.

But I wanted to get right down to this business about how to be proactive. There is no doubt from the presentations we have heard today and I think as everyone in this room and outside as well knows, the smart world – that world that we are moving towards, as Harry described to us – is one which will accelerate, will give fantastic opportunities in terms of medical records, transportation, crime management, smart energy, on and on, from the financial sector, etcetera. But as we get smarter, potentially, as we heard, we become more vulnerable and I think trying to balance these two things out becomes critical but I think can only be possible if as noted we can be proactive [inaudible] in this process. I wanted to get a little bit deeper on some of these proactive prospects.

I think the comment that was made earlier Erik by you; you had an interesting point in your presentation where you felt that it was important that the incidents that take place, reporting them should be compulsory but that you were very keen that the process as we undergo it should still be one based on self-regulation. It struck me that somewhere in there, there is an element of attention. Wanting to have certain aspects of compulsory behaviour in these areas of this national infrastructure and especially critical national infrastructure but at the same time recognising that the response are going to have to be somehow driven by industry and driven by business. Could you take just a couple of minutes to detach those two points: the compulsory element and the self-regulatory element? Maybe from any particular example you have in the Netherlands or beyond?

Erik Akerboom:

Well I think when you want to work in a public/private coalition you need to define the common interest and I think for a lot of businesses this is business continuity. To share information from government to business but also from business to government is based on trust and when you are on the way to compulsory elements and laws then you are on the way to a conflict model if you don't take care.

So this was one of the issues after the incident that in our Dutch parliament we had this question. We needed this information at the time, this DigiNotar business, it was hacked in June but did not report it so there was a very serious problem we were facing in the Netherlands. At the same time if you want to find a solution, a typical Dutch solution is that it will be compulsory but it will be confidential so that is the way the government knows what has happened to vital, critical infrastructure but at the same time we have to stay confidential about it.

Robin Niblett:

So it's this sharing the information, that ultimate first point, that's where you really feel the compulsory element needs to be brought in; beyond that you're looking for a far more partnership based model. But if you don't have the information then obviously the ability for the public/private partnership in this space isn't there.

Matthew or Harry let me turn to either of you two. How does it strike you, this balance between being able to share this information, the confidentiality that I think both of you raised? I know others have raised in the past issues of liability. If you admit you know something then you can put yourself up for all sorts of risks in the future.

Matthew where do you stand on this balance between the compulsory element and the ability to self-regulate this infrastructure?

Matthew Kirk:

Our natural instinct as a company is to compulsorily self-regulate in the sphere on almost everything but I think there is a critical role of government here which is not so much as compulsion but more momentum around this trust of sharing. Because the sharing of information, the ability to have, as close to real time as you can get, understanding not just within a sector, such as within the telecom sector or the banking sector as Steve was talking about, but also between sectors to understand what is happening. That will only happen if government facilitates it. It is extraordinarily difficult to make it happen between companies on their own, and to some extent the competition authorities wouldn't allow that to happen anyway. There is an important competitive element here too.

So I think government has to define the framework within which it can happen. We heard about the Dutch initiatives and similar initiatives that are happening in the UK at the moment and some other initiatives that are happening in some other countries. I think some of that is absolutely fundamental. I think it needs to be in an atmosphere where it is actually in the company's interest to disclose because what they will get back through participation is of greater value than what they are actually disclosing.

Harry van Dorenmalen:

Yes it is an interesting phenomenon. I think the private sector in general needs to step up much more than it does today in these so called societal issues because they demonstrated that in their company they know how to do that. They have global reach, they have understanding, and they have talent. So you always have two choices: hold your horses or join. Join, bring it in. So that is an appeal to the private sector to step up, be vocal, be connected and help.

Secondly, I like to bring into the equation this idea of pre-competitiveness if you will. I am also chairman of the ICT companies in the Netherlands. So what we do is rather than all of these different companies go to the defence minister because he has an outsourcing deal, we do this together. We all have the same questions so why doesn't Mr Defence explain in one short spell what he wants to do. So pre-competitive, that's the key word, and after that line draw the line and everybody fights for itself (sic).

The third thing, and its really, an essential thing: If all of us – collectively – we don't win in this game of globalisation then nobody wins. So it is also an attitude/mindset idea in my view.

I hate people who say it can be done but don't do it. Be a man, be a woman, and go into the middle and help. It is like my Arab friend here said, the world is changing. Young generations are taking over so it is leaders like us here who define the next steps. If we are not familiar with cyber security and we don't use our IPads and devices than the issue might be in this room. So I have just given you a few pictures. Don't be afraid, I'm done now. But it is around these themes. Really step-up, go into the middle, step-up and play along.

Robin Niblett:

I don't want to raise all of these points but just that last point he made about it's us in the room and maybe the people watching online but this ability to… this level of awareness into boards, not simply at the specialist level, not just at the technical level but for the risks to be fully understood, the capacity to be fully understood. I mean, what to do you think Bank of America Merrill Lynch do? How much do you think in your experience as a security professional, in boards in particular, about how central our cyber vulnerabilities are and our reliance on these infrastructures and technologies?

Simon Riggs:

I think it is clearly growing. I am greatly heartened that within the security industry these days we see a changing breed of chief information security officers coming through. Traditionally, and there is nothing wrong with this specifically, but they have come from an exclusive military career or intelligence background and that's fine but what we have to try and understand is that we need to be able to communicate in a way that's relevant to the business that we work with. So if you're going to go along to a boardroom and talk about widgets and bytes than clearly you're not going to

have much of an appetite for that sort of conversation. If you're going to go along and talk about genuine threats and impacts and what the business genuinely cares about in terms of bottom line, or customer trust or our ability to serve particular markets in an appropriate and credible way then you need to be able to speak in a relevant fashion that resonates with that board and increasingly we're seeing that to be the case.

Robin Niblett:

Let me open it up to the floor. We have microphones that will come to you and are able to take your questions.

Question 1:

I am deeply impressed about the innovation and cooperation on a worldwide scale, perhaps on the example of the Netherlands. We wrapped up already all of the knowledge at a political and strategic level on this topic but what I'm missing is a little bit of vision about who is taking on the leadership or guidance? Because you in the Netherlands have had that guidance, so on a worldwide scale, it is a little bit more difficult I would say. I would be very interested in your views on what is going on after this conference.

We heard that we will meet in Hungary and in Korea but what is happening there? Are there working groups? Are there specialists working on legal aspects or more technical aspects? I would be very interested in how you define on a worldwide scale what is going on? How we are working on this?

Robin Niblett:

I think this is the idea of international cooperation. I think you said yourself, Erik, you cannot work this purely on a national level. If you could share and if anyone on the panel could share the steps that have been taken internationally to build up these best practices and to build up an international approach… Erik, maybe starting with you.

Erik Akerboom:

I very much believe in informal structures. I have no expectation that we will create in a few months or years a complete governing structure for the international exchange of information and knowledge. But I think we do need

an international platform and on our way to that I think it would be very wise to start with things like basic principles. Of course we have to answer the question; what will these principles be about? Will they be on a high strategic level or will they be on a more concrete and pragmatic level? Maybe that is something that we can all talk about at our next conference.

I am very much a believer of informal platforms, trusted communities and core groups that bring dynamics to this issue and I think we need it because we have already a sense of urgency on a political level. I think it's' growing. We have a very strong operational international cooperation from the CPNIs on the certs but I don't think that we have anything in between. I think that gap should be filled by, I think, by informal platforms and core groups.

Harry van Dorenmalen:

I think it is a very interesting question that you're asking because what we are also seeking is a game change. We had this conference and three years later we have a follow up conference but if we are still on that model than we are missing the boat. The world is going so fast that if we don't operationalize all of it much faster, than we are missing the boat. So a few examples, first in America the Obama administration invited 13 private companies to go and talk to him. They had an employment issue, they had healthcare issues... talk to him and come with concrete examples of how they can help. It was done in America with Obama, that was an example.

Second is innovation. The old model is that people in a department have an idea and the manager decides what is good and what is not good. How can he or she still do that in this world? The new world uses innovation gems, it uses the internet, crowd sourcing and automatically selects the best ideas and you get the buy in from many people who want to do that. So you capitalise much more on collective intelligence. And the third thing is that if all of our countries on Monday morning pick up our phones, and ask each other, 'what did you do, did you go to your government?' If the answer is no, by Tuesday then we are missing something. Sorry for being so direct but something is happening in this world and if we still fix it all in a traditional way than we are missing the boat.

Robin Niblett:

Simon you have operations in 40 countries. How are you coordinating on a practical level across multiple jurisdictions, different approaches, and different

governments? Are there channels in place today that you want to take advantage of or are you having to create different channels in each jurisdiction as you go along?

Simon Riggs:

So we absolutely put in a lot of effort in forging those relationships on an international level and I have colleagues whose role it is specifically to take leadership in that space. I think that that is really important and I welcome all the assistance we get from government agencies and partners to get us through that but I think you have to be realistic. I'm not a massive believer in saying the agenda is set from some sort of higher organisation and passed down to us and we're told how to follow this. So from a personal perspective, I believe that from our leadership that we can bring personally to the table, we should go out and seek like-minded organisations and start that journey.

Interestingly I think Rod Beckstrom is speaking later today. He wrote a book about the power of leaderless organisations and it's a very powerful piece of work that talks about how in a leaderless environment you can grow organisations on an organic basis and become much stronger as a result. We should take it upon ourselves to actively go out and find people in our home areas that we can work with and we can start to foster the communities where we get better at this stuff. And over time you will see that gel and grow and partnership... So I think the formal relationships with governments are absolutely key but that has to be complemented by taking the initiative to drive that.

Matthew Kirk:

I think there are some very good examples of national best practice emerging. We had one of them described to you today and there are others in other countries. Many of those participants in those examples of national best practice like Vodafone, like Merrill Lynch, like IBM are themselves international leaders in that area. So I think we have a responsibility to spread that best practice to help governments understand what works for us and what creates the right kind of atmosphere of trust and so forth. And we're all very committed to doing that and it's a natural reflex to try and do it.

I don't believe in any top-down approach frankly because I think it will take far too long to find out what it is you are trying to achieve. The world is moving far

too quickly for that. So I think this is an organic growth but we have some good foundations on a national level and need to internationalise.

Question 2:

I just wanted to pick up on this theme we're talking about between partnerships and operating in multiple jurisdictions, dig in a little bit deeper into the public/private partnerships, into the incentives and the issues that were touched upon earlier. My question is, if I am a small telecom in the Netherlands and the government comes and ask for a public/private partnership, it is a bit easier if I'm a very large multinational that operates in the Netherlands and the government comes and asks for a public/private partnership. Given that nearly all of the speakers on the panel here today are from large multinationals, how do they balance this tension between commercial incentives that come from operating in multiples jurisdictions on one hand with requests for partnerships from government or even an alliance if it takes that sort of form? How do you balance that given that what we're talking about here is a less regulated form of cooperation?

Question 3:

I'm very glad that you have someone from Al Jazeera on the panel. All of the comments have been very interesting. I was wondering if you could address how a balance could be struck between the NGO sector, the private sector and then the media on how security on the internet can be maintained. And what we heard yesterday from Jimmy Wales on how community monitoring or editing can be put to good use on the internet? And also would that maintain full freedom of expression on the internet?

Question 4:

Having heard Ahmed's fine reparation at the end I was trying to find a link between his thought-provoking remarks and the themes of the earlier speakers and the thing that came to mind is that we're in the heart of an intellectual, cultural transformation. This is not new. In the middle-ages the arrival of the printing press caused a comparable disruption to institutions, particularly monarchies and the established religions. And the intellectual freedoms that were seized on by thinkers of the day, many of whom suffered and gave their lives to freedom of speech, led possibly to the reformation, probably the renaissance and then the enlightenment.

So where is the significance? I believe the transformation that we are beginning to see is of comparable worldwide and historic scale. However, the time scales are telescoped and the concentration of those time scales are so demanding for us. But we shouldn't lose hope. I think that the demands that it places on us, and Ahmed highlighted this, is really an issue of leadership. How does the older generation, managing and leading complex, international, cross-border enterprises, share its understanding of managing complexity and uncertainty with a new generation? And how do we develop the younger generation's leadership skills to lead in this new world in a way that in 10, 20 or 50 years' time, we will all be proud at the way that we tackled it?

I am particularly interested to hear perhaps Chairman Ahmed's views first and then the rest of the panels views on that.

Question 5:

I have two questions actually and I am addressing them to Mr Matthew Kirk and also to Mr Erik Akerboom. The first question is that we're having a lot of joy in this particular technology or in the internet and that joy is hiding behind a big fear of losing that particular technology; let's say a catastrophic attack or cybercrime on a wide scale. My fear is that at a particular time if we're going to lose internet access in any country is there any kind of mechanism to sort the interconnections inside the country itself such as internal DNS systems or internal systems that at least serve the inner services inside the organisations itself? I don't know if such a thing exists in the UK but I would like to have information about that particular part.

The second thing is about the free services that are available now on the internet, like Google, that wasn't popular when we started to use the internet, like Yahoo and other search engines actually. What would happen if Google disappears or Google Maps disappears? Other companies are dependent on those services like Booking.com. Is the market ready to have a replacement for that?

Question 6:

The title of this session is protecting infrastructure and yet we have talked mostly about data theft and data exultation. Now attacking a more complex industrial control system or any control system requires more intelligence and more targeted information. The question is particularly to the industry representatives on the panel, how concerned are you about someone actually

conducting a cyber-attack and shutting down your services? And I'm not talking about a denial service attack that shuts down a website for an hour, that's not serious, I mean not really serious.

Robin Niblett:

So to paraphrase your question, you're having a type of Stuxnet type attack where you're actually affecting services physically, rather than simply access to information and sharing information. A very important topic we haven't touched on yet.

And there was one question we had on Twitter from someone here in the room, Harry specifically for you, this business of reactive to proactive cyber security; can you give any good examples of how we are moving to a more proactive approach, specifically with some examples from IBM?

We have a number of questions here. Ahmed, I'm going to give you the last word about the younger generation and how might the older generation lead. That might be a good thing to have towards the end. Let me get some of these more technical questions out of the way first. Who wants to tackle this last point? We haven't really addressed it and this is a panel on infrastructure. Erik, I don't know if you want to start on this business of the risk of shutting down of actual services and what is the resilience available in that area? We only have about two or three minutes to get this finished...

Erik Akerboom:

Well to make a short comment. When we consider the main threats towards cyber security I think the main groups that may threaten us are espionage, criminals and hackers. Espionage states are not terrorists yet. But at the same time I think a lot of our protective control processes are built in a different time with a different threat analysis. Five or ten years ago we had a different vulnerability and a different analysis at that point.

So I think from my experience there is a lot to do building up the resilience and protecting process control systems better. I think it will take five to ten years to improve that. I think this is a very serious point which needs to be addressed very soon.

Robin Niblett:

So the five to ten years, is this a space where the information sharing, for example, would already apply; the Netherlands approach to information sharing would apply on a physical type attack, not just on an information type attack with this approach. Yes?

Erik Akerboom:

Yes.

Robin Niblett:

Harry, the question about the proactive approach, there are a couple of examples of this. Do you have any comments on that?

Harry van Dorenmalen:

I think proactiveness is all in the future and it means that the data that we have today should be analysed and we should think about what could happen in time. We know what is happening today with containers being examined when crossing borders with the use of sensor technology, with the use of people with DNA, fingerprints, etcetera. So we see a lot of techniques that are happening today and that we will explore in time. So our business analytics is used to predict what is going to happen. You use experience of the world. You use how demography is going to develop and therefore we are coming up with new ideas. A secure trade line is coming with cross border management that can be handled with time. So we are working on these examples with our research and development because we need them because this is complex stuff, difficult stuff.

Robin Niblett:

And we have this fundamental question – Simon I don't know if this is for you – about what happens if the internet goes down? I mean what if Google Maps disappears? Is this at all possible? Are we prepared for this kind of an outcome? Is there resilience backup for something truly catastrophic of that sort?

Simon Riggs:

I can't talk to Google's level of resilience, nor would I suggest I could. To be more generic about it we have to be more mindful about new institutions growing up and playing a role in society which become monopolistic in their own right. And I think we need to continue to promote a broader level playing field where we have choices and variety that we can call upon. I'm also very mindful about today's interconnected economy that it is not just about my organisation's strength and resilience; it's about my entire supply chain and the ecosystem around us. Certainly as a bank we place a lot of emphasis on understanding those partners that we work with and helping them understand how they can be as professional and resilient as they can.

Robin Niblett:

Matthew I don't know if it's fair to throw the question to you on this balance of commercial incentives with the request to play in national jurisdictions. I mean this is the question that we heard earlier on. For multinational companies getting pulled in multiple directions, this came in the plenary session yesterday as well. How are you coping with that?

Matthew Kirk:

I think it's a question that looks different according to what kind of company you are. If you are like us, a telecoms operator, you can only operate with a licence delivered by a national government so you have to have a corporate structure that corresponds with what national jurisdiction requires. We have that; every other telecom operator that I know of has that. In that sense about the small Dutch operator being asked [inaudible] the Dutch government as opposed to a large multinational presence in the Netherlands as we are, it doesn't look any different because a Dutch company is a Dutch company, incorporated in the Netherlands, subject to the Netherlands law.

There are a number of other companies; you mentioned Google and the types of services Google is providing, who do not require that national presence in order to be able to offer those services. So they essentially rely on our national services to get their services through to you. And they are operating to that extent with an ability to choose jurisdictional presence in a way that we cannot. And then you've got the interests of national governments and international organisations. So it's quite a complex patchwork within which, coming back to the theme of a lot of what we've been saying, we need to build

this ability to share information on a trusted basis which will allow us to build up the maximum level of resilience into the system.

I think the final comment just on that discussion about resilience is that the web has grown in such an extraordinarily organic way that it is of its nature hugely resilient. I know this is one of those dangerous comments to make; we'll see what happens tomorrow morning. But we've seen major, major crises; I mean the tsunami in South-East Asia, the tsunami in Japan... One of the remarkable things is the internet does keep operating, the mobile networks keep operating and the system is much more resilient than we think it is. I think that coming back to some of the questions that had been asked earlier, it is the behaviour of governments. If a government is determined to stop something happening in its country it has huge resources that it can devote to that and it is enormously difficult for companies, no matter how big they are, to stand against that.

Robin Niblett:

I want to make sure I give the last word to Ahmed. I don't know if you want to do it in English or in Arabic. How does the older generation get the benefit of the younger generation? How are you creating that cross-generational connection?

Ahmed Ashour:

I will talk in Arabic. We have to know from the outset that the main thing is freedom and this is the natural instinct so we have to have more trust in our people. Secondly, the thing that distinguishes people is the initiative and the spirit of initiative. So when we talk about the spirit we are not talking about a specific age, even if you're 50, 60 or 70 years old. What is important is your spirit of taking the initiative. Is it there or not? Therefore we should not fear the future. I believe that a lot of people fear the future, even heads of great countries. In the past for instance, Colonel Gaddafi said Libya is not Egypt, is not Tunis. Even Hilary Clinton said Wall Street is not Cairo. So I believe there is a great fear from these people. All those problems have a very simple answer: put your trust in your people, invest in the spirit of incentive and change and you are going to see this change in the world. What is required of this new generation? We need more freedom, we need to decide ourselves what we want to do.

Also I want to answer my friend from Medicine Sans Frontiers. I do not believe there is anyone who is capable of restricting freedom. For instance what we have seen in Libya and Syria, I believe that this was a shared display of the pressure that governments can pose. Yet they came over it thanks to the spirit of innovation, of taking the initiative. So we belong to the world. I believe this world has become a small village – we all know each other, and everybody can communicate with each other. So what we have been transformed into is this mass of breaking barriers between people and between countries.

So we are optimistic about the future and I believe the future is going to be far better than the present. Why are we not afraid? Because we are looking at the future. Why are you afraid? Because you are not looking at the future. So be optimistic when looking at the future. Thank you.

Robin Niblett:

Thank you for that very positive message at the end. Trust in the people: don't fear the future. I hope you can thank our speakers here: one with a very upbeat message, one about resilience, about being proactive, about not fearing the future, and trust. Thank you very much for your time.