March 17, 2013

Brussels Forum

Mystery Session: Cyber Security

Mr. Craig Kennedy: Why don't you grab a seat. Good morning, how are you? Okay. We're ready for the next session. Shh. So just to remind you of the background of this. One of the feedback that we got last year was save a session for something that is especially timely and newsworthy at the time, and let the audience decide it. It was very, frankly, close between two, cyber security and North Korea. We decided to go with Cyber Security. We have an excellent lineup. You're going to see in just a second, we're going to have some nice graphics up that will give you a sense of what's going on in the world today in terms of cyber-attacks. And we've asked one of our favorite moderators, Nik Gowing of the BBC, to do the honors this morning. Come on in, Nik, please. (Applause)

Mr. Mr. Gowing: Well, good morning, everybody. And--

(video): Cyber-attacks are increasing in both frequency and complexity. They target individuals, businesses, NGOs and governments. And because of them, personal information, wealth and national security are now at risk on an unprecedented scale. Who should have the ability and authority to address these threats and what needs to be done?

Mr. Gowing: That's a video attack. Well, thanks for staying and thanks for joining us on this. This is not a mystery anymore. Just to underline what Craig said, this is about cyber security, but there's a refinement to what Craig said. About half of you wanted cyber security when you voted on Friday afternoon and a quarter of you wanted to discuss North Korea. Last week, North Korea said that there was a U.S. cyber-attack on North Korea, so that means three-quarters of you are getting what you want.

I've got a laptop here because what we're going to do is make this more interactive with you, because I know a lot of you are catching up on your emails and

catching up on the morning webmail's and so on. I'd like you to use your tablets or your smart phones, whichever manufacturer you're using, to contribute ideas and at least to ping me if something big is coming to your mind as you listen to our guests.

Now, I need to explain what's up there. This is T-Mobile. You will not be able to read it from here, but we're going to leave that up there throughout the session because this shows cyber-attacks which are underway at this moment. You need a telescope to read it, but on the right-hand side, the 15 source countries in the last month. Russia is at the top with 2.4 million, Taiwan next, Germany, Ukraine, Hungary, U.S., Romania, Brazil, Italy, Australia, Argentina, China, Poland, Israel, Japan, the source of cyber-attacks. The density of the color inside the country indicates the intensity and that's why Russia, the Russian Federation, has the most--has the deepest color there. So bear that in mind to inform our discussion.

Philip Stephens stood here yesterday and gave

himself the gold cup in the moderator stakes for the privilege of moderating the most gripping session on China. Well, I did warn him that he would only keep that cup for 24 hours.

On Friday, when Craig gave you those three options, he did also say he wanted to experiment, and that's the kind of feedback that you've been giving those who've been here before, to experiment with new formats. So this is part of an experiment, including what's up there, and including the feedback that we're going to get both from you and elsewhere. And this is about constant innovation, a new cutting edge. And then Philip Stephens will give me the cup later.

I want you to feel more engaged and contributing organically to the direction of this. And what I'd like to suggest is that here with me is Sarah and Lindsey. If you want to tweet, and there will be addresses going up there in a moment, if you want to tweet or send a Facebook message, sometimes one of you might want to intervene at some particular point about a particular

point that's been raised in the discussion. And I'd like to know from you very quickly, because then we can make this a much more organic debate, which moves off in different directions according to the kind of things which are on your mind as it happens.

So it's not ruling out questions and involvement from you on the floor, it's just a way of helping me through this, via the curating of Sarah and Lindsey, to get a sense of where the crowd view is pushing us in this discussion.

What we're debating is invisible and it's insidious. It is a war. It is a conflict without bang-bang video appearing on television channels. I'll give details in a moment. Who have we got on the panel? Carl Bildt, Foreign Minister of Sweden, who, if he doesn't like the way the debate is going, will tweet me and send me a message from his iPad. President Thomas Ilves of Estonia, and, of course, you have a particular role in all of this because of what you went through several years ago and you are now hosting the NATO cooperative

Cyber Defense Center of Excellence. I'll repeat that. The NATO cooperative Cyber Defense Center of Excellence in Tallinn. And Nick Coleman, as well who is from IBM. He is currently the head of global cyber and has the distinction of having managed a cloud, which is a fascinating concept. He's also on the EU Security Agency advisory board, so comes this discussion we've chosen the panel, literally, in the last 24 hours, with that inside understanding from business.

I was talking about the kind of insidious invisible challenge that there is out there. Let me inform our debate by important statements that have been made in the last few days, first in Washington. That was from Jim Clapper, who is the Director of National Intelligence, the national intelligence director. He said that this now the most difficult and challenging issue on the outlook for the coming years. It's a world which our definition of war now includes a soft version. When it comes to distinct threat areas, our statement this year leads with cyber, and it's hard to

over-emphasize its significance. Increasingly state and non-state actors are gaining and using cyber expertise that, from the National Intelligence Director on the Hill last Wednesday.

Sir Jonathan Evans, the MI5 director in London very rarely gives speeches. His last speech was on this central issue. This is a threat to the integrity, confidentiality and availability of government information, but also to business and to academic institutions. What is at stake is not just our government secrets, but also the safety and security of our infrastructure. And he goes on to say it's very difficult for those in business to comprehend the enormity of this threat, which is invisible but is out there in the way that that mapping confirms to us this morning.

And finally, Admiral James Stavridis, he might have been here, SACEUR. He was testifying on the Hill on Friday and he says, "I think in cyber, we find the greatest mismatch between our level of preparation and

the level of danger." This is something that cuts across all parts of government and all parts of society.

So the question for us this morning is how engaged are people out there? And that brings me to a few of the kind of messages we've already been getting coming in on tweets. One of them, for example, in making policy on cyber security, how will the need for protection be balanced with privacy rights. There is real concern out there, and there are people watching us worldwide on a video link. Let me ask you first, Carl Bildt, how much is your government concerned by this issue?

The Hon. Carl Bildt: Well, I think every government is concerned by the issue. We might be somewhat more concerned than the average. And that is because of the fact that we are fairly high tech nation. We are the home of some of the world's leading communications in information technology industries. We have a fairly advanced industrial base in aerospace and other defense

technologies. And a lot of the things that we see in terms of cyber thefts and attacks in trying to steal things, information, is directed against those sorts of interest and accordingly protecting that and protecting our financial infrastructure and protecting sort of the government infrastructure is a key concern.

Mr. Gowing: What about the public understanding of this?

The Hon. Carl Bildt: Patchy would perhaps be the best way of putting it.

Mr. Gowing: Is that being polite?

The Hon. Carl Bildt: That is being polite, which is unusual for me. But the--

Mr. Gowing: What is the adjective you'd like to use then?

The Hon. Carl Bildt: Well, insufficient and needs to be developed. A lot of people are sort of--they are there with their PCs or iPad. They're totally ignorant of what might happen. But let me also say, Nik, for state the obvious that we are moving rapidly into a

world of hyper connectivity. We are all going to be connected. This is a fantastic development. It increases the potential of freedom and prosperity all over the world. We're all going to live in a cloud where the possibilities for human development, economic prosperity's going to increase at a phenomenal speed, but we need to be concerned with the reliability, the safety, the protection and security of the networks and ourselves. And that awareness of that has not developed with the same speed as, I think, the awareness of the potential for good that is up.

Mr. Gowing: Given the warning from Jim Clapper, from Stavridis, from Sir Jonathan Evans, what do you believe needs to be done and how quickly?

The Hon. Carl Bildt: Well, I mean, those statements were hardly sensational. But we have been working with these issues for a very long time. Are we perfect? No. Are we struggling with the same issue as a lot of other governments to get the structures right? Yes, we are. Are we struggling with issues, what's going to be the

framework of a national corporation on some of these issues? Some of them involves extremely sensitive issues. So are there problems associated with that? Yes, we are struggling with that. Are we perfect? No. Are we working intensely on this? Yes. You bet we are.

Mr. Gowing: President Ilves, you went through a major cyber-attack. What would be your reflections on how seized of this critical issue are your country, Europe, and globally people are?

H.E. Toomas Ilves: Well, let me start by--I mean Estonia was in the news six years ago because it was the first time there was a clearly politically motivated attack. But they were very primitive. I mean, those are DDO's attacks, distributed denial-of-service attacks, so that is not a concern. I mean, for us, why we are at the forefront of all this is because we are probably at the forefront of governance where we put more government services online than just about anyone else. So we deal with this a lot. But people should be thinking about it much, much more anyway because there

is no such thing anymore as critical infrastructure. It is critical information infrastructure. Everything, all your power plants, your water supply, everything, it runs actually over the internet. You may not know it, but it runs over the internet. That is that you can turn your entire army and military into legacy technology if you just bypass that and cripple a country: no telephone service, no financial services, no banks. You know, a dam stops working. And so we need to start look at this in a much more sophisticated way than we have up till now because I think largely people outside the area of specifically cyber security have not really followed how dependent everything around us is on a functioning internet actually. I mean, and most supervisory control and data acquisition systems that--SCADA systems which run everything in our societies are highly vulnerable and it's only--and of which the best example was the Stuxnet attack. But that was against one sort of secret military installation, the Bushehr, whatever, you know, nuclear power plant development

site. But, I mean, that same virus can wipe out your electrical system, so it's a big problem. Now, I'll just--which I will add to that is that this does lead to a completely different definition of war because we have all of our NATO Article 5 ideas are based on an appropriate and proportional response. So if someone blows up--sends a rocket to your electrical plant, you send a rocket back, and you know where it came from. Today, your electrical plant could just be out of commission. You don't know who did it, where it came from, and moreover what is the appropriate response. Those are the kinds of issues we need to be thinking about much more.

Mr. Gowing: Nick Coleman, how much is business gripped by this, understanding the enormity of what might face them an hour from now?

Mr. Nick Coleman: So I think there's awareness. I mean, I think the issue gets talked about, gets--the fact that it's topical issue here is it's not just an issue in businesses--an issue in government as well,

about government systems. It's an issue about the private sector systems. And I think that the question is, you know, what's happening out there? So two things, for me, are happening. One is we are instrumenting more technology into our environment. So if we think about--we've talked about maybe mobile phones, smart phones, but explore a little further. What we're doing is making smart grids. We're making smart meters. We're doing e-transport, which is digitized. We are actually connecting more and more systems with more and more devices, which is giving us more and more information to have to watch in spots, and more connections, more dimensions. The other side of the thing, which we've touched on a little bit, is the threat is becoming more advanced, persistent, and sophisticated.

Mr. Gowing: But the challenges to mitigate, to prevent, to close those doors, to shut them tight, how many are really understanding the enormity of that challenge and the necessity?

Mr. Nick Coleman: Well, I mean, some are advanced, but it is--

Mr. Gowing: Percentage-wise, can you give a--

Mr. Nick Coleman: There isn't a percentage. I think it's a maturity level. But I think what it is really is whether the organizations have proactive ability to mine the information and work out who's attacking and spot it and be able to defend it. And I'd say there's a small percentage of organizations who are sophisticated at that level to be able to really get the intelligence. I mean, I watch--we have 133 countries monitored at the moment for our infrastructure and for our clients that we're monitoring. And what we're doing is having to respond quicker with more active intelligence to be able to provide those insights. So it's more that what we have to do is then work at how we share with government, how we build those intelligence platforms to collaborate, to really create what I think--what we're really talking about is not just being aware of cyber security, but being able to

spot it, being able to respond to it. And, frankly, if your neighbor or your fellow organization in that sector is being attacked, you need to understand and be prepared for it yourself. And that's about us providing intelligent platforms.

Mr. Gowing: All right. Many of you wanted this debate, so I hope that you'll come in now with issues and points you want to raise. But we are lucky to have Chris Kojm who is a chairman of the U.S. National Intelligence Council and therefore is aware fully of what Jim Clapper said. Can you add with your assessment of how much the public, corporates, governments really understand the scale and enormity of what is happening?

Mr. Christopher A. Kojm: Well, I think exactly the reason why Director Clapper began his testimony with a strong emphasis on cyber threats was for the purpose of public education, bringing the attention, shining a spotlight for members of Congress and the public because the understanding is, as Nick stated, it exists, but it's insufficient and given the enormity of

the threat, the level of understanding and action needs to be greatly elevated.

Mr. Gowing: Do you believe that can be done? And how should it be done?

Mr. Christopher A. Kojm: Well, it's done in many ways, not simply public testimony but close consultation with corporations and with those who are responsible for infrastructure, 85 percent of which is in private hands in the United States, but all of which is linked to IT control systems now.

Mr. Gowing: Finally, how many of those who need to be educated are simply saying, it's not likely to happen to me so I'll leave it to another day?

Mr. Christopher A. Kojm: Well, I think it's less a question of overall awareness, but for a business, it always comes down to cost and benefit and demonstrating the enormous risks and potential costs of the loss of intellectual property, the loss of documentation with respect to negotiations, of contracts. So I think the case can be made quite persuasively that the costs are

substantial. But then private sector leaders then need to commit the resources to protect themselves.

Mr. Gowing: Chris Kojm, thank you. And you'll be talking at greater length to David Ignatius at 1:45 today. Let's pick up. I'm getting a lot of messages and ideas of the kind of things which are on your mind. Don't worry. These are people outside at the moment, so I'd like to get a sense from you at the moment how many of you would like to intervene so I can scale this somehow. Three, four, five, six--okay. Good. I've got an idea there for--let me give you one particular point from Farah Halima in Egypt. Why is cyber security so easy to breach? Hacking of both huge companies and governments, especially in the Middle East, seems to happen every week. It's happening more frequently according to that.

Mr. Nick Coleman: Well, I think, as we just talked about, you know, people are opening access to infrastructure. They're plugging in more mobile phones. They're putting more digitized infrastructure, and,

frankly, we have to catch up. And we have to understand at the same time, as we also touched on, that there are lots of groups, different actors, people looking to take information, intellectual property. There are also people trying to cause disruption. There's a whole set of motives. So what we've got is the technology revolution, and we've got the more sophisticated piece. And, frankly, at the same time, there are--it comes down to people processing technology, so we've got to get this hygiene level. But we've also got to be able to respond. Why does the challenge exist? Because, frankly, we are living with lots of technology in our daily lives, and we have to embed security into all those processes. We've done some, but we've still got a long way to go.

Mr. Gowing: President Ilves and Carl Bildt, let's just quickly define the players who are threatening us.

H.E. Toomas Ilves: Well, the worst actually is a new form of public-private partnership, Mafioso groups who rent themselves out to governments or--

Mr. Gowing: Rent themselves out to government?

H.E. Toomas Ilves: Well, I think it's quite clear that that's what is going on in the case of a large--I mean, much of what we have to deal with today comes from hacker groups. If you read Misha Glenny, who was here but left, his book "Dark Market," he talks about a group in Ukraine that basically signed an agreement with the FSB, the Russian intelligence group, promising not to steal credit cards from within the former Soviet Union, or actually the CIS, and that then they would be--but they would not be prosecuted. They had to agree to do things only in the West and also offer their services when needed to the FSB. I mean, that's an example of one. I mean, when you see this deniability that we constantly see from various governments--in the sense there's plausible deniability, the government itself is not sitting there hacking into your companies, stealing intellectual property. They have people, students, working for them doing it. So the government is not doing it. They'd say, oh, they're

just--it's just a dormitory, or it's just, you know, as the Mandiant Report of two weeks ago, which I recommend everyone read. I mean, it just happens to be in a certain area where there just happens to be a PLA inflation.

Mr. Gowing: This is in Shanghai.

H.E. Toomas Ilves: Pardon me?

Mr. Gowing: This is in Shanghai, the PLA cyber headquarters there.

H.E. Toomas Ilves: Well, this is--I mean, I'm just referencing the Mandiant Report. I'm a president. I can't accuse anyone of anything.

Mr. Gowing: You were mentioning China and Shanghai though. Carl Bildt, define the players who are threatening.

The Hon. Carl Bildt: Well, as President Ilves said, I mean, there's a huge variety of them, the hacker community. Those are people who start by saying it's just fun to see what they can do. But then they are sometimes recruited, sometimes by state actors,

sometimes by criminal actor. We've got a huge problem of cyber criminality. I was there the other day in the Hague with the European Cybercrime Centre where we are pooling resources to do advanced forensics and tracking. And it is just mind-boggling what these people are doing in terms of stealing money. But also, really unpleasant things in terms of child pornography, and those sorts of things.

Then we have, of course, commercial operations of different sorts. And then we have state actors. State actors that are, of course, more sophisticated because they've got the resources, they're involved in theft, intellectual property, intelligence gathering of different sorts, and then at the higher end of the scale, we have destructive things. I mean, (inaudible), there really we cross the Rubicon in terms of the first time in advanced cyber weapon was deployed.

And that is, of course, a dangerous development. Because you have to make one remark on that. I mean, there's lots of differences.

A weapon that you send away, a normal one, a bomb, I mean it destroys and the bomb is destroyed. This type of cyber weapon, I mean, first you might not detect it, but once detected, it's still there. You can take the weapon. You can re-engineer it. You can send it back. So this can easily--if you send out an advanced weapon, cyber weapon, you can get it back with devastating effect. And that's why there's--but these are at the very, very high end. And I think the actors are, I think, increasingly careful with it. But everything below that is, I think, affecting our society more than we think.

And, as said, networks are growing. Just one figure in 2017, we believe that roughly 85 percent of the population of the world will be covered by mobile broadband networks. And with a couple of years more, most of the world's population will be on mobile broadband, and we will be living, literally, in the Cloud, with all that that entails.

Mr. Gowing: Which brings me to you managing a Cloud

up until recently. I mean, I don't know where you sit on that Cloud, but it creates a lot of images. Is a Cloud secure or not?

Mr. Nick Coleman: Well, security is a relative concept. Right.

Mr. Gowing: Well, it's either secure or not. If you lose your data, it's insecure.

Mr. Nick Coleman: Well, you design security into a system, and then you operate it with security features. I think the answer to your question is, there are different kind of Clouds. When we talk about the Cloud, it's like--

Mr. Gowing: What, gold-plated Clouds? Silver? Bronze?

Mr. Nick Coleman: Well, certainly, yes. Ones which have higher levels of security than others. And it's how you construct that security.

Mr. Gowing: So, how do we know whether we're using a gold plated or a mud plated Cloud?

Mr. Nick Coleman: Well, first of all, you have to

ask, I guess, if your Cloud--you should ask your Cloud people, who you're--

Mr. Gowing: If you can find them.

Mr. Nick Coleman: I mean, let me give you a practical example. Last year, I led the company to create a paper about how does IBM deliver Cloud security around those Cloud infrastructures we're running. And we actually put a paper out. It's the first paper we've done on Cloud, which describes what we do.

For example, let me just give you a couple of things that are helpful. You know, people talk about where is my data in Clouds? So, in our engine, the customer who comes and uses that Cloud, can specify where they want the data to reside. So, that actually they're making the choice.

If you take physical security, the Cloud makes it look like it's in the air somewhere. But actually it's in a data center, in storage networks. So, actually, you know, this is--I've taken advantage of the

infrastructure and the security we had in our outsourcing business to put these Cloud Centers inside data centers, which have all that security. So you--

Mr. Gowing: Did you get emails from people saying is my data safe on your Cloud?

Mr. Nick Coleman: No, I actually got emails from people about other Clouds and said could I comment on their Clouds more than that.

Mr. Gowing: You're a Cloud rating, so we know where else so we know whether our data is secure.

Mr. Nick Coleman: There is some assurance you can get. So, for example, on the Cloud, there are international standards. So I sold 27,000 for security and the Clouds that we have, certify to that standard. We've also gone through external audit to get something called SSA16. So these are technical standards, but they are (inaudible) mechanisms.

Mr. Gowing: This is your chance to reassure everyone then.

Mr. Nick Coleman: Yeah, I mean--

Mr. Gowing: Both here and out there.

Mr. Nick Coleman: But you have to ask the question. I mean, I don't think you should just think that because someone writes "it's a secure Cloud" on a website which happens to some other people that it is secure. What I mean is you have to ask the questions.

Mr. Gowing: Let me ask the question in a different way. Is data on a Cloud vulnerable?

Mr. Nick Coleman: It depends how it's looked after. It can be secure. I can give you--

Mr. Mr. Gowing: (inaudible)

Mr. Nick Coleman: Let me give you one example. There was a law firm, a mid-tier law firm, who said actually going to the Cloud made them more secure because actually what they'd been doing previously was having one guy running with the tapes and they had no idea what the operation is. Moving to the Cloud, they understood they have process and they could get some confidence that actually they get the benefits. So it's--I wouldn't put everything on the Cloud, but

certainly the Cloud is--it can be made very secure and (inaudible.

Mr. Gowing: President Ilves.

The Honorable H.E. Toomas Ilves: I head the EU task force on Cloud computing for EU with my other hat. The issue is not the Cloud. It's not whether it's--the data is in your hard drive or it's somewhere else. The fundamental issue that we have here always is identity. Can you--is the person, the address, the thing coming in, is it who it says it is.

All of the problems have come from something coming in that claims to be something else. So, I mean, you get an email from me, and you say, oh it's Tom. But it turns out it's not Tom. What you need is to first--you need a secure identity. The current level of identification on--authentication is insufficient for anybody.

You need minimally a two-factor ID, which we have installed in our country, and which now Google has come out with as a thing you can buy. But unless you have a

two-factor ID, anything is breakable. I don't understand how people, especially in the United States, where there is not even a pin on their credit card, a chip, will give their credit card and then in the back, there's a three-digit number called the CVC. And that's your security code. And you type that in and then you're secure. This is nonsense.

You need to have a two-factor, minimally. I mean we'll probably go to three-factor, but at the point, I mean, it's all up to us. We can prevent these things if we actually have secure identity.

I mean, the White House was broken into. The Élysée, the French President's Offices, were broken into. They were both broken into, because someone went into somebody's Facebook account and saw that, you know, the cousin of a secretary had a baby. And so the person working in the White House or the Élysée gets an email, pictures of Johnny. Or pictures of Jean.

And they say, oh I'll click that. And then it turns out what they've just taken in is not a picture of

their cousin's son, it's malware that then has a keystroke logger, and everything that's typed in the Élysée is going to a certain country somewhere else.

Mr. Gowing: I can't guarantee that anything you said in this meeting will be secure this morning. That's not my job. Carl Bildt, to be clear, are you comfortable about the security and safety of the data of the Swedish government on the cloud?

The Hon. Carl Bildt: Nope.

Mr. Nick Gowing: Why not?

The Hon. Carl Bildt: Well, depends. We've got different systems. I mean, for the real sensitive stuff, we've got very--what we consider very secure systems. Then you have to be careful nowadays. I mean, you have to think of what information you put on what kind of systems.

And that is always sort of the message that I give. Put the information on the system according to what you believe is the security of that particular system.

And it has to be said, also, that I think we live

in a world where far less things are, at least in the political world, far less things are secret than used to be the case. So, there are more things in terms of diplomacy and other things that we can have on systems that are fairly okay from the security point of view than was the case before. But then, we have some things that are really sensitive, and those I think we are reasonably certain that we are protected.

Mr. Gowing: There are a lot of questions coming in here. Let me go to two or three here to build on what we've been hearing. Please, introduce yourself, will you?

Mr. Mike Hertz: Yeah, Mike Hertz from North Carolina. I work with a group called Community Care and we provide big data population health management for over 5,000 doctors and 60 hospitals across the southeast. So, what I'm interested in is this is obviously a huge concern for us because there's a lot of critical data in health care data, everything from financial data, to personal health histories that are

involved there.

We see ourselves as very vulnerable in any cyber-attacks of the future, because we have an attractive treasure trove of information. And what I'm interested in is, is where's the conversation going to occur about what our priorities are in cyber-attacks, given that like any warfare, we'll have limited resources. We need to decide what are going to protect first? What are going to protect second? Does that kind of conversation occur at an international organizational level? Is it a national decision about what they're going to protect, you know, electricity versus health care? Where do those conversations occur?

Mr. Gowing: I think there's a question here from, which is similar about governors, from Katherine Fitzpatrick. Should there be a kind of Helsinki of courts type talks against this kind of thing, to try and organize it, to try and calibrate it? Let me just take a couple more. Can you get the microphone along there? You've got the microphone now.

Female: Inmye, from the Tokyo Foundation and Profit Think Tank in Tokyo. And I have a rather basic question from an ordinary user. One of, or most powerful, attractiveness of the internet has been its democratic aspects, I believe. You can connect everyone, any time, and its--everyone is equal. So, contrary to that, because they are afraid of the security models, we have to introduce a little code of conduct on IT. Don't download any files or don't open any doubtful emails and so on. So I'm afraid, would it undermine the possibility of IT community, like promoting democracy and so on?

Mr. Gowing: Fine. Okay. Good. Keep your questions short. We're all ordinary users, I suspect. So don't apologize for that.

Female: Hello. My name is (inaudible) Minister of Defense of Latvia. I also have a question regarding of what can be done and, more on international part, and here I actually want to refer to (inaudible) Minister when you said about privacy and then I began

representing. Describing the process, what can be done? We have to start from identifying the problem, knowing where the weaknesses are. So, I have a question coming from defense sector knowing how difficult is actually it is to share sometimes information, which is particularly sensitive. And I know that this is issues about companies actually sharing around the birthdays. So, my question is, do you see, and where do you see, the international efforts where nations wouldn't shy away to actually share information about those vulnerabilities so we can actually deal with it. Or we can just walk around it and create a code of conduct or standards without sharing that information. Thank you.

Mr. Nik Gowing: A number of questions already coming in from outside about privacy as well. About really whether this is the central issue. Carl Bildt.

The Hon. Carl Bildt: It's one of the central issues. I mean, if you want to protect your privacy, you must do it. And you must be careful what you put on the 'net. I think this particularly for the younger

generation that are sort of living on Facebook and Twitter and whatever. And they should be aware of the fact that everything that is there will be there forever, more or less. We have a discussion going on whether you have the right to erase data. That's an interesting one as well, which I think it's in the European Parliament at the moment, as a matter of fact.

But privacy, a key concern. But not necessarily the other one. On the question from Japan, I still think that we should not underestimate the powerful good, for freedom and prosperity and whatever, that this development--look at Africa what is happening there. I mean, the World Bank is saying that if you increase internet penetration, or broadband penetration by roughly 10 percent, you increase the DIP by one percent. I mean, probably have more effect of broadband penetration than development aid in terms of what we're doing for Africa.

And then, of course, when they go mobile banking in different ways in which they do in innovative ways out

in the farmers there, vast new possibilities. Of course, they need to have an adequate level of security, as well. So there's not cyber criminality develops in Africa to same extent that it's already done in Europe. So they must run in parallel.

But the good things, of course, by far the dominant one. And we are also pursuing a very active international debate on the 'net freedom issues to be against trying to push back those governments that wants to restrict freedom of information and freedom of speech and all of those issues on the 'net. I mean, I think we know roughly who they are.

Mr. Nick Coleman: Two things. On privacy, we need another sort of mental shift here. We are stuck in the big brother paradigm and the thinking that came out of Orwell's *1984* and the government is bad. The government, I will argue later, is actually the last guarantor of security in the Hobson world, but right now, (inaudible). Every one of you has one of these things, and you have an app and you have a free app.

Just keep in mind, there's no such thing as a free app. I'll repeat that. No one is making these--creating these things out of the goodness of their heart. They want to make money.

Now, if you download a free app in which you put in whatever, how many pushups you did, what your cholesterol is. I mean, there are thousands and thousands of free health apps that you can do and then there's all kinds of other apps. There's no such thing as a free apps. Someone is monetizes that. You are voluntarily putting the most private personal information into an app and you're doing it and giving to someone who is going to make money off it. It's not the bad government. It's not big brother. It is someone else who's making a lot of money off you. I mean they're making a little money off you, but with big data they're making a lot of money. So that's their privacy issue, not does the government know something. And on health care, one of my other hats was I did the EU Commission taskforce on the health, but if you read

our report it came out last May and there are a lot of issues there. We treat those issues in particular. All medical records in my country are online and accessible to the patient because he owns the data, not the doctor, not the hospital, but again, you need a very secure you need a two factor ID with independent authentication in order for that to work. Without that anyone can do what they want.

Let me keep pushing on privacy for the moment. I'd like to ask if anyone particularly would like to talk about privacy and that level of security. That last comment was from Mark Jacobson. There are a couple more on privacy from Shi Yinhong. In making policy on cyber security, how will the need for protection be balanced with the privacy right of citizens. And another one, quite long, from Joe Bailey in Switzerland. Rather than an opt in policy, when it comes to personal privacy, you can ask a company to release all information they hold on you and they're obliged to do so. Why do we not have a system where companies are legally obliged to

keep you updated about all private information they hold on you through mail, a database, or something similar. Further, upon finding this information, does the individual have the right to request it be destroyed. Given what you've been managing and given that you're on the EU of Security Agency Advisory Board, which direction of these predicaments moving in?

Mr. Nick Coleman: Well, I think it's a debate, and I think that the question we're also asking is how much information do we really want to have communicated to us. If you actually ask users about how much security information, how much real system information they want, they don't really tell me they want a lot of information, but they want the confidence and assurance. So that is the system being adequately designed for security. Is it doing that and frankly, can they put their policies into place. So when you want to say what you want to achieve for privacy, I want those kind of settings, can you see that reflected into your environment.

Mr. Gowing: Is security the same as privacy or defined in a different way?

Mr. Nick Coleman: Well, security and privacy are two parts of information and how you look after it and some terms. We have a number of terms. Even cyberites suggested we use in lots of different ways and context and actually it may mean different things. For me, the bit that you really want to know is who's accessing my information and frankly, is it the people I intend it to do that and can I have some assurance. And in this world where we're now finding more persistent advanced threats, then actually what we're trying to do is build intelligence platforms where we can spot really, not only who's (inaudible), but whether it's unusual behavior. So you may think of that in a financial transaction in the old sense of, if you paid in two places with your credit card at the same time that would be unusual. Now, with the internet of course, that becomes a bit more sophisticated, but what we're really talking about is unusual patterns of behavior.

So what I'm doing is having huge analytics deployed on those infrastructures to really deep mind the piece so I can look for patterns. Coming to your point about re-use of threats and how those things come back again. What you really start to think is, okay, so you start with the infrastructure. What's usual? What's unusual and then making the user aware involved in that conversation.

Mr. Gowing: Are you ahead of those who are trying to get the better of the system or are you printing them.

Mr. Nick Coleman: Well, I think that in some cases, in lots of cases, you're spotting things and being able to disrupt it. In other cases you have to manage for things happening. But all comes back to actually having the information about what's going on in your system, having it appropriately assured, but then monitored in real time so you know what's going on and can respond.

Mr. Gowing: Right. We've got 30 minutes to run. Who particularly would like to talk about privacy at this

point? Who'd like to come in on this part of the discussion? Anyone on privacy, otherwise I'll move it on. Please. Introduce yourself, please.

Male: Hi. I'm Isham (inaudible). I'm from the City Council of (inaudible) in Belgian and I have actually two short questions. One, I don't understand actually, the focus on China. They have only one 80,000 attacks and we are forgetting the focus on Russia that has actually more than one million attacks. And actually, one on three countries that (inaudible) of attacks are EU members. What's really shocking for me. And the second thing I want to say, if we create a regulator, if we create something that actually close and shut the doors to those hackers. I was wondering as an Arab, actually what helps the Arab (inaudible) in those countries to get into the very important information, like in Syria, like in Egypt, are actually hackers. So how can we use that for the good goal and how can we actually not create something that comes in the hands of demons.

Mr. Gowing: I should say for those who can't read this that Russia is right at the top. China is number 12. You almost sound disappointed that China is only listed at number 12 at the moment.

Male: Like the focus was only on China the whole time. So I don't read much things about actually Russia.

Mr. Gowing: All right. There are important issues here and I'll defer to anyone from Romania, particularly, but I've heard senior people in this business talk about towns in Eastern Europe who's business and economy is based on violating cyber security. Carl Bildt.

The Hon. Carl Bildt: Well, in the foremost Soviet area, there are a couple of places where, I mean there are a lot of people there who are very skilled in mathematics, in different cyber technologies. If I were running a software firm and wanted to outsource to somewhere, I would not sort of (inaudible). I mean (inaudible) is a place where you have a lot of

competent individuals in this particular business. And I'm not quite certain that all of those competent individuals are doing entirely innocent things. So these sort of hackers and seeming hackers in more advanced communities, they can be found anywhere as what's pointed out, but then is question what are they doing? Some are doing it for fun. Some are doing it for criminality. Some might be sort of recruiting tool for what I call cyber riots. That is they saw defectors saying to them, these things are evil so go and attack them, the Estonians are bad. So attack whatever you find in Estonia and sort of encourage these cyber hackers or take out the computers of Saudi (inaudible) was done, 30,000 of them, this autumn. And then some of them are recruited into the, sort of the higher echelon extremely advanced state operations that are run by some. And those I would argue are so sophisticated that they are extremely unlikely to be shown on a gulf like that. I mean, the most sophisticated operators operate distinctly below the radar screen.

H.E. Toomas Ilves: Let me clarify that. I mean, if you lump all possible kinds of cyber-attacks together. I mean, you're comparing a lot of apples and a lot of oranges. I mean, first of all, the first thing you have to remember, it's very difficult to find out where something is from. You can camouflage yourself fairly well. That's the whole problem. Retribution, when it comes to NATO Article 5 applications, but more important is that, I mean, simple primitive hacker attacks, there can be thousands of them, but if one country gets by through self-technology, which you don't even know sits in your computer. It's sucking out all of your intellectual property that you've been working on for ten years and you've invested billions into it and suddenly it's for free in some other country. That's just one attack, but the damage is far, far worse. So this is why I'm always wary of these things saying well, who's doing how much because you're comparing--

Mr. Gowing: Who's saying where it's coming from?

H.E. Toomas Ilves: Well, firstly, it's hard to say where it's coming from. I mean, a (inaudible) attack comes from all over.

Mr. Gowing: Are you saying we should doubt that data from T-Mobile?

H.E. Toomas Ilves: No, we don't have to doubt that data, but we don't have a breakdown of what kind of attacks those are and there area all the things that you don't know are in your computer and you don't know that there's a keystroke logger in the White House that is pushing everything off to someplace somewhere else and that I would submit. That one attack is far more damaging than any number of attacks that primitively sort of take down a computer site.

Mr. Gowing: Is there anyone who's a government, an official from any of those countries in the top 10, 15, who'd like to explain the dilemma they face as ministers or senior government officials when trying to track down this stuff? I'll give you your chance to respond at this point. Anyone from any of those

countries? Russia, Taiwan, Germany, Ukraine, Hungry, US, Romania, Brazil, Italy, Australia, Argentina, China, Poland, Israel, and Japan. You've had your moment. There's silence on that issue. Nick?

Mr. Nick Coleman: Can I just build on that? I mean, there are lots of things happening in systems and a lot of them look legitimate but then what you're having to do is actually build, for example, and I'm sorry to get a bit technical, but if your firewall is behaving poorly going outbound, as one organization discover and then they worked out, the reason why that was doing it was exactly the intellectual property theft. The firewall itself looked just like it was a technical performance issue and what we're having to start to do, and this is where I come back to this intelligence picture, so you can create a culture, but you then have to have the intelligence live operational stuff. Because what you're going to have to do is pull that firewall data and say, okay, that user and that firewall and then you start to build a picture of

what's really going on. This means lots and lots of data. This is why it's a big data issue. And then coming to the lady's point about information sharing, it's then about how do you work with sensitive, or other partners, to actually create that collaboration. So increasingly what I'm doing is helping one energy company see what's happening in their sector. Come to the point of the gentleman. Is it a regional? It's both a regional perspective you're looking at and a sector perspective and it's also then down to the personal organizational perspective of what's really typical of that government organization or that private organization, but it really starts with the intelligence platform that you're creating to be able to spot it.

Mr. Gowing: Nick, given you're on the EU Security Agency Advisory Board, when you look at those countries, many of which are EU members, what discussion goes on about why is it going on there?

Mr. Nick Coleman: Well, I think as a minister said,

it’s a global problem. It’s not one particular country and, (B) I think it’s about a whole different set of actors with different motives operating from a variety-

Mr. Gowing: You’ve already identified sufficiently for you to be in a position to take action if you need to.

Mr. Nick Coleman: Well, it’s always about spotting--it comes back to again. Can you spot it and then can you respond to it. And the fact is, it comes from different places in the world and shifts very quickly. I think the other thing is groups and actors in this space shift. Can you identify some of that? Sure. We can see some patterns of that stuff and lots of us could put out graphs like that, but is the graph helpful. The fact is, if I’m still sitting in organization, what I want know is can I spot stuff. Can I respond to it? Is it an issue for me? And frankly, do I have the intelligence feeds and the information coming into my organization, which puts me ahead of the game, rather than reacting once my intellectual

property has been stolen.

Mr. Gowing: Let me keep pressing on the politics of this. There's a tweet from David Johns. How do we most effectively engage China in conversation about cyber security. Obviously, the question is broader. How do we effectively engage many countries in combating the threat from whatever is happening on a laptop or wherever in any country? What about the politics of this Carl Bildt?

The Hon. Carl Bildt: The politics of it is that we have to be (inaudible) the level of confidence in our different law enforcement agencies. I believe, at the end of the day--

Mr. Gowing: But Europol is across this big time, isn't it?

The Hon. Carl Bildt: Europol is now working intensely and we have Euro crime, cybercrime center that is starting to coordinate all of this. And it's pretty sophisticated things that you need to do in terms of forensics and trying to understand exactly

what it is and then take it to the prosecutors and the police and whatever. And this is different from people speeding on the highways, to put it mildly. It requires another level of competence among prosecutors and law enforcement officials in all of our countries. That's one area where we do need in terms of cooperation. We have a communication now from the European Commissioner, the high representative, by the way, on cyber security that is on the table of the ministers and of the European Parliament to increase the level of network security all over Europe. That's another aspect of it. We have exercises going on between our respective authorities within both the EU and NATO and some sort of diffuse, whatever context that is. (Inaudible) more well informed countries about this. So there's an evolving network of these national cooperation's, but are we ahead of the game? No.

Mr. Gowing: Are you saying though that a legal case has to be constructed essentially by prosecutors before anything can be put on the political agenda for action

to be taken?

The Hon. Carl Bildt: No, no, no. No, I'm not saying that but I mean you have two things. First we need to build our protection so that we are reasonably, that we feel that we're reasonably secure. But then when we identify someone doing something, I mean if it's a state act then we have to take it up in different sorts of ways. But lots of it are not state actors, I mean hackers and cyber criminality, then it's a question of law enforcement and then our respective law enforcement agencies of different countries must develop the techniques, the capabilities and to some extent the legal frameworks to do it. A lot of this is by definition cross-border so it requires a new level of cooperation across the borders. We are trying to do that in Europe and we've taken some significant steps.

Mr. Gowing: Would you say there's an acute imperative on this but --

The Hon. Carl Bildt: Yes.

Mr. Gowing: -- from the political side first?

H.E. Toomas Ilves: Yes. Let me, I mean there is a lot out there already. I mean there's the Budapest Convention which came out of the Council of Europe which has been exceeded to by the United States, by Japan, by a number of countries that we would sort of consider part of the Huntingtonian liberal democratic west. But some members of the Council of Europe like Russia and Belarus have not exceeded to it nor has China and this precisely foresees cooperation and prosecution of cross-border computer crime. But it doesn't work because the places where the problems come from have not exceeded. Now this is the whole issue. We identify someone as being a source of some problem and the government, and this is where I talk about the sort of the funny kind of public-private partnership does not want to cooperate. Now that's a real a problem. The government of a country will say we don't want it, we're not going to do it, we're not a part of this convention. The other issue which I think people have, I mean it's closely tied to this and something that

only reached the radar screen in December in about the second week was there's a think called the ITU, which came together to resolve the issue of who controls the internet. And the argument was if you want from the sort of the two-thirds of the people who were for the ITU convention, was that well we'll take care of cyber security but you have to give up freedom of speech on the internet. That was really what it came down to I mean that's really distilled the whole issue. So you got certain governments saying yeah, we will cooperate on cyber security but you can't have dissidents on the internet. Are we willing to do that? Well the EU was not willing to do that, the United States was not willing to do that and so if that's that kind of binary choice that you're given that's a pretty tough one.

Mr. Gowing: Let's get some more issues. We've got ten minutes to run. I'll go to this lady here first.

Ms. Sampson: Victoria Samson, Secure World Foundation. I have a question about the Donilon manual, the proposed Code of Conduct for Cyber Security. I'd

like to hear some more why was that chosen as a normative process? What is the end goal? Yeah, and the other question is that in the United States it seems like I'm hearing more and more that we really cannot defend against cyber-attacks, it's more important to mitigate as opposed to defend. I'd be curious to hear the panel's discussion on that. Thank you.

Mr. Gowing: Okay, bring the microphone down here and right over there please.

Ms. Schultz: I'm Teri Schultz. I'm a reporter with National Public Radio and CBS News. This may be geared mostly toward Toomas because five years ago when Estonia was attacked.

H.E. Toomas Ilves: Six.

Ms. Schultz: Six? Five years ago after Estonia was attacked at NATO we talked all the time about this would become an Article Five Offense and you only mentioned it in passing. And we actually, as I cover NATO, we don't talk about it much anymore. Has the whole threat completely just completely bypassed any

usefulness of whether or not this could rise to the level of Article Five and as we're talking about these as being non-state actors, how threated would they be if NATO governments say we're, you know, an attack against one of us is an attack against all of us? Has that whole debate just gone away?

Mr. Gowing: All right, bring the microphone down here because there is several incoming messages about the issue of governments like from Tim Souse can be there an effective cyber security defense without an agreement, clear rules on internet governance?

Ms. Hajeimer: Hello everybody, my name is Zarina Hajeimer a Romanian journalist living in Italy and first of all you were talking a lot of Romania and the threat from hackers but as I see that up as of many as not one of the first interviews inside the European Union, I'm afraid Germany's up above us. But the question, my question --

Mr. Gowing: I've invited someone from Germany to respond to that.

Ms. Hajeimer: -- yeah, yeah actually. And if I may say my ATM is blocked from the Italian bank in Romania and maybe it should be --

Mr. Gowing: Let's not get into your banking problems. What's the question?

Ms. Hajeimer: -- but yes, yes, so let's get to the point. My point was about anonymous. We are seeing a lot of attacks from anonymous group in all of the countries and a lot of these attacks are look as though, all have as a result of a lot of personal data of private citizens online so what I'm asking is how come we cannot get to a politic, a common politic you know to stop these attacks since they have, these anonymous groups have a let's say a common politics in the entire world?

Mr. Gowing: Right. In fact Mousier Glenny at dinner last night was indicating that his research and his work suggest that actually what anonymous has done, quite apart from the politics, has actually been rather good for tackling cyber security in terms of making

everyone aware of just how profound this is. One more question, who's got the microphone? I did ask you to come down here please. Down here, can you pass it down? Thanks.

Mr. Oono: My name is Oono, Japanese Parliamentarian. I would like to ask the political question, the dimension with a question that the United Nations General Assembly of last year conducted, you know, to discuss the new and the norms of the cyber security because some country like Russia, China, I wanted to emphasis that the security in the cyber space is to for example the occult, those anti-government factions rather than the security of the freedom and the speech in the internet so that we have I think a space to cooperate among those countries which share the same common, same barrier so that we should have such kind of cooperation among all those countries. So what --

Mr. Gowing: There's plenty of questions on NATO's Article but particularly this issue about anonymous.

Who'd like to pick that up? Carl Bildt?

The Hon. Carl Bildt: Well on the intervening to the governors which is connected with this I, someone alluded to it, it's immensely important for the future. We have a rather successful although somewhat difficult to understand system for internet governance, this sort of multi stakeholder approach. That has worked phenomenally well but it is under attack by certain number of regimes who often are using cyber security as a pretext by the way or they might have their legitimate concerns. Or saying let's go for some sort of international body, whatever, and their agenda is to also the one to control the net also from the more political point of view. So protecting and preserving the system of internet governance is from our point of view, from political point of view, a prime objective. It comes down to democracy and freedom and all of those particulars. On top of that, we need to develop the dialogue on cyber security issues with all of the different governments; the Budapest Convention is part

of it, implementation of it. From the EU side, we've tried to get this issue same to the dialogue with say China, say Russia and it is possible to engage them on cyber security because they have an interest in this as well, and they also are increasingly subject to attack by their own hackers, I mean that should not be underestimated either. But when we try to bring in that other component and that freedom as well, it becomes obviously somewhat more difficult. And I do think that it is important in the international dialogue to have both of these. Net freedom is fundamental and if it's only in the net security debate, I see the risk of that tilting in such a way that we develop structures that will be used by those where the real agenda might not really be net security but might in reality be control the net in order to limit the freedom of the net. So that is an issue where we have to be vigilant when we discuss the net security issues.

Mr. Gowing: That specific question about NATO, President Ilves?

H.E. Toomas Ilves: Well there's another question on this which is the Italian manual and why did we do it? We did the Italian manual, well actually it was done by NATO, I mean we didn't do it but NATO did it, is to look at the whole sort of from A to Z, everything concerning law and conflict. I mean, there are so many different laws, we're not only talking about something like Article V but and see how this applies to cyber, how cyber is affected by these laws, when something is a violation of some aspect of the legal framework on conflict. And that's why we did it. I mean it was just to see what would come out of this because we really didn't, I mean we knew all of the various things that have been developed on conflict and all of the laws and conventions and they apply to poison gas to germ warfare, to what you do with prisoners but suddenly we have this new realm and that had never been done before and so now it's available and you can get it.

Mr. Gowing: Nick, the issue of anonymous could you --

H.E. Toomas Ilves: Wait, on the NATO which is specific side of this this, I mean we have not really addressed in NATO the Article V issue to its full extent because there's a certain unwillingness to deal with it. Now on the other hand in May of 2011, there was a very important announcement by the Department of Defense by the United States that said we will not necessarily respond in kind or in the same modality to a cyber-attack. What does that mean? A cyber-attack against the United States, I mean the U.S. need not answer when in cyber, they can do it kinetically, the can drop a bomb, I mean who knows? But the point is that this thinking, I mean the U.S. has thought this through and I mean I think that's where we are heading and given the use of cyber-attacks in conjunction with kinetic attacks, that's flying things and in the Georgian war for example, where the Russians blacked out entire areas and then proceeded to black them out on the internet and then proceeded to bomb them, I mean this is going to be a very, very serious issue in the

future.

Mr. Gowing: Right. Okay, we can't get into the defense implications in detail at this point but Nick, that issue of anonymous and what you've learned about anonymous and what kind of signals it's sending?

Mr. Coleman: Yeah, I'll talk about it, I just want to talk a little bit about policy for one second before, so when we talk about this, we've recognized, I mean you gave the statistic about the percentage of infrastructure in the private sector. That the thing which we really, and you talked about I think about Minister about the cross-border dimension to this, so when we're thinking about public policy responses, I think there's a couple of things. One is we have to think about international standards because actually the infrastructure is global. The other thing we have to think about is how we get bilateral, by that I mean public-private sharing of information exchanges and that much to be more sophisticated because frankly we've all got to work together. And we've got to do

that on a basis which really starts to think about the kind of information we need to share. So we might really want to focus a little bit on the critical national infrastructure and I take the President's point about you know, let's define this, it's critical information infrastructure. And then to look specifically to take your point about the groups, so there are lots of flavors even of something like anonymous so there are lots of people that use brand names like that to kind of come together under a banner. So let's not again be too concerned about a name but let's get to the specific which is again it comes down to what's the motive of the organization, what are they doing, how are they doing it and frankly can we, coming to the question over there, can we mitigate and defend against it?

Mr. Gowing: Steve Erlanger. I'm being asked to wind up but can you do something quickly?

Mr. Erlanger: Very, very quickly. The United States and possibly Israel have attacked Iran with Stuxnet and

other viruses. Why isn't this a declaration of war from Washington's point of view an attack on the United States is being considered a declaration of war and is there any sign that Iran has been striking back? Thank you.

Mr. Gowing: Right. Is it, quickly is it a declaration of war in your view, attacking with Stuxnet Carl Bildt? You're on the record.

The Hon. Carl Bildt: I'm on the record and I think I was ordered in record saying that I think it was a Rubicon that was passed. And the implications have not been fully understood and fully explored. Has there been any counterattack? I don't know but I know that 30,000 of the computers of our Aramco in Saudi Arabia was taken out, well early Autumn, October or November whatever it was. And it might well have been "X" numbers of other things and I think that it's profoundly dangerous if we enter a process of escalation here. And in contrast to, I mean nuclear weapons and the nuclear weapon power, that is bloody

complicated and expensive and it takes a long time over to detect it. But here it is possible for all sorts of states and actors to fairly quickly buy or develop a very advanced attack capability and if we started attacking each other the one way or the other, yeah, I'm not quite certain where we end up, in a bad place I suspect.

H.E. Toomas Ilves: Let me just say about Anonymous, since Sue asked me (inaudible) I mean, Anonymous, there is no such group.

Mr. Gowing: I'm talking about an act of war, actually.

H.E. Toomas Ilves: Act of war, okay. Act of war--

Mr. Gowing: (Inaudible) up to this (inaudible) there is a--there is--

H.E. Toomas Ilves: I can say that, I mean, we don't still--we still don't know who did it. We really don't.

Mr. Gowing: Yeah, but there are several questions here, like, from Rubén Gallego. Where is the line for state actors using cyber-attacks? What is considered an

act of war? Mr. President.

H.E. Toomas Ilves: Well, any aggression against the territory of another country is an act of war. And especially if there are casualties, as--if there is--if someone dies, if you've blown up a power plant, that's an act of war. The problem is more that--there's huge reluctance to admit that or to go along with that because the implications could be really horrible.

Mr. Gowing: All right. I'm going to have to close it there and I'm going to leave you with two messages here. First of all, I think, from my point of view, it shows that we need to reconsider this next year because so much is changing so fast. Two messages; firstly from Marcus Freitas. Does cyber war place everyone on the same level as to inflict damages? Will wars be commanded by youngsters sitting in their homes? And secondly, a sobering thought from Nina Sophia. Could cyber security be a higher priority than addressing issues of poverty or education? Those reflections from at least two people who have been monitoring this

outside. Thank you very much, indeed. Very dynamic, very sharp, very focused but I think we've got to revisit it maybe not next year, maybe next month. Carl Bildt, President Ilves and Nick, thank you very much, indeed.

Mr. Craig Kennedy: Nik, that was terrific. And thank you very much, all three of you. I think this mystery session idea worked out pretty well, but if you got beefs about it, let us know. We'll probably do it again next year. We're going to take a break and then we're going to come back for our penultimate session on the global Atlantic, which promises to be very, very interesting. We'll see you in a little bit.