2016 Halifax International Security Forum
Plenary 7 Transcript
Spies Love Us: Protecting Information in the Age of Openness

SPEAKERS:

Greta Bossenmaier, Chief, Communications Security Establishment, Canada

Baroness Pauline Neville-Jones DCMG, Chair, Cyber Security Advisory Panel, Bank of England

Adm. Michael Rogers, United States Navy and Commander, United States Cyber Command and Director, National Security Agency/Chief, Central Security Service

Gen. Amos Yadlin (Ret.), Executive Director, Institute for National Security Studies

MODERATOR:

Steve Clemons, Washington Editor-at-Large, The Atlantic

Steve Clemons: I'm Steve Clemons, I'm Washington Editor-at-Large of The Atlantic. It's great to be with you, and I have brought Halifax International Security Forum coins for the best questions. I'm going to give David Kramer a coin in advance there, pal. (laughter) And I know that Wendy Chamberlin's going to have a great question for me, right? So here you go. So that's to get you all prepared for, for later so that we have a very active discussion. Howard, you get one too. Yeah. I know you like these coins. (laughter)

Let me first share with you who our panel, we have here on our panel. Just to my right, we have Baroness Pauline Neville-Jones. She is the DCMG Chairman for Cyber Security at, and advisory of the Bank of England, a member of the House of Lords, but more importantly, she was the former Chair of the British Inte-, British Joint Intelligence Committee. My understanding is that Judy Dench learned everything about the roles that she played from Baroness Neville-Jones. (laughter)

Then we have Admiral Michael Rogers, who is a US Navy Commander, US, head of US Cyber Command and had Head Director of the National Security Agency. He's occasionally in the news. (laughter)

We have Greta Bossenmaier, Chief of the Communications Security Establishment for Canada, called by Power and Influence magazine Canada's top spy. And we'll go – And then we have Amos Yadlin, Executive Director of the Institute for National Security Studies, the former head of the IDF Military Intelligence Directorate in Israel. Also played a starring role in which he told me he was deceived in a fascinating Alex Gibney film called Zero Days, which he says none of you should watch, but, but nonetheless is quite interesting.

So let me just start out, I want to get into a variety of things. We've going to have a conversation, try and make it as conversational as possible and I want to really go to al of you as soon as possible. So to do that and be successful, I want everybody who's going to pose a question or make a comment to do it in less than 30 seconds. If you go over it, I'll cut you off. That's just the way it's going to go.

So I guess I want to start off with Greta and ask you do spies love us?

Greta Bossenmaier: Well, thank you for that question, and let me say it's just such a pleasure to be here today and to see you all here today.

Having a session on cyber security I think says a lot about the forum in terms of placing the importance of cyber security in a very prominent place on the overall agenda. Let me just say from the Communications Security Establishment, we have been in the business of helping to protect Canada and Canadians for over 70 years. It's our 70th birthday this year. So we're in the —

Steve Clemons: Because they had so much cyber 70 years ago? Or, yeah. Yeah.

Greta Bossenmaier: That's an important comment actually. We've been in the business of protecting Canadians' information for 70 years. Back in the days when were primarily focused on communication security, that's been a key part of our business for 70 years. And over 70 years, we've now had to continue to advance and innovate to help protect Canada and Canadians in the cyber world.

Steve Clemons: My understanding is that your agency is both a combination of the NSA and the Department of Homeland Security. Is that, is that right?

Greta Bossenmaier: Well, I don't want to maybe make comparisons to other countries, because we're all a little bit different. We have three key roles at Communications Security Establishment: cyber security and helping to protect electronic information infrastructures of importance to the Government of Canada. It's a key role of ours. Second key role is providing foreign signals intelligence, providing information to the government. And we also play an

important role in helping our law enforcement and security partners as well under their legal authority.

So an important combination of activities that are really focused on helping to protect Canada and Canadians.

Steve Clemons: Thank you. Mike, Admiral Rogers, I want to ask you a little bit about a statement you made at the Wall Street Journal Forum last week. You said there shouldn't be any doubt in anybody's minds, this was not something that was done casually, this was not something that was done by chance, this was not a target that was selected purely arbitrarily. This was a conscious effort by a nation state to achieve specific effect. And that's an extraordinary statement and I'm interested in whether you're essentially saying that Russia achieved what it wanted in Donald Trump's victory?

Adm. Michael Rogers (Ret.): No, I certainly didn't talk about outcome or effect. I talked about effort, desire and intent, which is different than outcome. I agree, I think it was Senator McCain who said earlier, hey, I think really think (inaudible) and I would agree with that assessment. I don't think in the end, it had the effect it potentially had hoped that it might.

But it's an interesting challenge for us as a nation, and I would argue it's not unique to the United States. As we think through, for example, well, what does the definition of critical infrastructure man in the digital age of the 21st century – –

Steve Clemons: Right.

Adm. Michael Rogers (Ret.): — if you had asked us 10 years ago is our election structure critical infrastructure, we probably would have said well, we really don't view it that way. We tend to think a very industrial output process as aviation, manufacturing, telecommunications. I think it highlights to us we need to think about what the definition of critical infrastructure is in a whole broader way.

Steve Clemons: Is the WikiLeaks arena and what you and other intelligence officials have said occurred, is that a failure of the NSA? Is it a failure of, of cyber command? And, and my understanding is that cyber command is also prepared its own responses to what may have happened. And, and I guess the question is have they been deployed?

Adm. Michael Rogers (Ret.): So Cyber Command and NSA have no responsibility for the day to day defence of networks, individuals or connectivity outside the federal government, and we're largely focused on the DOD day to day. Cyber Command does have a mission if directed by the President or the

Secretary of Defence to provide our capabilities to help defend critical infrastructure in the United States, but that requires a presidential or secretary order to do so. That's not a day to day normal —

Steve Clemons: Yeah.

Adm. Michael Rogers (Ret.): — activity for us.

Steve Clemons: Pauline, in, in, have the Russians messed around in your internet space very much in England?

Lady Pauline Neville-Jones: Mm-mm. Well, I would like (inaudible) to answer that question. I'd be very surprised if they haven't, they haven't made an attempt or two. I don't think they've, so far as I know, there haven't been any, sort of, spectacular examples of manipulation of that kind. But it is something that they're doing, you know, right throughout Europe.

Steve Clemons: I know that in the UK, you have played a very large role helping to sculpt the, the scaffolding of the infrastructure of UK's both cyber capabilities but also its intelligence capabilities, and I guess my question is now that you are more of a free person in this world, what would you say the bigger blind spots are of the UK intelligence infrastructure?

Lady Pauline Neville-Jones: I think probably a (inaudible) UK would not be unique in this, is that we still haven't reached the stage where we can really seriously talk about resilience. We can talk about security but security, you know, is not something that stands by itself. It needs to be backed up by the capability to recover from a penetration from a break-in into your networks.

And there, I think, there's a long way to go before we have actually got into a situation where the organizations concerned have a plan, have exercised it, know what each individual in a given situation needs to do, know who and when they need to inform the regulator, and most organizations these days, you know, have an information commissioner or a regulator to which they must report a breach of any seriousness.

And, and actually, have sufficient technical and business knowledge combined together actually to recover. And there, I think, where probably all societies would still, would still say they're weak.

Steve Clemons: We, we, (inaudible) —

Adm. Michael Rogers (Ret.): Can I, can I —

Steve Clemons: Yeah, go ahead. But, but I want to ask you when you do answer this, is where is that responsibility? Should it be more in the private sector? Should it be more in the government? You know, this is one of the big —

Lady Pauline Neville-Jones: It has to be a partnership.

Steve Clemons: — debates going on.

Lady Pauline Neville-Jones: It has to be a partnership.

Steve Clemons: Right.

Lady Pauline Neville-Jones: The government sets the framework, I think. In the case of regulated industries, it probably has a direct hand along with the regulators themselves. But when it comes actually to the private sector, what people have to realize these days about national security is, but it's not just a government thing. It's actually a whole society thing and it includes the individual. But it crucially involves the private sector. And they have to regard themselves as players in national security.

And it's not just for national security reasons, it's also for good business. I mean, what are you doing the shareholder if actually you lose all your data, which is your most valuable thing to the, to whatever process you're involved in?

Adm. Michael Rogers (Ret.): I think that's one of the inherent challenges of cyber. The way we often (inaudible) problem sets, as a military guy, we love to think of geography. It's why we have a Central Command, it's why we have a Pacific Command, it's why we have a European Command. In our nation, we have traditionally put very strong delineations between what is an inherently government function and what is a private function.

Cyber just doesn't recognize these differences. And so I think part of our collective challenge is how are we going to adapt to recognize that this really doesn't recognize many, not all but many of the traditional mechanisms, boundaries and structures we've created to deal with problems.

Steve Clemons: Amos, Israel is considered a cyber superpower. Why? What are you doing so well that others aren't doing?

Gen. Amos Yadlin: First, let me help the audience with the three dimensions of cyber. We spoke, and this is in the title about espionage —

Steve Clemons: Right.

Gen. Amos Yadlin: — which collecting information. [sic] There is cyber security to stop the other guy from collection your information [sic] and there is a cyber operation, which is if you are already there collecting the information, you may do something else out of the information. You can destroy something and (inaudible) the movie, it was weapon of mass destruction.

So here are the bad and the good news. The bad news is that privacy as we know it is gone. It's gone.

Steve Clemons: That's a tweetable moment.

Gen. Amos Yadlin: If you, if you think —

Steve Clemons: From Amos Yadlin.

Gen. Amos Yadlin: — that your —

Steve Clemons: Do you have a Twitter account?

Gen. Amos Yadlin: — that your cellphone is protected —

Lady Pauline Neville-Jones: He's right.

Gen. Amos Yadlin: — there is somebody in the world, usually a superpower —

Steve Clemons: Right.

Gen. Amos Yadlin: — that can reach anything that you think that is secure. Okay? This is the bad news.

The good news is, or another bad news is (laughter) that if, in cyber, the attacker is now a head of the defenders. So defending is always a problem, much more difficult because you don't know where you'll be attacked. In cyber, the attackers are ahead of the, of the defenders and we put a lot of money in defence, a lot.

And here's the good news. It is not weapon of mass destruction. If it was a weapon of mass destruction, it would be already exercised against us by terrorists, by small countries, maybe, maybe the superpowers. And I'm not sure in that. Because 10 years ago, everybody wanted to be the Bill Mitchell or the doer of the cyber power. You know, 19th century, Army and Navy, the 20th century, air power, 21st century, cyber power.

And what we saw is that it is not that easy to destroy a country with cyber, because unlike nuclear weapon, there is thousands, maybe millions, of cyber

attack every day. And with all due respect, the effect is not that strong. Not that strong. Yes, the media is making it —

Steve Clemons: But, but Amos —

Gen. Amos Yadlin: — and you know what? Cyber —

Steve Clemons: — is that a function that it's not —

Gen. Amos Yadlin: — security companies —

Steve Clemons: — isn't it not that strong yet?

Gen. Amos Yadlin: Yeah.

Steve Clemons: Because one of the, the yet element I think is interesting. In the movie that you don't like, Zero Days, the, one of the comments made in it is that since Stuxnet, there have been more than 100 state-based, state-launched types of malware attacks in the world. And that a lot of people fear that these Zero Days malware are out there lurking in every —

Gen. Amos Yadlin: Have you heard about —

Steve Clemons: — infrastructure.

Gen. Amos Yadlin: — each one of this, under the —

Steve Clemons: No, but I'm just interested in the degree —

Gen. Amos Yadlin: — (cross talk) damage, any damage?

Steve Clemons: No, but I'm just interested in the degree, I mean, how much should we worry? How much should we collectively worry about this?

Gen. Amos Yadlin: See, the problem with cyber is that it's not tangible. You don't see an airplane, you don't see an aircraft carrier. And it is zero at once. And very small group of people know really what is cyber. And it's mostly classified.

Steve Clemons: Anything you want to share on that?

Gen. Amos Yadlin: So you can, you can build a lot of stories about it. But at the end of the day, cyber weapon, unlike a JDAM, which is a guided bomb —

Steve Clemons: Right.

Gen. Amos Yadlin: — when you deliver it, it's not explode. It — [sic]

Steve Clemons: Pauline?

Lady Pauline Neville-Jones: Can I come in on your, on your (inaudible) yet.

Steve Clemons: Yeah.

Lady Pauline Neville-Jones: I think it's absolutely right to say these are not weapons of mass destruction. They aren't therefore existential threats, as things stand, to societies. And I'm suggesting they ever necessarily will be, but what we shouldn't forget is that we are moving into a word of, of artificial intelligence where the availability – and I mean availability – non availability and the uncorrupted nature of data, that's to say not interfered with, so therefore not penetrated, not manipulated, not unavailable, all those things are absolutely going to be absolutely crucial to a network society.

(inaudible) Romey (ph) had a session on the network battlefield or future battlefield. And it's exactly the same now, going to be exactly the same in civilian society. Increasingly, how we operate in society is going to be with certain things automated, but things are autonomous too. And they have, they can only operate safely on the basis actually of having uncorrupt and available data.

So the daily running of our society is going to be increasingly dependent on security. Now, increasing, we ought to be able tin that world, you know, to build in cyber security by design, but there are going to be an awful lot of, of bits of technology which linked into systems capable of interfering with systems that are actually not up to scratch, which are still liabilities to it and which will interfere with it. And we have several instances, you know, of cameras being used, for instance, actually to (cross talk) —

Steve Clemons: Yeah. (cross talk) Greta real quickly.

Adm. Michael Rogers (Ret.): Go ahead Greta.

Steve Clemons: Yeah, Greta.

Greta Bossenmaier: Perfect, thanks. I just want to pick up on both those last conversations. We can debate how big the threat it and the nature of the threat, but I think when we look at it from a number of dimensions, we know that our citizenry, our businesses, our government are doing more and more of our lives online.

Steve Clemons: Right.

Greta Bossenmaier: Personally, business, government, etc. So more of us are online. More and more data is online, more information. We have more and more devices connected to the internet. So more devices are there. And we have different types of, the threat environment is evolving as well in terms of different players and different types of technology.

So yes, we can debate at how big it is, but the reality is we're in a very dynamic environment, and I think what the imperative is – and it is a team imperative – I definitely agree with my colleagues that it's not one organization or one part of government or one part of society that can, has to take the only lead. It's a team imperative, the cyber security.

The reality is it's dynamic, it's changing and the imperative upon all of us is to help ensure that it can be as safe and secure as it can —

Steve Clemons: Is cy-, Greta, before I get into Mike, is cyber security an illusion? I mean, when the CIA director's account is hacked in the United States, it just, it makes one wonder whether there's any degree of protect- -- Amos just said, you know, the attacker has the advantage, but I'm really interested in this notion are we getting sort of snake oil salesmen in the cyber security world saying we can make you safe?

Because when you look at what has been hacked already, what's on the, the roster of victims, they're extraordinary victims with extraordinary capabilities. And it makes one wonder whether you're in the private sector or you're an individual how you're even going to play in that world. And I'm interested in how you see this?

Greta Bossenmaier: Well it's an interesting paradox because we spend often a lot of time in talking about the successful attacks. We spend much less time talking about actually what good cyber defence means and how it's actually being enabled and, and quantified. We put out statistic recently and we talked about in the Government of Canada space that Government of Canada systems are being probed 100 million times per day in terms of looking at what the systems are and, you know, (inaudible) actors probing our systems.

We're not having 100 million successful attacks a day. So I don't think it's an illusion. At the same time – cyber security, to answer your question – at the same time, there's risks that abound. We are operating – again, going back to my earlier comment about diversity of information players, technology, threat actors, it's a very dynamic environment.

Steve Clemons: Mike?

Adm. Michael Rogers (Ret.): Two points for me. First, Paul-, (inaudible) Pauline, in addition to artificial intelligence and Amos' point, look for the increased interconnectedness of the world. As we move into the, to the internet of things in a much broader way, look for that potentially to amplify the impact of —

Lady Pauline Neville-Jones: Exactly. That's my —

Adm. Michael Rogers (Ret.): — that (inaudible) —

Lady Pauline Neville-Jones: — point. Exactly that.

Adm. Michael Rogers (Ret.): — to see how that changes. And many of the hacks that you've identified, for example, were against personal individuals, not companies or businesses. One thing, I think, for all of us, we oftentimes differentiate in our minds between well, what I do at work versus what I do at home, and in the digital world that we're living in, this is such an arbitrary boundary that many actors out there just don't recognize.

There are implications for each and every one of us, but how you lead your digital lives, what your, what your footprint looks like, what are you comfortable in this digital world, I'll be the first to admit as a parent, this is something I, you know, my wife and I have sat down and talked about with our sons about hey, this is something you guys need to be thinking about. I can tell you what the right answer is, but you have got to think about this.

Steve Clemons: Let me ask you all, and Mike, I'll start with you, a question about the pipeline of talent out there. You know, I'm an addict with David Ignatius novels. David, for those of you who don't know, is a major writer for the Washington Post, he's been at this forum before, and when he tells the story of the downfall of cyber regimes and governments, it's all done by a highly tattooed goth, you know, completely irreverent, iconic plastic game player.

And I'm wondering whether those are the people that you are hiring, Mike, (laughter) to help us and, and what that world is like? And, and, and can, I mean, you're a man in uniform and your hair's done well, and (laughter) you know, I, I just, you know,

Adm. Michael Rogers (Ret.): I have someone. (laughter)

Steve Clemons: And you, and on a serious front, I mean, you had a problem with people that had been in your employ and what I understand is a tailored access operation of Booz Allen Contractor, another unnamed guy who's in jail somewhere right now, who's been there. And I'm interested in the culture and whether your, when we saw Facebook folks up here, were those, would they

want to go work for you or any of your agencies and is there a gap between the people with a real talent who, some of them are out there helping ISIS right now, and the kind of, you know, world in which you're operating from —

Adm. Michael Rogers (Ret.): So for us, —

Steve Clemons: — a national (inaudible).

Adm. Michael Rogers (Ret.): — I would tell you both as United States Cyber Command, a very traditional military organization, 80% military, 20% civilian versus the National Security Agency, 60% civilian, 40% military.

Steve Clemons: Right.

Adm. Michael Rogers (Ret.): But both organizations, we had more people trying to join the team than we have space for. I find the challenge not —

Steve Clemons: But are they cool people?

Adm. Michael Rogers (Ret.): — well, let me finish. (laughter) So I find the challenges less getting people in. It's how you retain them over time. If you, take NSA, if you come to NSA spaces, you will see individuals in the middle of the winter at Maryland in tie-dyed t-shirts, pony tails, shorts, Birkenstocks, you will see transgender, gay, my comment to the workforces, I want the best darn people we can get. And we cannot close ourselves off to it's one size fits all.

It's one reason why in our model, we have both a military component, a civilian component, and a contractor component. Through those three vehicles, I would argue it enables us to access a much wider —

Steve Clemons: And they —

Adm. Michael Rogers (Ret.): — (inaudible).

Steve Clemons: — love the culture you have, all the forms they have to fill out, all the (inaudible) they have —

Adm. Michael Rogers (Ret.): Over.

Steve Clemons: — (inaudible).

Adm. Michael Rogers (Ret.): It is an interesting -- I mentioned this before, it's an interesting leadership dynamic. How do you take a skill set that traditionally does not like hierarchy, doesn't like control, is not really into oversight all that much, and believes I should be given a problem set and a high degree of

autonomy and left to do what I need to do and how do you bring it into this bureaucratic, rigid, hierarchal structured, you know, part that I've lived my whole life in?

And that's an interesting leadership challenge and we've got to be willing to make changes and we've got to bring in, for example, the reserve component, as our UK teammates have done. You know, there's no one size fits all here. We've got to think a whole lot more (inaudible).

Steve Clemons: But some have criticized you for not cap-, you know, not having the safeguards in place, that you have these two alleged leakers and criminals, gatherers of, of classified data who've taken it out. What's that story?

Adm. Michael Rogers (Ret.): So, ongoing investigation, I'm going to get into specifics. We've acknowledged this.

Steve Clemons: I've tried.

Adm. Michael Rogers (Ret.): Right. I am proud of the fact that on my watch, we caught these individuals, even as I remain accountable for the fact that they were there and had been there for an extended period of —

Steve Clemons: How long was Ames in place?

Adm. Michael Rogers (Ret.): Oh, the (inaudible) about 22, I mean, if you go back over the history of, you know, espionage against the intelligence structure in the United States, sadly you will find examples where individuals had decades —

Gen. Amos Yadlin: This is the time —

Adm. Michael Rogers (Ret.): — of access.

Gen. Amos Yadlin: — to answer your first question. Why Israel is so good in cyber?

Steve Clemons: So tell me.

Gen. Amos Yadlin: And it's an issue of culture. These Israeli culture is innovation, not formal, debriefing, younger soldier, younger Lieutenant, (inaudible) commander what you are doing is wrong. And the eco culture, the eco climate of the intelligence, the military intelligence in Israel basically created these wonderful young people, and we have an advantage. Everybody go to the military. So we can pick those who can be the brightest and the best and send them to cyber units, call them cyber warriors.

And they have a special culture that not only helping us to be a cyber superpower, they are finishing their time of serving, can be three years, can be six years, and then they go to the, to the private sector. And over there, they are bringing the knowledge and making the high tech sector in Israel the leading locomotive of the Israeli economy. So we are gaining twice.

Steve Clemons: So Amos and Pauline, let me credit you, you've raised a very interesting point. You're taking the cream of the crop of people that you see, training them at very sophisticated levels. They eventually leave and they create capacity in the private sector. And this all sounds warm and fuzzy and wonderful. Are you training bad guys as well? Do you find, what is the worry that you begin training super empowered manipulators of this world that can go out and actually, you know, do a great deal of harm.

I'm intrigued right now —

Gen. Amos Yadlin: We are not training —

Steve Clemons: — as some of the challenges we have to —

Gen. Amos Yadlin: — we are not training bad guys.

Steve Clemons: — is that, is that ISIS or other nefarious players and other non-state actors have enormous capacity. I mean, I just want to put the threat on the table and ask how, how do those folks get so good at what they're doing?

Gen. Amos Yadlin: We are not training bad guys. We screen them, if we think that they are bad, they are not trained. But we let them be exceptional, different and Mike described it very well. Some of them never graduate high school. But they were all day on their computers, they have unbelievable innovative ideas, they know how to work in teams, and in every society, in the very, very extreme, you may find people who are, at the end of the day, finish in the wrong place.

Steve Clemons: Pauline?

Lady Pauline Neville-Jones: Well, several issues here. I mean, on the skills shortage, I think it's true. Everybody, every country in this room has a skills shortage in this area. And you have to put a national plan in place actually to train people. We've done quite a number of things, including revamping how you teach ICT in schools computer, which was so boring —

Steve Clemons: Pokémon Go festivals.

Lady Pauline Neville-Jones: — (inaudible) kids didn't want to do it. Didn't want to do it. Now, now, now it's been transformed. And we're beginning to identify

a professional cadre into which people can go. They can begin to see it as a career. It wasn't true previously.

Government's problem is, is retention, low pay. People who go into GCHQ of the Government Communications Centre, on the whole, have really interesting jobs. You can retain them. Out of sheer (inaudible) interest of, of what the organization does. But it's quite hard across government to retain these people. And I think we have to reckon that people come in, go out, come back. There's big movement now between public and private sector. And people do come back —

Steve Clemons: But to this question of —

Lady Pauline Neville-Jones: — from private (inaudible) government.

Steve Clemons: — the talent, the, the talent caliber of, of the threat seems to me to be extraordinarily high. And I understand that there's Russia, there's China, there's North Korea, there's Iran, but there's a pool of other players out there. I'm just interested in how —

Lady Pauline Neville-Jones: Yeah. You've got, you've got —

Steve Clemons: — you know, what the ecosystem of that is?

Lady Pauline Neville-Jones: — you've got several kinds of threats, haven't you? You've got the criminals, the criminal underworld, which is very big. And you have, you know, you have a black (inaudible) street, you know, you can go in, actually is a fairly uneducated manipulator of all this. You can go and buy your malware, you can go and buy your advisor to tell you actually to make this penetration. There is a whole economy there.

So it can recruit quite ignorant people. You don't have to be a great expert to become actually successful penetrators. That's one thing. And the second thing, of course, is, is when it comes to the terrorist threat that we haven't mentioned yet. But their talents there are not so much actually that they're great technologists. What they know how to do is to use social media – it is primarily social media these days – with extraordinary communication skills, which they really do specialize in, and there they're highly skilled.

Steve Clemons: Greta?

Greta Bossenmaier: Well, maybe I'll follow my colleague's lead and give you a good news and maybe two pieces of bad news.

On the good news point, we are attracting truly the best and the brightest mathematicians, engineers, computer scientists, analysts, technicians, linguists that are being brought to bear to work on the cyber security problem -- and again, not in isolation, with academia, with the private sector. That's the good news. These are extremely talented people that are committed to their country and to their mission.

Steve Clemons: So we're braced for the bad news.

Greta Bossenmaier: The bad news. I do think that as was mentioned, that we need more of these people. We're down talking in terms of the educational institutions, how do we ensure there's the appropriate pipeline of folks coming up. And one of the things I've been particularly advocating for is to get more women into the STEM subjects, into science, technology, engineering and math. I think there's an opportunity here that I'd love to see more women coming into this field.

The other piece of bad news is, again to the comment that was made by my colleague, is that the economic formula for cyber security is it's asymmetrical. It doesn't take, it's perceived that it doesn't take a lot of skill or cost to get into the cyber threat business. There are tools available. There are, you know, various levels of, the economic cost of entry is relatively low to the perceived, sometimes, results.

So one of the things we're trying to do is to change that equation. We need to make it harder and more costly for people to try to penetrate our systems, and I think that's one of the things that we're trying to do in terms of building security in from the start, making it harder to penetrate our networks, penetrate our systems. We can change that, that out of whack formula.

Steve Clemons: Mike, you're a dual hatted guy. You had the NSA and cyber command. One of your colleagues, James Clapper, has said never again should we have another of you dual hatted people. (laughter) And, and I'm interested in your own perspective on whether you think that, that having both of these responsibilities is, is wise from an efficacy perspective in intelligence?

And secondly, one of the, some of the critics of this have said that because of this, in part, the cyber command has been slow to disrupt ISIS. And I'd be interested in your kind of insights on that.

Adm. Michael Rogers (Ret.): I'm not going to get into this noise stuff. Let me give you my opinion. First, first right now, it's not my decision, nor should it be. My input to the process has been look, we're working through a process, we'll make a decision, others will do it.

Steve Clemons: But do you think it makes sense —

Adm. Michael Rogers (Ret.): Let me, if I could —

Steve Clemons: — (inaudible)?

Adm. Michael Rogers (Ret.): — just let me finish the thought. What I've said is hey look, I believe in the long run pulling them apart but keeping them closely aligned is the right, is the right thing to do. You've evolved over the seven years. Cyber Command will hit its seventh year anniversary in May of 2017. In the course of that seven years, the capacity, the capability, the things we're doing defensively within the department affects the things that we're doing offensively now that we have acknowledged in broad terms against ISIL are some really amazing work.

As we generate more capacity, as we generate more capability, I'm the first to admit that at times, there's a different perspective, different focus between the two organizations in operational command and intelligence structure. My only input to the process is we spent years building this. I think it takes us some period of time to make sure we prepare to separate them so we ensure the long-term success of both organizations cause you, the worst outcome is that we pursue a course of action that results in risk (inaudible) for either organization and I don't think is what anyone would want.

Gen. Amos Yadlin: I belong to those who think that they should be together, and let me give you my argument.

You cannot really protect and be a good cyber security guy if you don't know how to penetrate the other guy, how to attack, how to make the collection. If you try to be a cyber security expert without knowing the other side, you will fail. So I think the, the pilots – and in my background, I am a pilot – the pilot of the, the pilots of the cyber security are the second people, those who know how to penetrate the enemy systems.

If you separate them, you will lose a lot. It will cost you more because you're double your head, overhead and there will be competition. The fact that he is commanding the two make it much more —

Steve Clemons: Well, I think that John McCain —

Gen. Amos Yadlin: — the right decisions are —

Steve Clemons: — (inaudible), I think, —

Gen. Amos Yadlin: — are taken.

Steve Clemons: — I think Senator McCain's (inaudible) view, but one of the interesting things in the US case is that while Mike Rogers appears to be running all of this by, by title, you know, in our system — I think the other interesting question is Homeland Security, the Department of Homeland Security, not under Mike's authority, has enormous, has much, much more capacity in cyber, and I just, is that a smart thing? I mean, I, I'm trying to ask a question, not a political one, but more of a, one on efficaciousness.

You're head of Cyber Command and you're head of National Security Agency, but a huge block of this capacity is actually the part (inaudible) —

Adm. Michael Rogers (Ret.): I mean, the key to success —

Steve Clemons: — is that, is that accurate?

Adm. Michael Rogers (Ret.): — right, we partner with others. The Department of Homeland Security and the current US structure has overall responsibility for defence of the dot.gov domain, as well as providing federal capabilities for the private sector. And we partner with them, and doing it as we do with the FBI and other elements, both as Cyber Command and as NSA, it'll be interesting to see with upcoming changes, have an opportunity to step back and assess and say to ourselves so, we have a structure that's been in place for some period of time now, is there an opportunity to ask ourselves is it effective? Is it not effective? Are there changes that we would make? We'll see what, we'll see what happens.

Steve Clemons: Pauline?

Lady Pauline Neville-Jones: I mean, I, we belong to the culture that says take them and put the two together. I mean, if you look at GCHQ, it has two missions. It is the, it started as a second agency, you know, with a duty, among other things, to intercept communications when needed for national security reasons. It's also the Cyber Security Agency, protecting the systems.

And in the end —

Steve Clemons: So you're saying Jim Clapper is wrong?

Lady Pauline Neville-Jones: I, I don't see an (inaudible) contradiction and I think actually it, it actually results in greater understanding of, of the threats you face. And one of the things that the UK has done recently, and that is certainly a development in our public posture on cyber security, with the publication of the second cyber security strategy, which came out just about a month ago, the (inaudible) the Exchequer, who is seen to be the lead on it these days, said it absolutely explicit terms, we will have a full spectrum capability and if we are

attacked, we will reserve the right to respond in kind, in kind, not necessarily – I mean, you could, a number of ways in which you can respond, but we include in that in kind.

Now, you've got to, you know, you've got to know what you're doing if you're going to do that.

Steve Clemons: You know, the National Security party said, you know, one of the interesting things here, if you're at a cocktail party, are you folks – I don't mean this facetiously, I mean it actually seriously – in a, is your world taken as serious as it should be by the rest of the national security establishment? And I ask this with respect to the NATO Summit in Warsaw where I was there, and if you read, you know, the findings that came out, I had the privilege of interviewing Sandy Vershbow later, that a lot, I would say almost 90% of thinking about the future of war, how to position people, seem to be in a very kind of different gravitational field than what, Amos, you just defined in the, in the cyber area.

There were three or four items about cyber, a little bit more about the notion of hybrid war, but I'm interested in, in just your own sense of your colleagues in this room. Are they with it? Are they behind the time? What do they need to do in terms of thinking ahead about what warfare and, and how states are going to pursue their interests (inaudible). And I do think, and I just want to, my own view is there is a tension that, that at the NATO Warsaw Summit, this was a sideline, not a central focus. I had that discussion with Rose (inaudible) here as well.

So what, what is your view, Amos?

Gen. Amos Yadlin: You know, if you think about the 20 centuries, the century of airpower, we are in 1960. What we had in airplanes in 1960, we had airplanes made of wood and they dropped very small hand grenades from airplanes. Not efficient. So cyber is somewhere there. Maybe it will come to 2050 or to 2080 with B2 and F-16 and F15. We don't really know. And here, I'm fully with Mike. We need some time to understand whether cyber is a false dimension of warfare or some other try to be the force dimension space.

We spoke about space and in the late 80s and early 90s as the false dimension of warfare, and today's space is okay communication, a little bit of reconnaissance and certainly it's not a new dimension. So we don't know yet, I think that -- you cut me before – but cyber weapon —

Steve Clemons: But it was with a smile.

Gen. Amos Yadlin: — cyber weapon, you launch it to the enemy, it's not explode. The enemy can take it, look at it. If it has a good cyber defence, otherwise something happen.

Steve Clemons: Look at it and mimic it? Copy it?

Gen. Amos Yadlin: And can boomerang it but to you. And sometimes you, you send in cyber weapon and you don't know whether, were maybe not by the enemy, by the nature of cyber and the networks, it will come back to you.

Steve Clemons: Some people view this as saying —

Gen. Amos Yadlin: So it —

Steve Clemons: — alright, this is happening already.

Gen. Amos Yadlin: It's not happening. So it's, it's a different kind of thinking. All our military terms of deterrence attribution, peace, war, decisive victory, when you try to move them to cyber, it's very difficult to redefine that. And this job is ahead of us, based on what we will do with cyber in the coming years.

Steve Clemons: Greta.

Greta Bossenmaier: Just a quick answer to your question in terms of, you know, how important is cyber seen in the overall national security context. Even beyond national security, also it's an economic imperative as well. So just form our own context in Canada, our government has launched a cyber security review in addition to a defence policy review and a national security consultation.

But it's, a cyber review, a cyber security review, I think just underlines the importance and the dynamic nature of these issues to try to get a handle on what does this mean for the country, both from a national security perspective, and from an economic perspective, going forward.

Steve Clemons: We already have, like, 40 or 50 hands going up. I hope the mic folks are ready. We're going to go to – but let me finish with, with Mike. Mike, just, just for fun, I heard las Thursday you were in New York and how was Hamilton? (laughter)

Adm. Michael Rogers (Ret.): What was the next question.

Steve Clemons: Pauline, your, your thoughts, both of your thought on this question because, you know, I've actually had the pleasure of listening to Mike

in the past when they were, they were doing the public rollout on Cyber Command on the, some of what Amos just said is that in the, in the world of deterrents, and I remember Mike, you saying this on the record, that we needed to work with the Chinese, we needed to work with the Russians, that we need to define pathways to communicate, to create the norms in this space.

And I'm interested in how that pro-, cause I think when you did this was about a year ago. And I'm interested in, in whether or not given what you have, a lot of people have alleged about Russian hacking you, whether that process is, is bearing any fruit or whether that is a hopeless cause to try to define pattern norms and behaviours and deal with things like deterrents, you know, the line that Amos just outlined and whether or not that's happening with the Chinese and with the Russians.

Adm. Michael Rogers (Ret.): Pauline, you may go first.

Lady Pauline Neville-Jones: I think, I think this is very, I won't describe it as (inaudible) work in progress, and still right at the beginning. I think the more fruitful work at the moment is taking place between allies, actually trying to define some of the terms that we will intend to use in our approach to use of the internet internationally, the extent to which you can keep it as a free space, which is also another issue, you know, given Chinese policies and numbers.

Israel has a whole question of criminal use, and the degree of international cooperation that you can actually establish effectively to trace people —

Steve Clemons: Right.

Lady Pauline Neville-Jones: — and none of those things frankly is yet working between the various camps in the world. So I would say that we've got a very, very long way to go before we actually get any kind of international regime of a kind that you would think is —

Adm. Michael Rogers (Ret.): No, I agree.

Lady Pauline Neville-Jones: — effective.

Steve Clemons: Mike?

Adm. Michael Rogers (Ret.): I mean, the dialogue's ongoing. Clearly, we haven't arrived, you know, at a destination by any stretch of the imagination. It's another interesting aspect —

Lady Pauline Neville-Jones: (inaudible) goes on.

Adm. Michael Rogers (Ret.): — of cyber domain. It's a comment, you know, I always make within the DOD in the broader US teams that I'm a part of. Cyber is a journey, and where we are today is not where we're going to be a year from now. It's not where we're going to be three to five years from now. We have got to be open to the idea of change. We have to acknowledge that given the rate of change in this mission set, we are going to have to evolve and be open to the idea that perhaps some of our initial approaches may not prove to be opt-, optimal over time, and therefore, we got to be open to the idea of hey look, we, we've got to constantly assess and ask ourselves questions.

Steve Clemons: I don't know if this is right, but —

Lady Pauline Neville-Jones: If I can just say one thing about (inaudible) –

Steve Clemons: Yeah.

Lady Pauline Neville-Jones: — which, I mean, we are focusing particularly, I think, on the government side of things.

Steve Clemons: Right.

Lady Pauline Neville-Jones: But all our economies, in the end, depend upon our capacity to create wealth. Where does that lie in our intellectual property and mostly in our private sector. And this is, I think, the area where you begin to worry because there still isn't sufficient attention paid to the security of the assets (inaudible) which are vital to a company. And so intellect-, effective intellectual property is still going on, and you know, but there are documented cases of companies that invest a great deal in a given, a given product or invention and it turns up in another market, you can guess which, on the market before the company that's developed it can actually get there.

Steve Clemons: I've been reading a little bit —

Lady Pauline Neville-Jones: These, these are real losses and long-term losses.

Steve Clemons: Right. And it's a real battle going – I've been reading a little bit about Sergei Naryshkin on the Russian side. I guess that's one of your counterparts, right, Mike?

Adm. Michael Rogers (Ret.): Mm-mm.

Steve Clemons: And, and —

Adm. Michael Rogers (Ret.): We've never met.

Steve Clemons: — do we have – you've never met, we could get a video perhaps next year or Skype in – but, but I'm interested in, in whether you think that Cyber Command, that you had has the same kinds of capabilities to do in Russia or in China what is happening in the United States?

Adm. Michael Rogers (Ret.): I'm not going to go down this road.

Steve Clemons: Oh. Can't blame me for asking. Let me go to the audience here. Let me start with – do we have mic runners? Alright, let's go to Josh Rogan in the very back. And Josh, so just jog over there as fast as you can. I'm in favour of throwing the mics, but — (laughter)

Question: Thank you very much. I have a —

Steve Clemons: I'll give you your coin later.

Question: Thank you. I have a very short seven-part question for Admiral Rogers. (laughter)

Steve Clemons: Yeah. The clock is ticking.

Question: Yesterday, the Washington Post, a very well respected independent newspaper —

Adm. Michael Rogers (Ret.): If, if I could, let me cut to the chase.

Question: — no, no, I'm going to finish the question, sir —

Adm. Michael Rogers (Ret.): (cross talk) Let me cut to the chase.

Question: — let me finish the question. (cross talk)

Adm. Michael Rogers (Ret.): That's fine. Just let me cut to the chase if I could, cause I'm interested in saving us all some time.

Question: No, no, no. Allow me to ask the question.

Adm. Michael Rogers (Ret.): If I could, let me finish sir, and then I promise I'll let you -- I'm just not going to go down this road. I'm not going to comment on anything that's in the media. I'm accountable for my actions, I certainly understand that. It's not appropriate for me, so I just want to make – if anybody else wants to go down this, fine, you're welcome to ask, but I'm going to give you the same response.

Question: Okay. So —

Adm. Michael Rogers (Ret.): I just don't want to waste your time.

Question: — since I'm welcome to ask, allow me to proceed. Yesterday, the Washington Post, a very well respected independent newspaper and based in the nation's capital, reported that Defence Secretary Ash Carter and Director of National Intelligence James Clapper recommended your removal over a month ago to President Obama. I'm wondering did you, were you aware of this recommendation? Did President Obama speak to you about this at any time? Did this factor into your decision to meet with President-elect Donald Trump outside of the regular transition process? Did you tell Donald Trump about this when you met with him? Why didn't you tell anybody in the Obama administration that you were meeting with Donald Trump?

Steve Clemons: That's, Mike, I got to, we got to move around the room, Josh – –

Question: And do you think —

Steve Clemons: — (inaudible)

Question: — the Obama administration released this story in order to hurt your chances to become Director of National Intelligence? (inaudible)

Adm. Michael Rogers (Ret.): I go back to my previous answer and boy, we could have sure saved ourselves a lot of time, sir.

Question: I don't believe that asking questions is a waste of time.

Steve Clemons: Okay.

Adm. Michael Rogers (Ret.): Thank you.

Steve Clemons: Joseph Bahout.

Question: Thank you. Thank you, Steve. Quick question, Russia, China, Iran, what's your ranking in, in terms of efficiency in cyber warfare? The second question, very quickly —

Steve Clemons: I can only take one —

Question: Okay.

Steve Clemons: — cause we've got 50 questions out there. So Russia, China and Iran, great question. Let me ask Amos.

Gen. Amos Yadlin: No doubt that Russia and China are superpowers. I wonder whether Iran is in the same level.

Steve Clemons: Where's Israel compared to them?

Gen. Amos Yadlin: With China and Russia. (laughter)

Steve Clemons: Interesting. Greta? Greta, comment?

Greta Bossenmaier: There, there's a lot of different threat actors out there. We've talked about nation states, we've talked about terrorists, activists, criminals. I don't really want to get into a ranking game. I think the reality is there's a number of threat actors out there and it's a very —

Steve Clemons: Do you think —

Greta Bossenmaier: — involved —

Steve Clemons: — non-state actors are of increasing weight in this field?

Greta Bossenmaier: I think there's an increasing number of them. That's a very good question. And it goes back a bit to my earlier comment about, you know, relative low cost of entry. So I think there's more of them trying to do different kinds of things.

In terms of the actual impact they have, we're seeing different types of impact. We're seeing (inaudible) service activities, but I think the verdict is still out in terms of what the real impact —

Adm. Michael Rogers (Ret.): Can I —

Greta Bossenmaier: — (inaudible)

Adm. Michael Rogers (Ret.): — (inaudible) though, remember, the greatest segment of activity out there is criminal, remains criminal. And those are predominantly —

Steve Clemons: Are these drug cartels, are they —

Adm. Michael Rogers (Ret.): — non-state actors.

Steve Clemons: — you know —

Lady Pauline Neville-Jones: I think quite a lot (inaudible) —

Gen. Amos Yadlin: The 16-years old boy and the terrorists in the cave or in the, in the basement are not a concern. Concerns start from criminal organizations that have resources, that have many people that can recruit. And they can reach to a state level.

Lady Pauline Neville-Jones: But just going to say I think many of the independent actors, the lone individuals are more in the game of disruption than they are actually of gaining anything very effective.

Steve Clemons: Howard Dean. Just very quick, we're going, we're going to bring you a mic cause literally, there are, I'm not exaggerating, millions of people watching online right now, so make it good, Howard.

Question: A very quick one for Admiral Rogers, which may be classified. But if, if, if we retaliated for what they, the Russians did in the election, is, or if we didn't, excuse me, is one of the considerations that by reta-, we'd have to wait for the right time because by retalia-, they will then know a whole lot more about our system than we want them to know?

Adm. Michael Rogers (Ret.): I mean, there's a whole lot of factors that go into a policy decision about -- take Sony as an example – where we, both publicly now as the activity, we publicly attribute it to the North Koreans, and then the President of the United States talked about very publicly we're going to take direct action in response to this. We opted to use a non-cyber lever, in this case economic, and then in addition, we said if this fails to achieve the desired outcome, we are prepared to take additional action at the time and place of our choosing.

One of the reasons I highlight that is I try to tell people look, there is no one size fits all to this problem. Every situation is viewed as something unique. The other testament, I think that's important or kind of foundational principle, I'm a big proponent of just because someone comes at us in cyber, doesn't mean the default mechanism has to be we have to respond in kind. I believe we should play to our strengths as a nation and those of our friends and allies, and we should think more broadly. We'll see how this plays out over time.

Steve Clemons: You know, and when the North Korea-Sony case happened, Lisa Monaco and Fran Townsend did an event with The Atlantic and Fran strongly indicted Sony's management and other corporations out there that weren't taking the precautionary steps that they should. I'm interested in just from all of you as you deal with the private sector, you've talked kind of nicely about partnership, how derelict or how with it is the private sector in addressing these problems?

Pauline?

Lady Pauline Neville-Jones: It varies. (inaudible) it varies. Actually, I think you begin, you can begin to say that well run companies have taken this aboard and it's the less well rounded companies that actually, and they can find themselves deficient. And I come back to what I said earlier on in that there is no such thing as perfect security. You must have resilience, you must know what you're going to do when you are penetrated. And Sony hadn't got their act together.

Steve Clemons: Mike?

Adm. Michael Rogers (Ret.): I think the phrase I'd use is uneven. And many companies, you know, if you look at the high (inaudible) and the financial sector, you have several banks among the largest in the world that have publicly announced their baseline for cyber security every, every year, annually, is half a billion dollars. How many companies can afford an annual investment in just preventative baseline work of half a billion dollars. I, for me, it's uneven and then secondly, I worry a little bit less at times about the largest segments within a particular sector in the mid and the smalls because they don't really have their, the resources.

Steve Clemons: Greta?

Greta Bossenmaier: Very much along the same lines. The private sector's not one homogenous group. And there are, it's companies now taking, having the realization that this is a, you know, board, you know, board level kind of issue they need to deal. This is a business risk issue, —

Lady Pauline Neville-Jones: Exactly.

Greta Bossenmaier: — put it into the risk matrix that businesses have to deal with and pretty soon, you'll find that people are taking this very seriously and it's not only investment, but it's also that senior level engagement around a business risk.

Steve Clemons: I wasn't joking earlier when I read about you in Parent Influence Magazine Canada. Are you regularly interfacing and interacting with private sector leaders on infrastructure? Is there a, you know, a regular rapport that you're building with them?

Greta Bossenmaier: We work – and I'm going to come back to the partnership angle again – we work in partnership with other components in our government, and with the private sector in terms of being able to provide advice and guidance and we're both learning. I mean, it's a two-way street in terms of learning.

Steve Clemons: Amos.

Gen. Amos Yadlin: It's an issue of cost benefit. If you are a private sector company, you want to make money. If you defend yourself in a, in a way that you spend all your money on defence, you're going to lose your company. So it's, you have to do the sweat assessment, you have to define what is the (inaudible) that you want to protect and don't protect everything because I told you, somebody will be (inaudible). So protect the real important (inaudible) of your business and it's a cost benefit analysis that you should have to do with experts.

Steve Clemons: I just want to take this public moment to thank Israel and Amos and whatever role you had in for the app called Ways. It's, it's (applause) you may not know (inaudible) but I just want to basically put that on the table. Yes, Dixon Osburn right here.

Question: Hi. Dixon Osburn, Centre for Justice and Accountability. We were talking about cyber threats, but can we do the flip side of that, which is government transparency and accountability? What can we do to reduce the over classification of communications?

Steve Clemons: Right. Over classification, height of secrecy. Pauline?

Lady Pauline Neville-Jones: Well we've had —

Steve Clemons: I, I just want to – yeah, when, when you, when you, when Theresa May, the now Prime Minister of England, was head of I guess Home Affairs, and you told her she wasn't cleared and couldn't get a report, I just found this a very juicy moment that many people may not know, but, but on the issue of secrecy and who's in and who's out.

Lady Pauline Neville-Jones: I think there's something (inaudible) about this story (inaudible). (laughter) I mean, the, the, the essence, I suppose, of good classification is keep it to the minimum. And we've had a reform over the —

Steve Clemons: Is anybody keeping —

Lady Pauline Neville-Jones: (inaudible)

Steve Clemons: — it to a minimum?

Lady Pauline Neville-Jones: Well, there's always a temptation, isn't there in any human to, to put the word confidential on when it doesn't need to be. We have, recently had a real reform of the whole system, and there is now a great deal of, of paper that used to have a tag on it which no longer does.

The second thing is, of course, is who has access to what?

Steve Clemons: Right.

Lady Pauline Neville-Jones: And actually who accesses what is quite as important as what label a piece of paper or a communication bears. There, there I think, that's where the real control lies. It's not in classification, it's access to, to it. And you have to get those, in a, in an electronic world, you have to get those two things in line. So, I think it's, it's quite important for, for governments and organizations to get there, and a lot of companies do have, you know, limited access and they're quite right too.

And you've got to get that in line with real responsibilities and not with nominal status. So there's a lot of things to do actually, to make both your, your classification system efficient and not (inaudible) stifling.

Steve Clemons: As I go to the rest, I think it's a very important question. In the early 1980s, a bunch of Sovietologists, Arnold Gorlick was one of them, but the leading Soviet experts in the country campaigned with Bill Casey, then head of CIA and said you know, the problems of official secrecy are stifling our ability to understand what's going on in the world to do with this. And when I think back to that time in 1984, when this effort was done, I mean, there just, the growth of official secrecy has been staggering.

So, Mike, I'm interested, not in the kind of soft notion that reform, I mean, is it a problem for your, from your guys perspective or is it something that we just need to —

Adm. Michael Rogers (Ret.): I think particularly —

Steve Clemons: — accept?

Adm. Michael Rogers (Ret.): — in the world of cyber security, it's something we got to continue to get better at. I feel very good when you see high profile activity. What concerns me is that's not enough. We got to get this to the day to day so we get real time information flowing back and forth. And as a government guy, my, what I always remind our workforce is the measure of success needs to be defined by the individuals who are providing the data to us. What's the right foreman at the right classification level? What is the essential data that they need, not what do we think they need. And that is an area we got to keep working harder on.

Gen. Amos Yadlin: Chief of Defence Staff from UK want to ask a question.

Steve Clemons: Yes.

Greta Bossenmaier: But may I just come in on this, on this issue though in terms of transparency cause it's really an important issue. And it's one that I think that we've made a lot of strides but we need to do more. We've done our first ever technical briefing this year. We've watched our Twitter accounts this year. We're making a lot of efforts to be more transparent. At the same time, I think that Canadians understand and expect that we can't tell everything we do in terms of our targets or our methodologies or capabilities cause it impedes our ability to keep them safe.

Steve Clemons: I'm so tempted to ask about real news or fake news being tweeted, —

Greta Bossenmaier: — but I do —

Steve Clemons: — from an intelligence (inaudible) but I won't.

Greta Bossenmaier: — but I do believe that, again, this is of a priority for me as a leader of the organization, is how we can be more transparent around our activities.

Steve Clemons: Pauline, you want (inaudible).

Lady Pauline Neville-Jones: I just wanted to add that, I mean, you know, not over classifying is very important, but I, I think it's overrated as a problem about government. I think one of the more fundamental problems is the closed mind. It's operating inside that circle, you know, and forgetting about the outside world, and actually not communicating with it. And that's, that's very, very easy for the average civil servant to fall into that.

Steve Clemons: Just, just before I go here, which I will, I'm going to give you a coin for your question, but Mike, what, what, you know, for those of us who sit on the outside, particularly in journalism or NGOs and we're worried about this, what do you think our blind spots are, that we're not understanding about you, that you feel that we're beating up on you too much? What do you think is the, you know, defending?

Adm. Michael Rogers (Ret.): I'm not, look, the press has an incredibly important role. It stood our society – I only speak for our nation, for 241 years as a nation, it has stood us in good stead. Is it challenging at times? Heck, yeah. But you know, the challenge at times is I wish there was a little bit more of a dialogue, but Sir Peach, who's been waiting a long time.

Steve Clemons: Yeah. You got your, your Halifax Forum coin.

Question: Hi. Sir Peach, —

Adm. Michael Rogers (Ret.): But you got the coin.

Question: — Chief of Defence Staff, United Kingdom. I think I'd like to go right back to the beginning of the session and something Amos said in his very first intervention. Actually, throughout human history, states and military actors have always positioned for advantage and they're using cyber to do so now. So actually, I think there's a symmetry to the way in which cyber's being applied across the spectrum of warfare by states and as the panel made clear, non-state groups and criminal networks, which actually may need to be met with a symmetrical response.

And one of the dangers with topical debates, is to try and create something that is new. Actually, espionage is not new, stealing IPR to save your 25 years research into new weapon systems is not new. But people are using this way of stealing information, of positioning for advantage, of being first with the story to make for success on operations.

And I think there's something about the debate by being so topical and inventing new terms, I agree strongly with Amos, that traditional terms of warfare do not apply to cyber, but we need to be really careful that cyber doesn't become the real Achilles' Heel of the western way in war, because actually, we, I've always applied the spectrum of electronic spectrum to operations and we need to continue to do so. And sometimes, the response may not be a cyber response, it might be an electronic warfare response or a kinetic response.

So I just would caution, as a military man, that the debate —

Steve Clemons: (inaudible) before you close out —

Question: — (inaudible) all about you.

Steve Clemons: Yeah, before you close out, how worried are you about that Achilles' Heel question? It goes back to my comment about yet, and as you look forward, I mean, you wouldn't be articulating this in the way you said if you didn't see this as a growing concern. So as you simulate this, look, I mean, how worried are you given trends? Because this is not a warm and fuzzy world. This is a world of people that are trying to basi-, so I'm interested in how worried you are about that —

Question: I, I believe we —

Steve Clemons: — that part of the Achilles' Heel?

Question: — in the military, operational sphere, we need to remember our discipline, our discipline about communication security, our discipline about

operational security, our discipline of not joining the social media as servicemen and telling everybody what we're about to do on operations. So actually, I think there is a discipline which is necessary in the modern age in order to defeat the things the panel has talked about.

Steve Clemons: I just want to say to the organizers that I haven't heard anything about time in my ear, so I don't know if this working and —

Gen. Amos Yadlin: (inaudible).

Steve Clemons: Yeah. But, but we're going to you in a second. Rosa Brooks over there.

Are we going to 11:45 or longer? Is someone going to tell me?

Question: Thanks. Hi. Rosa Brooks, Georgetown University. A quick question. I wanted to go back to the issue of attracting and retaining top talent. More and more, certainly in the United States, the math PhD students, the smart cyber folks are not US citizens at our universities and, or if they are US citizens, they come from families that have very strong ties to many foreign countries, some of which are on our not friend list. What do we do about that? It means they often can't get security clearances. Obviously our strength is our diversity, but how do we make sure that our efforts to stay secure, we don't cut off our nose to spite our face?

Steve Clemons: Mike?

Adm. Michael Rogers (Ret.): It's an interesting challenge. If you look at other problem sets where we've kind of had the same issue, like, take language for example, particularly in the wars of the last 15 years, we created mechanisms where we provided access to linguistic skill for a particular type of language we wanted them to translate or provide feedback on. And part of me is wondering is there a tier-like approach that we can take within this mission set where you could potentially bring people who you might have some concerns about, that you might want to actually give complete access to everything, but on the other hand, they bring a particular skill and the risk to go to, you know, one of the points Greta made, is reasonable. I think we may find ourselves going down that (inaudible).

Steve Clemons: Quick responses Pauline, Greta?

Lady Pauline Neville-Jones: Well I, I mean, I think in the UK, we're pretty rigid on this issue, you know, you've got to have UK nationality to get into any area with (inaudible) government service. The private sector, a different matter. The private sector needs to be careful, you know, cause these are our valuable

secrets for, potentially for, for other powers. So it's, I think it's one of the few areas now where government remains less open to, to employing people who are not, not a home nationality.

Steve Clemons: Right. Greta?

Greta Bossenmaier: Well, I think to the point I raised earlier, whether it's women or having a diverse workforce, I think we all benefit from having a diverse workforce that can bring different points of view and different perspectives to bear. At the same time, we have to respect the security clearance processes that we have.

Steve Clemons: Right. And Amos, you have a sort of intelligence system built in with everyone joining the military, I suppose?

Gen. Amos Yadlin: Yeah. I think diversity is important. Cyber needs out of the box thinking. And if you need out of the box thinking, you better have a diverse population.

Steve Clemons: Terrific. Yes. Hi.

Question: Hi, Heather Roff, University of —

Steve Clemons: Why don't you stand up?

Question: Heather Roff, University of Oxford and the Global Security Initiative at Arizona State. I have a question for the full panel. I'd like to know how you all feel about encryption, particularly when some governments, or at least some folks in governments have rallied against encryption, particularly in the UK, for instance. And if you do like encryption, you think it is good for everybody in an overall security, then how does that square with many governments and militaries' pursuits of quantum computing?

Steve Clemons: Great. Thank you. So quick answers on encryption, Amos.

Gen. Amos Yadlin: Encryption is one of the reasons that not every kid can break to everywhere. Encryption is very important in the cyber realm. And very much like other cyber parameters, it can go both ways. We don't know where it's going. It can go to a place that even superpowers will have difficulties to break encryption. It can go to artificial intelligence or some other invention that may, may break encryption as we know it. We do it totally different. And this is one of the $64 billion question. Where encryption is going.

Steve Clemons: Right. Greta?

Greta Bossenmaier: As a cyber security organization, encryption is, is key to how we protect the Government of Canada, Canadians in information. That's the key part of how we do our business. At the same time, there's a debate going on, you know, in a variety of countries around what happens when nefarious people, (inaudible) actors are trying to perhaps hide behind the veil of encryption. That's a discussion that's happening. It's playing out across our nations and an important discussion, I think, to have.

I'm glad the issue of quantum computing, you've raised that. It's one of the ones I wanted to come in on, if we could, at the end. We've said that, I think a number of us said that the whole challenge around cyber security is about to get a whole lot harder because of quantum computing. Offers huge potentials in terms of science and engineering and benefits for, for our populations. But from a cyber security perspective, it's going to make our jobs a whole lot more difficult, which is an imperative for us to be able to try to get ahead of that curve and to work with academia to be able to —

Steve Clemons: Thank you.

Greta Bossenmaier: — address the —

Steve Clemons: Mike, your thoughts?

Greta Bossenmaier: — quantum challenge.

Adm. Michael Rogers (Ret.): Encryption is foundational to the future. Anybody that things we're going to walk away from this, I don't think understands what's going on in the world around us. Encryption, though, to me is the kind of epitome right now of the disconnect we have between the current state of technology and the (inaudible) policy frameworks that we have in place. And collectively, as societies, particularly democratic societies, we've got to figure out what's the right answer for our societies. You don't want people like me making that decision unilaterally. I don't look to companies to do that unilaterally. We have got to collectively figure out what's the right answer here.

Steve Clemons: Pauline?

Lady Pauline Neville-Jones: I agree. I mean, encryption's coming and a lot of diverse voices are, are (inaudible) are ahead in the UK, but the government is very clear, encryption's coming. We'll use it when, and we'll use quantum when it comes. And our parties are going to use it. It changes the nature of the, of the activity. Encryption, after all, can make your communications more secure. It also means they're harder to break.

Steve Clemons: Right.

Lady Pauline Neville-Jones: So these are the old trade-offs. And there's a whole debate, I think, behind the question, which is, you know, what rights and under what conditions do governments have the right actually, to break in.

Steve Clemons: I want to apologize to everyone. There were so many people I've winked at implying that I was about to get to them. This gentleman, (inaudible) and others, I've been asked to wrap it. We're right near the end of the session. But I guess in closing, I, I, there's one 900-pound question that I myself worry about that I've just got to put on the table, and I just want to get very short thoughts from you as we wrap this up.

Donald Trump is going to be the next President of the United States, and he was elected, but during that campaign, he practically asked for other governments to hack, and I'm interested in the question of literacy and leaders. So, so both about, you know, we can about Donald Trump, but, but I think literacy of civilian leaders in dealing with an extraordinarily complex set of challenges, and I'm interested in how each of you, whether you worry about the gap between Theresa May and the intelligence community between a Donald Trump and what the realities and, you know, that you just sort of scoped out.

Amos, you just said the rules are just very different in this world, and I'm wondering whether we need to worry about that literacy challenge among —

Gen. Amos Yadlin: It's Chief Intelligence Officer —

Steve Clemons: — political leaders who do not come out of this. Go ahead.

Gen. Amos Yadlin: — a Chief Intelligence Officer or a Chief Cyber Command has the duty to educate, to educate the political echelon, the political masters of his. And this is not only about cyber, there are other issues that since you are there 24/7 and they are —

Steve Clemons: And so what grade would you give BBnet and Yahoo on cyber literacy?

Gen. Amos Yadlin: He is very good on cyber.

Steve Clemons: Okay.

Gen. Amos Yadlin: And —

Steve Clemons: So it's an A.

Gen. Amos Yadlin: A minus.

Steve Clemons: A minus. (laughter) Okay. Greta?

Gen. Amos Yadlin: It's a very high grade.

Steve Clemons: Greta, how about Jus-, how about Justin Trudeau?

Greta Bossenmaier: Well, I'm not in the, in the grading scheme, but I think I would maybe approach it from a little bit broader perspective.

Steve Clemons: You'd make major news if you graded Justin Trudeau, right? (laughter)

Greta Bossenmaier: As we said in the beginning, this is a very dynamic environment. it's hard for anyone to be able to stay on top of all this all the time. So I think it's incumbent whether, again, it's in the corporate suite of major institutions, major commercial corporations, whether it's a private citizen, whether it's government. I think it's imperative on all of us to remain very agile and very well informed on such a dynamic issue.

Steve Clemons: Right. Mike?

Adm. Michael Rogers (Ret.): I'm not doing grades. But I'm, look, cyber's no different than any other challenge for a leader. No individual has perfect knowledge of every issue going on in the world that's going to shape and drive their environment. So the key always is you get good people, you get a broad disparate set of opinions and you try to come together collaboratively to work out solutions. I'm very confident in our ability to do that. There is no doubt, you know, these are not easy topics, but I'm confident in our ability to come together and keep moving forward.

Steve Clemons: Do you think, you know, the Hillary Clinton debate about e-mails and, you know, she sort of thought this was standard practice, are there things that we're doing today that we'll look back on five years from now as criminal, Mike?

Adm. Michael Rogers (Ret.): I wouldn't say criminal, but as our knowledge continues to grow, we'll certainly come to realize over time that perhaps some of the things we've done historically had carried a greater (inaudible) risk than we were aware of at the time.

Steve Clemons: Pauline?

Lady Pauline Neville-Jones: Well, I think David Cameron got it, and I think Theresa May gets it. I mean, a bit surprising that (inaudible) didn't. but I think what I would say is that I think that, you know, political leaders, they don't have

to have an absolute profound understanding of the technology. They do have to have some grasp of it, in my view, in order to be able to do what they do have to do, which is actually distinguish the right policy implications and the right policies. And there, I think that the system needs to help them and, you know, they get the nuclear briefing, they should get the cyber briefing these days.

I mean, this is, you know, they need help in order to do their job. (inaudible) we should commit to them.

Steve Clemons: Well, I want to thank you. I don't know if we fixed this spies love us riddle, but this has been a (inaudible) conversation. So please give a round of applause to Baroness Pauline Neville-Jones, Admiral Michael Rogers, Greta Bossenmaier and Amos Yadlin. Thank you all very much. (applause)

Lady Pauline Neville-Jones: Thank you so much.

Adm. Michael Rogers (Ret.): Always a pleasure.

Steve Clemons: And for those of you who asked great questions, I have your coins.

- 30 -