TRANSCRIPTION/TRANSCRIPTION
EVENT/ÉVÉNEMENT
Transcription prepared by Media Q Inc. exclusively for Halifax International Security Forum

DATE/DATE: November 23, 201914:45 AT
LOCATION/ENDROIT: Westin Nova Scotian Hotel, 1181 Hollis St., Halifax, NS
PRINCIPAL(S)/PRINCIPAUX: Shelly Bruce, Chief, Communications Security Establishment
Golnaz Esfandian, Senior Correspondent, Radio Free Europe/Radio Liberty
James Appathurai, Deputy Assistant Secretary General, NATO
Andrii Zagorodniuk, Minister of Defence, Ministry of Defence, Ukraine
Lyse Doucet, Chief International Correspondent, BBC World Service, Canada; and, Moderator
SUBJECT/SUJET: Plenary 5 at the Halifax International Security Forum, entitled "2020s Vision: Responsibility to Pro-Tech".

Lyse Doucet: Ladies and gentlemen, welcome to our next panel discussion. And again, because I told you I come from the Maritimes, you have to indulge me. It's so unjust. You wear your lobster pin, and you say you're from here, and then they say you're part of the family, which means we can tell you what to do. So when Edward Luce had to drop out at very short notice, me, the Maritimer, was asked to stand in.

So I'm appealing to all of you to help this be a conversation about all of us. And why is that so crucial? Because when we discuss the responsibility to be pro-tech, or, in other words, who's responsible for protecting us, it's not just about those big cyber hacks that hit the headlines with such irresistible names, like Stuxnet or WannaCry. This is not also just about the accusations of meddling by Russia or other state or non-state actors in elections the world over.

And this isn't just about the growing power of the tech giants in our democracies and beyond; not just about the increasing sophistication of facial recognition software and other related technologies and artificial intelligence in China and other countries. This is about all of us carrying our smart phones, carrying our computers. You may have seen on your – in your e-mail traffic the poll carried out by Ipsos and the Halifax Security Forum, in which three out of four respondents, 75 percent, said the greatest security threat facing us today is not an attack; it's the hacking. It's the hacking of our data, either for purposes of fraud or for espionage. This is one of the challenges of our time. The technology which has transformed all of our lives with its dazzling power to bring us together is now pulling us apart. It's weaponizing the Internet, and has the great power to damage our democracies. I urge you to read the very good essay by Pauline Neville-Jones, which is in your book, The Halifax Papers, about 2020's The

Responsibility of Pro-Tech.

We have a great panel of experts here who are confronting these issues day in, day out. In fact, it may be keeping them up at night. And we have all of you. First of all, we're very privileged to have the Minister of Defence from the Ukraine. If you think you have problems with your data, imagine if you were the Minister of Defence for Ukraine. Andrii Zagorodniuk, educated at Oxford, now defending the state of Ukraine, welcome. Welcome. Thank you for joining us.

Andrii Zagorodniuk: Thank you. Thank you very much. (Applause).

Lyse Doucet: My fellow Canadian, James Appathurai, who is the – NATO's Deputy Assistant Secretary General for Political Affairs and Security Policy. We don't usually ask these things at the – at the Security Forum, but because it's Halifax, James' teenagers are going to be watching. They said Dad, you're going to be talking about technology? So please, when you give a question to James, say wow, you're such an expert on this, you know so much. (Laughter). It'll just help him back home. (Laughter)

Golnaz Esfandiari, a colleague of course, is the Senior Correspondent for Radio Free Europe, for Radio Liberty. And also, we have – we're very pleased to have here Shelly Bruce, who's the Chief of Communications Security Establishment, in other words, Canada's centre for cyber security, the Canadian equivalent of GCHQ. But here she's just taking care of her – her pi—her part in the panel.

Minister, let's begin with you.

Andrii Zagorodniuk: Sure.

Lyse Doucet: You're about to decide what to do about, for you, what is the biggest challenge when it comes to the – the power of technology to create problems, in your case for a government, for a nation.

Andrii Zagorodniuk: Yeah. We are – I'm – I'm from the country which we're a hybrid. Our history is being written as we speak. And all different (inaudible) and influences, people and processes differently (inaudible). So if we're talking about cyber – cy—cyber, that impacts the data, and it impacts the security of the networks of the critical infrastructure and so on. We – we have cyber attacks daily, like multiple every day. And that's what we have to deal with, like – like, all the time.

Lyse Doucet: From whom?

Andrii Zagorodniuk: From Russia, usually.

Lyse Doucet: And you – you --
Andrii Zagorodniuk: Not always, but -- but usually --

Lyse Doucet: -- how – how can you be sure it's Russia?

Andrii Zagorodniuk: Well, because sometimes you can trace these things and sometimes you can find out where it comes from, and sometimes the patterns. The biggest issue with the attacks is that you have to recognize the pattern as quick as you can. And sometimes in – in various hybrid attacks, the – understanding what's happening is – is the key. Because reacting to this rather than proacting or reacting very quickly is – is the difference between the success and failure in a – in encountering this.

But it's not only cyber; it's also the information attacks. And they are – if he cyber deals with the hardware, information campaigns, they deal with the people's perceptions and people's minds and their opinions and shaping opinions the way that is, you know, needed by – by the ones who started it. And (crosstalk) --

Lyse Doucet: And this is what all you see on the Inter—this is (crosstalk) --

Andrii Zagorodniuk: Oh, it's – it's – oh, yeah. This is a whole – the whole – there's a whole school of doing this. And it – the biggest problem of, well, kind of what you had to deal with, is this – the technology's constantly evolving. So you can't be ready because tomorrow something new may happen. And the information campaigns, they are especially dangerous in democratic societies because it's where people's opinion matter. You know. So by creating the – shapings people's opinions and influencing decisions, sometimes the chaos is created. And since our enemy, Russia, you know, they have a doctrine on creating chaos, where the military side comes at the end. So it's much easier to invade the country where – where is the social and economic and – and technological chaos.

Lyse Doucet: So – and you – as far as you see, this is the most powerful weapon, if not one of – one of the most (crosstalk) --

Andrii Zagorodniuk: It's --

Lyse Doucet: -- (off microphone) in the armoury of Russia.

Andrii Zagorodniuk: It's – it's very powerful, yes.

Lyse Doucet: Hmm.

Andrii Zagorodniuk: And obviously. So that's --

Lyse Doucet: If you had the means, you'd – this is always (crosstalk) --

Andrii Zagorodniuk: Well --

Lyse Doucet: -- the question, is that you have to keep up. You've – the – either your enemy or your rival develops something in terms of technology, then you have to --

Andrii Zagorodniuk: Yeah, you have to keep up.

Lyse Doucet: -- (crosstalk) to – to keep up with it, and then --

Andrii Zagorodniuk: Yes. And all be one step --

Lyse Doucet: Are you keeping up?

Andrii Zagorodniuk: Yeah, and all be one step ahead. Yeah, absolutely becau—well, obviously we have these various turmoils and – as you know, I mean, but at the same time, we – we still develop, we still – the – the economy grows, the – you know, the – the armed forces become stronger, democracy becomes stronger, which means they're failing at the end. But still, that's – we go through this daily. Yeah.

Lyse Doucet: So you – you – do you think you're winning in this?

Andrii Zagorodniuk: I believe so. Yeah.

Lyse Doucet: Not – or your constantly --

Andrii Zagorodniuk: Yeah.

Lyse Doucet: -- just trying to (crosstalk) --

Andrii Zagorodniuk: I'm – I'm here.

Lyse Doucet: -- keep up. You're here, so – We don't know what's happening back there when you're here.

Andrii Zagorodniuk: Certainly. Well, we do. I just had a call just to check everything's fine before I came here on the panel. (Laughter).

Lyse Doucet: OK.

Andrii Zagorodniuk: But yes, yes. So we – we are – we are winning, but – and – and again, but it – see, this thing is that you see the battles when the tanks and the ships and – and everything. We have that as well. But you don't see that – those battles, and they happen, like, as – again, as I say, as we speak.

Lyse Doucet: OK. Well, we're going to come back to you.

Andrii Zagorodniuk: Sure.

Lyse Doucet: I'm going to just pick up, then, on what you said. Shelly Bruce, do you think you're winning?

Shelly Bruce: Well, it's a really interesting conversation because every time you pick up the newspaper, every day, or you check out the – the – your clippings, you'll see more and more incidents that are being captured in terms of entities that have been exploited on the cyber dimension. And at that point, then, we're trying to respond, as the Minister said, and deconstruct it into indicators of compromise so that we can then put those indicators into the system and make sure that we can detect new activity, and then hopefully eventually prevent it. And so the conversation is largely geared towards the sensational end of it and who are – who are the victims and what is the impact of that. And I think at the national level what we're trying to do now is to really shift the – the conversation, as much as we need to clean up when we need to, when incidents happen, to shift that conversation back to the prevent end of the spectrum and make sure that we are trying our best to set ourselves up so we're not victimized by these kinds of attacks.

The bottom line is that most of these incidents are the result of – or are – are perpetrated through known vulnerabilities. And so the more we can do to practise good cyber hygiene, cyber – the basic cyber security practices around good passwords, around updating your operating system when you get the prompt, around, if you're a system administrator, patching, or, you know, any of the other basics, really, really helps reduce the threat surface that exists for any entity.

So at the national level in Canada we've done a few things, and I'd just maybe mention a couple of them. One is that we've created a centre for cyber security, the Canadian Centre for Cyber Security, which is based on, you know, 70 years of expertise at CSE in the ComSec, the communications security space, but we've also pulled together all of the operational expertise from across government. So we've consolidated into this centre, so we have one national touch point for advice and guidance. We've focused very much on protecting government networks right now, and, as a result of that experience, we've been able to – we're stopping about a billion actions a day against the Canadian government networks.

Lyse Doucet: A billion?

Shelly Bruce: A billion on top of commercial enterprise networks.

Lyse Doucet: What does that mean? I mean, translate that for – into real language into – is that – what does that mean? How is – how does that take shape, the billion --

Shelly Bruce: So government networks are protected by commercial-grade defences. And what CSE has done is put more defences on top of that, and we use the information we have at our disposal. We are of course also a signals intelligence agency, so we monitor foreign cyber threats. So we're able to translate a lot of that into indicators that we can then use to add an additional layer of protection onto the government networks. And now we have also received new legislation that allows us to take some of that information and help critical infrastructure owners and operators so –

repackage that and help them out in th—in their defences.

Lyse Doucet: It's – are these billion state or non-state actors?

Shelly Bruce: (Crosstalk)

Lyse Doucet: I don't know how much you can tell us, given --

Shelly Bruce: (Crosstalk) these are just actions that are coming against the government that need to be blocked, otherwise --

Lyse Doucet: Like, can you – you share --

Shelly Bruce: They could be scanning – scanning of – for vulnerabilities. They could be very basic --

Lyse Doucet: Is it so sophisticated it must be a state?

Shelly Bruce: No. No. Not at all. I mean, we are – take a very agnostic approach, so we don't really care who's behind it at this point.

Lyse Doucet: Really?

Shelly Bruce: We just – well (crosstalk) --

Lyse Doucet: I mean, the Minister of Ukraine has to know who's behind it because it's --

Shelly Bruce: Eventually maybe --

Lyse Doucet: Yes.

Shelly Bruce: -- it's important, but it's more important --

Lyse Doucet: But Canadian – Canada doesn't?

Andrii Zagorodniuk: It's more important to make sure it doesn't happen. And then you don't need to worry about who's behind it. So the activity in – that we do on a daily basis I think is – has helped raise the bar for the Government of Canada. And we're – we're happy to be providing that – we've also put out tools and tradecraft based on that and put it into the open source development space so that other people can have access to it.

The legislation that was put forward also provides Canada a new tool in its toolbox to reach out and conduct defensive cyber operations in infrastructure outside of Canada. So that is a capability and an authority that had not existed before. So if – if malicious

activity is directed at Canada, we can take action to neutralize that activity.

The third thing that we've really been focusing on and investing a lot in is awareness, and just raising that awareness. If – it – it's – it's a lot more interesting perhaps to talk about the political intrigue of – of who's doing what to whom, but it's really, really important to have those conversations. And when you think about the number of people on line, from kids of five years old through to, you know, seniors 105, that – that's a very broad spectrum of people you need to reach. And people are a bit overwhelmed by information these days, so we're trying very hard to find the opportunity to get them when their attention is piqued. So for example, during this last electoral process, really working with the political parties, campaign managers, people who were running, candidates who were running, and make sure that they have advice and guidance that can help protect them, especially when they're – they're hypersensitive to the risks that are out there, based on their specific circumstances.

But it all adds up to really being resilient as a nation and – and trying to push more conversation into the prevent space so that it can raise the national bar and raise the costs to adversaries trying to penetrate your systems, whether or not they're cyber criminals or state actors or adventurists who just are looking for a good cyber time.

Lyse Doucet: Oh. OK. I'm sure there'll be – there'll be questions here. But I'm going to (inaudible) Golnaz Esfandiari now. Of course journalists are in the position of both having to cover instances of cyber hacking, trolling, intelligence issues, and are also affected by it. What do you seek, to perhaps discuss one of the main challenge – I know your special interest is in Iran, where we have seen how the weap—the Internet can be weaponized.

Golnaz Esfandiari: Yup. Since Oc—since November 16, 80 million people have been offline in Iran. The reason is that there've have been protests. Iran has raised the price of gasoline, and people took to the streets on November 15th. A few hours later, Iran shut down the Internet. This is the largest Internet shutdown probably in any country. It's been down a week, and it's just coming back. People are being connected. But for a week it was only five percent Internet connectivity compared to normal levels. And those five percent were probably state institutions and some universities. So it's basically a collective punishment, what Iran has done, because of these protests, because it wanted to prevent protesters from organizing themselves and also from informing others, informing the outside world about what's happening in that country.

So basically, Iran had something, was doing something that it didn't want the world to see. And now, slowly, we are receiving information, we are receiving videos, which appear to be probably one of the harshest crackdown that happened in that country. Within only a week, Amnesty International has said that 140 people have been killed probably, and that's a conservative estimate. Other estimates are 300 people have died. The videos are horrible. It looks like a war scene, you know, and you see the police forces shooting at people.

But what's very, very concerning is that Iran had been preparing itself for this moment for ten years. Ten years ago, Iran faced protests, the 2009 protests against the re-election of a hard-line President, Mahmoud Ahmadinejad. So people took to the streets and they started using their cell phones to send out videos of the crackdown and of the protests. And I'm sure you've all seen the video of Neda, this young girl who was killed. He was shot dead in the street in Teheran. So to prevent that, this time they don't want any symbol, they don't want any – this kind of video that goes viral, they just shut down the Internet. And now they know how to do it, so it's very dangerous because I'm pretty sure that they're going to do it more often. And other countries, repressive countries, are watching this.

A human rights organization that monitors Internet disconnectivity and human rights said that last year there were about, I think, 200 cases of Internet shutdown. And I think this is something that we need to take very, very seriously. Because especially for people who live in these countries, repressive countries, the In—if – unfiltered Internet is like oxygen. And when you take that away from them, they feel they're suffocating. This is what people have been telling us. And I'm sure --

Lyse Doucet: (Crosstalk) it's become a weapon in these – in these protests --

Golnaz Esfandiari: It's a weapon. And – and Russia --

Lyse Doucet: -- (crosstalk) – use it.

Golnaz Esfandiari: -- is now going to use it.

Lyse Doucet: But then there was – there were reports that – I think coming from the United States, which of course welcomed the protest, that there were efforts to try to help people get access to the Internet through – I think they shut down the VPNs as well, so it was being used on the other side as well, wasn't it, the Internet as a tool. How did that work, that some people did – did manage to get material out? Because we did see the photographs and the videos, despite the --

Golnaz Esfandiari: You mean this time?

Lyse Doucet: Yes, this, time, yes.

Golnaz Esfandiari: Yeah, but we got very few. Yes. It appears that some – so there was five percent connectivity, at some point four to seven. So I believe – we don't know exactly. In some border areas we received report that people were using Iraqi sim cards. You know, they would just use it to send information and then tore it out, because it's also traceable. Other parts of the country, we don't know really how people managed to get on line. Some people, there was one journalist who sent a tweet that went viral, and he said that he used 42 anti-filtering tools, proxy, to get on line to write a single tweet. And the tweet was knock, knock, hello, world, do you hear us? Millions of

Iranians are without Internet. He sent the tweet then he got disconnected, and now we just received report that he has been arrested.

But I also believe that, you know, this is a speculation, but it seems to be the case that some people either managed to get through the – the servers who were still on line, or these were people in the government who helped the protesters send some of the videos to the outside world, so that the world sees what's happening in that country.

Lyse Doucet: As you say, this is rather un—this is unprecedented, this – this extensive use of – of a shutdown. We saw in what was called the Arab Spring, I mean, a misnomer now in retrospect, that in Egypt, for example, it was shut down temporarily; that it was used temporarily and then governments at the time said can't have the whole country hostage to using this as a weapon. Iran has used this this time. But it's also known that in the – in this conflict between Iran, the United States, and Israel, that the cyber hacking, cyber tools, have been one of the battlefields that has been used, that we understand is used even now, to have a --

Golnaz Esfandiari: Absolutely.

Lyse Doucet: Yes. To undermine each other.

Golnaz Esfandiari: The US and Israel have reportedly used cyber attacks to slow down the Iranian nuclear program. Iran has launched cyber attacks. Actors within Iran, which we – we believe are close to the government or work for the government, have launched cyber attacks in the US. So this has been ongoing. And they've also – you know, Ira—the Iranian government doesn't like free media in general. They don't like – they – you know, they want everyone to report what they want, so it's heavily censored inside the country. And using this hacking and cyber attacks, they try to censor journalists such as I and my colleagues, who are outside the country. So they try to – to hack into our e-mail accounts. There was one case, a journalist in the BBC, they detained her sister. She was – she's with the BBC Persian. And then they contacted her via Skype, I think, or one of these tools, to interrogate her and to threaten her. So they're very good at using these tools.

And – and what's also interesting, while 80 million people were offline during the past week, Iran's Supreme Leader was tweeting his speech, saying that these protesters are all thugs and they're foreign agents.

Lyse Doucet: OK, but so we've got a sense both of the problems and how to respond to the problems. James, I'm going to turn to you now, and I think because NATO is supposed to be the great alliance that protects all of us, how – and cyber has been on your agenda for some time. Are there any approaches, developments coming from NATO to respond to this – this threat, challenge of our time?

James Appathurai: Definitely. And I would say maybe in two baskets. One is exactly as the Minister said: securing our networks. And second, it's fighting

disinformation. So in terms of strengthening our cyber security, I would point to two main baskets. One is cyber security itself, and that would include, for example, as I think was mentioned earlier, we've now said that Article 5 can apply to a cyber attack. So it can reach a threshold, a level, which triggle Ar—trigger Article 5. Second --

Lyse Doucet: Does it ever come close to that?

James Appathurai: I don't think so, no.

Lyse Doucet: OK.

James Appathurai: Second, now the military considers cyberspace to be, for NATO, a military domain, like air, land, and sea. So it is integrated into the planning of what we do, and the whole military chain takes this very seriously. So that's also new. Third, we've created infrastructure, so now we have a Cyber Defence Operations Centre at SHAPE (ph), at our military headquarters. We have cyber response teams which can go out and support allies. And actually, we just deployed one to one of the allied countries to kind of upgrade their systems. And we can now reach out to nations to use their assets for when we also might need to do more than just strict defence. So that's strengthening NATO's cyber security.

Second, which is also relevant to many of the discussions that we've had here, is steps to strengthen the resilience of nations' infrastructure. So under Article 3 of the NATO Charter, nations are obliged to make sure that their systems are resilient. So our defence ministers just met last month, and they agreed a set of sort of baseline guidelines that countries need to look at when they're looking at their own IT infrastructure. And yes, that does include 5G. And it includes things like you have to use or look at trusted providers and suppliers. So that's an important thing to look at.

Second, you have to develop options to manage disruption. If something gets turned off, you need to be able to figure out how to turn it back on again. Third, governments need priority access to communication systems in a crisis. So we need to be able to use it. And sorry, corporations, we have to be able to use it. Fourth, we need to look at the consequences of foreign ownership or control of strategic assets in this area. So this is a big ask. Many countries are doing it. I'm quite sure Canada is doing it too. So that's the sort of second package: strengthening our resilience against the threats to our systems.

And then the third aspect is – is fighting disinformation. And that's something we have been forced to do. You know, you and I used to work together when I was in the information world, and it was quite clear that this was becoming, when I was NATO spokesman (inaudible) and, you know, we started, but certainly my – my successor has really embraced fighting back. So we have from NATO – and you can go to our website and instant response to disinformation. So that's part one. Second, we work very closely with the European Union as they work on fighting disinformation. So we're really tied together.

Lyse Doucet: Can you give us an example of when – how that happened recently that we can imagine that something came on your radar that was disinformation and you responded immediately?

James Appathurai: Every single day. And if any of you want to look on your phones and just go to the website, every single day there are false narratives. For example, there is a constant stream of false stories, which I have to say I think originated in Russia, about what the Canadian and other troops deployed into the Baltic states are doing: you know, raping little girls, stealing, causing environmental damage. And it's just never true, but we have to respond it, and our – the governments in the Baltic states respond very quickly. And we've seen a sort of evolution, and I think that's positive.

So for example, there was a story propagated by the pro-Russian online media in Germany about – this is a couple of years ago – about a rape of a little girl, which was not true, but there were all kinds of demonstrations, and President – Foreign Minister Lavrov, you know, amplified this story. And then when German troops moved into Lithuania as part of our deployment, the same story was immediately propagated. And it didn't last two hours because the media there knew what was coming, the population had been prepared – coming back to po—prepar—preparing the population – and it just died.

And so that brings me to the – to the next point, which is we have a – what we call a centre of excellence in Riga, which focuses a hundred percent on how to detect disinformation, how to fight back, and how to build resilience. And they do that with all of the NATO allies, but also with partners. So Ukraine also has access to this. And they share best practices about how do you educate your journalists, how do you ca—educate your population, how do you build in resilience to the system.

So in Belgium, my kids, who are I'm sure quite shocked – I mean, when you said they said you're talking about tech, I think the tone of voice was different, like *you're* talking about tech, is much more what it was like, with an OK, Boomer at the end of it. (Laughter). But they get education in school, all the kids do, on how to detect fake news. How do you check it? How do you check the url? How do you confirm it? So these are the kinds of things we all need to – to start doing. And NATO doesn't do the school net—and the education in school, but we do try to make sure that all of our allies and any partner that's interested gets access to this centre of excellence to learn best practices. So secure the system, fight disinformation.

Lyse Doucet: And in this so – oh, I love this, that the places are called centre of excellence because you think that they've reached the – the peaks of --
James Appathurai: Of excellence (crosstalk) --

Lyse Doucet: -- of achievement. But reality inside must be that they are – it's a race. Because --

James Appathurai: It is.

Lyse Doucet: -- in effect, we haven't seen the worst yet. We're now beginning going into deep fakes (ph), and that's certain that it's already coming up in the US presidential election campaign. You've all seen that video of Nancy Pelosi where you distort the video, you put words into people's mouth. This is going to be used more and more. We've got the rise of the robots as well, increasing use of artificial in—intelligence. I mean, James, can you – it – it involves a huge commitment of resources, forward thinking, to imagine the unimaginable, in effect.

James Appathurai: You know, that's absolutely right. And I think it's important not to just fight the symptoms; you have to fight the cause and protect the system. Because if we're always playing Whack-a-Mole, coming back to what you said, you're always going to lose. So we have to build resilience into the system so that it can deal with the unexpected. That does mean of course we have to take account of emerging technologies. So we have just adopted in NATO a policy on dealing with artificial intelligence and machine learning and quantum and all of those things, and will also have to apply to the – obviously to the information space.

But I think also – and this comes back to an earlier discussion – we need to build a stronger relationship between industry and government to protect these systems. So we just had an industry forum last week, and the president of Boeing participated in that with the Secretary General. It was a very useful discussion. They talked about exactly these things. But it's once a year. And I know that there's all sorts of hesitation in places like Google, for example, you know, they – what you read in the newspaper, where they're a little bit leaning back when it comes to governments, and particularly when it comes to security. But I think we need to actually sit down, figure out how we can have an organized, dedicated discussion.

And I'll – I'll just conclude with this little analogy, because I – I talked to someone very high up in a Canadian IT company last year – like, super high up – and I said, you know, we need to set up some sort of.

Lyse Doucet: (Laughs). You mean Shelly? (Laughs).

James Appathurai: Some – no, in a company. In a – in a company, a major IT company. And I said to him, you know, we need to set up a way in which this dialogue can take place because, in the end, government has to regulate and protect and, you know, you guys are – you own the infrastructure. And – and he said OK, James, so let me explain to you how it works. Anyone you hire who is any good, I can hire them for ten times the price, and I'm going to. Second, you have half a day per month to focus on this; I do it all day, every day. And third, I'm going to tell you what I want you to know so that I get the regulations that I like. So good luck to you.

So we have a real challenge working with industry because we don't have the expertise,

we don't have the money, we don't have the time, it is so complicated, it moves so fast, that we really need industry to come to us and kind of share.

Lyse Doucet: Hmm. And I think – well, I think today we have in this – in this nice gathering we have Boeing here, we – I think we have Jigsaw here. And if any of you want to put up your hands at some point and – and help us to answer James' question, his question affects every single person in this room, no matter what you do and where you come from. And so we all have to pull together when it comes to dat—protecting our data. But I'll give you time to think about what you want to say. Minister of Ukraine, you wanted to say something.

Andrii Zagorodniuk: Yeah, just a couple of points to add. So fi—the – the hygiene, and generally the understanding of how technology can be dangerous, including the, you know, something which you use every day, all those things should be taught in schools, and it should be, like, everywhere. Yeah. And this is because you know how long it takes to hack the simple phone? Sixty seconds.

Lyse Doucet: Wow.

Andrii Zagorodniuk: And that happens, like, all the time. And if you think you have a password, your password could be detected while you sitting in café and – and dialling in. Somebody can make a picture. And that happens, like, in our country all the time. So you know, somebody takes a video of you, like, using your password, that's it. It – you no longer have a password. So all these things. And then through the phone, especially if you have a, like, corporation connection to the – to – to corporate network, the people can – and then you keep the phone all the time, use it, and you don't even understand that that's a channel for people to get into your – all – all your information, and it could be go on for years without even noticing.

So these things people should understand that – how to – how to – how technology can be actually dangerous. Because everything is digital right now. And since it – it does, you know, that – that – certain things much simpler. You can install an app which does access to your data, and that app could be actually the – the way – the channel how – how people get – get to you. And for instance, there are apps for various social groups, and they can trace your location, they can trace, like, where you go, who you meet, and – and all these sort of things, turn your camera sometimes.

We just detected apps for ex-military and current military, and then you check, like, who owns these maps – apps – and they're owned by, in our case, Russian companies. So – so it's just every time you have to deal with – with the ways like people – people are very creative, actually.

Lyse Doucet: How many – how many people in this audience feel confident that they're doing everything they can within the existing technology to keep themselves – their data safe? How many here feel really confident that they're doing everything they can?

Andrii Zagorodniuk: Not – not many.

Lyse Doucet: How many of you – (laughter) – how many of you are like me and you go to another country and you're da—you don't want to add roaming charges, so you go into the Starbuck's; or – or you came to the Halifax International Security Forum, there's an open Internet, you don't check that the – oh, there's no password, great, and you log on? How many of you do that without thinking twice?

Andrii Zagorodniuk: Maybe twice.

Lyse Doucet: And who's the expert who can answer? Shelly, what – what do you say to all of us?

Shelly Bruce: Yeah, don't do that. (Laughter). Or investing in a good VPN is – is wise.

Lyse Doucet: Is what?

Shelly Bruce: Is wise, to invest in a virtual private network service that you can use, like to help --

Lyse Doucet: A VPN?

Shelly Bruce: -- secure your – your communications and the connections, for sure.

Lyse Doucet: OK. Let's get some – and as I mentioned, if someone wants to contribute something practically to the scus—discussion to move forward in how we can confront this challenge, and if I could ever—if anyone would like to use the Halifax Security Forum to announce from an industries, a tech giant, they're going to undertake a major initiative to help us, well, you'll make news and make our day. But let's get some questions. Esmeralda's (ph) here. Yeah. Where's the microphones? And then we'll have it in the back. Oh. I see some familiar faces.

Question: Thank you, Lyse. Espen Barth Eide from the Norwegian Parliament. I used to be Defence Minister and established a Norwegian Defence Command – I mean, the cyber defence command – for exactly the same reasons that Canada did. I'm very happy about the thrust of this panel. I wanted to point up a specific concern I have and discussed with some colleagues also. It's that any future war will be a cyber war, and it might also be a kinetic war, but it will most likely start in the cyber domain or in some kind of hyper domain.

Lyse Doucet: Yeah. Yes.

Question: That also means that it will not start in the military domain. It will more likely be in – the first signs that you're in war will happen in the banking

system, electricity system, in the – in – in the water dis—distribution system. And you might actually not know that this is more than the background nouse that – noise that we all have because, as you said, Shelly – and we have and you have and of course Ukraine is in a shooting war – constant attacks. So what's the difference between the background noise of the penetration attempts and a real, massive attack?

So my question is maybe to Shelly and – and James. When do we know that this is something beyond that, it's beginning of something that could lead to an Article 5 situation? I very much agree that it could. But when do we know, and how do we know, and do we have systems that picks up in time that this change is happening and that this sum of events is actually the beginning of a war?

Lyse Doucet: And while you're standing up, since we often see Norway as the gold standard, topping the charts in many other measures of quality of life, how ready is Norway for those challenges?

Question: We are more ready than we used to be, but we're not as ready as we should be because, as our measures increase, the threat increases faster, so the gap continues to grow.

Lyse Doucet: It's exactly – it's is – it is – is a very – very, very good question. And I think from the –

Unidentified Male: (Crosstalk)

Lyse Doucet: -- we have two – we – we have two questions there, then I'll come to the – come to the panel. Yes.

Question: Thank you. Ayman Mhanna from Lebanon. I – I work in the field of human rights and freedom of expression. So my question is related to responsibility to protect individuals and human rights, and what NATO, Canada, and mo—better equipped organizations and countries can do to help others that are not necessarily formally allies. And I'll give you some specific examples. Responsibility to protect: human rights defenders, lawyers, journalists, who are attacked by friendly countries like Saudi Arabia, the Emirates, using software that is theoretically made to protect the entire country that that is in fact targeting individuals that are not necessarily promoting the same ideas. Where is the responsibility to protect people from decisions? They can buy companies, insurance companies, based on biased data that has been collected? What – where is the --

Lyse Doucet: You're (crosstalk) the Pegasus (ph) technology –

Question: For example, absolutely.

Lyse Doucet: -- developed in Israel, sold so Saudi Arabia, the United Arab Emirates –

Question: Exactly.

Lyse Doucet: -- and that is being used (crosstalk).

Question: And one last example is related to my possibility to go and seek retribution, recourse, judiciary recourse in many countries, actually most of the countries, maybe not represented in Halifax, where the judiciary are not prepared, there is nothing in how they are trained in their schools to actually deal with these questions in terms of forensics, in terms of actually knowing who is responsible and what retribution can be in order to bring justice back. What is being done at the level of international cooperation on these levels? Thank you.

Lyse Doucet: Yes. And very much a low – low-intensity kind of war. We had real war here, low-intensity. And we'll take one last question before we bring you to the panel, then I'll come to this side of the room.

Question: Hi. My name's Leah West, and I'm a professor at the Norman Patterson School of International Affairs in Ottawa. And James, you were astoundingly intelligent on tech, but I'm going to ask Ms. Bruce a question instead.

James Appathurai: Oh, yeah.

Question: So CSE, you mentioned the defensive capabilities, also has active capabilities. The definition of what that could entail captures what would typically, if conducted in a physical space, be the domain of the military. Recognizing CSE's close connection with the military, and that the Minister of National Defence and Foreign Affairs would have to sign off on any active measures, will the acal—actual operational exercise of active measures been – be done in collaboration with the military, given the potential collateral effects? And what does that mean in terms of our military allies?

Lyse Doucet: OK. James, do you want to take the first question, which is very much an echo of what we heard earlier, but a very important one, about how it starts and --

James Appathurai: Thanks. So of course we fully share that analysis. Let me make four very, very quick points. One is you're absolutely right that this is the risk. And what's, I think, really important to recognize, that in the European context what we're really talking about is Russia, if we're going to talk about war. And what's important to understand is how Russian strategic culture has changed. I'll try to do it one sentence, two sentences. It used to be very similar to ours: force on force. Now – and anyone can see this publicly, it's not a big secret – it's about ambiguity, pre-emption, strategic surprise, what some people call the Gerasimov doctrine. So it's hybrid. It's all built on ambiguity and thresholds. And Ukraine, like Georgia, have witnessed it, so they do it. And they have a command headquarters built in Moscow to coordinate it, and anyone can go on line and Google it and you'll see it.

Lyse Doucet: Can we just be clear on this? Because Russia's always mentioned, but the technology's changing and more people are getting it. Is Russia really the only state actor that we're – that Europe has to worry about, or the neighbouring --

James Appathurai: In terms of state actors that could conduct war against – certainly against NATO, the only country that's anywhere in that context, in my view, is Russia. China has no in—you know, it's nowhere near us --

Lyse Doucet: OK.

James Appathurai: -- etcetera.

Lyse Doucet: OK.

James Appathurai: So what we're talking about is – is Russia. So I think first of all we have to recognize this. And I think we – in NATO of course we do, and – and of course Ukraine, they do too.

Andrii Zagorodniuk: We do.

James Appathurai: Second point I would make is, for me, what is the most important element is attribution. Because everything that follow is unlocked by attribution. So we need to invest in knowing what's happening. That's the key to everything that follows. And of course it's precisely the strategy to avoid attribution. So I think we need to get over any shyness about that and invest in the capacity to do that.

Third is to put the pieces together, to answer your question, because a cyber attack is one thing, and so's an energy cut-off, but as soon as you see those in combination with troop movements, then you start to think OK, there's more to it than that. Fourth (off microphone) --

Lyse Doucet: I think we lost something.

James Appathurai: Yeah, I have two last ones. One is our – in our experience, the country under attack will know first, and they'll tell you. So outside detection is great, but if you're under attack, you're pretty sure you're under attack. And they know. And we've all become much more sophisticated about knowing what it means.

But then the final point – and this comes back to what our Polish colleague said this morning: all those things below the threshold are one thing, but as soon as there's a military threat crossing our borders, we know how to deal with it. It will not be an ambiguous response.

Lyse Doucet: OK. Shelly, I wonder if you could respond to both these

questions, both as a procedural question about how it would – would work in terms of signing off and how the institutions work together, and then Ayman's point about defending people against technology being used to squash and to harass, intimidate the human rights defenders, lawyers.

Shelly Bruce: OK. So I'll start with the (inaudible) question. It's very important to recognize that, as well, the military has just put out its – its national strategy around being secure and engaged, and in that there are very explicit references to cyber as a domain. So the military is – clearly has a space to occupy here.

In the Cana—in the CSE context, in the CSE Act there are explicit authorities – very – very explicitly registered in terms of the kind of activities that are possible in that space. But there are also some certain prohibition – or some – some conditions. So these have to be activities offshore against foreign infrastructure. There are also prohibitions against causing death or bodily harm. Oh. There are also prohibitions against causing death or bodily harm. And there are also conditions about – prediti—prohibitions against perverting the court of – course of justice or democracy. So – so there's some pretty clear red lines there.

The fact is that the CSE legislation also provides for an authority for CSE to assist the Canadian Armed Forces, and that's new – and the Department of National Defence. So when you combine all of that into one package, it makes us really natural and necessary partners in this space because we cover most of the spectrum of activities. So that's – that's kind of the con—the dialogue that's happening right now to make sure that we can operate together and seamlessly, as – as seamlessly as possible.

Lyse Doucet: And Ayman --

Shelly Bruce: (Crosstalk)

Lyse Doucet: -- is worried about the technology – tech—well (inaudible) we'll actually move on.

Shelly Bruce: (Crosstalk)

Lyse Doucet: Technology's being used by some friendly countries to – to follow, intimidate, enrest (ph) journalists, human rights defenders, lawyers.

Shelly Bruce: So from the CSE context, we really are about detecting and it—and finding, from a foreign intelligence perspective, what is happening out there. If we detected these kinds of activities, we would report them, and that would be the responsibility of a different set of players to take action to either single out and defend or to alert those a—those actors that might be affected by those foreign hostile activities.

Lyse Doucet: Just as we all have – I mean, I think Ayman's point is – is important, that some – it's one thing for the United States, Canada to be responding to

this challenge. There's some very vulnerable people, and I think we should use the Halifax Forum to signal to countries involved here, organizations, that there's some people out there who do need help. Again, this is some – what seem to be friendly countries but are doing very unfriendly things. So I just wanted to signal that, Ayman's – Ayman's point.

Golnaz Esfandiari: I mean, Saudi Arabia chopped up a journalist. Nothing happened. A friendly country. There was a few condemnations and that's all. And according to the CIA, it was ordered by the Saudi crown prince. But they're still our allies.

Lyse Doucet: Hmm. Yes. I think it's always bearing mentioned, especially in the forum of this time, when journalists are being attacked, it means democracy's coming under attack. I'm just going to take a very quick round of questions and we – what do we have? – just about nine minutes left. Peter MacKay, and then one way in the back. Quick questions and quick answers.

Question: Thank you very much, Lyse. I'm a bit shocked to hear James – and I understand the reason why – dismiss China as also being one of the more pernicious threats. China's doing it in the wide open. It's a bit like walking out of Canadian Tire with a canoe on your head and not paying. They're out there saying we want your 5G network so we'll have access not only to all of your critical infrastructure but all of your Five Eyes information. And I guess that's my question. From a strictly defence and security perspective, isn't Canada or Great Britain or other countries who might be entertaining a Huawei 5G network automatically saying we're out, we are no longer going to be recipients or participants in information gathering, because we will be wide open to exploitation by the Chinese?

Lyse Doucet: OK. Thank you. Yes, please.

Question: Rafal Rohozinski, SecDev Group Canada. So I'm one of those Canadian cyber companies of which you spoke earlier. A comment and maybe a question. The comment, I think I'd just really like to agree with what Shelly's saying. Ninety percent of all bad activity that happens on an Internet has one vector. And you know what that is? The individual behind the screen. Awareness is the number one way that we deal with the vast majority of issues that we have on line and that we're simply not doing at the moment at all.

We also have a problem in recognizing the threat, or at least getting perspective on the threat. Unfortunately, because industry does own the majority of cyberspace, whenever we hear threat information, it's a little bit like getting recommendations on pharmaceutical drugs from your crack dealer. You always get the perspective that the vendor wants to tell you, and not necessarily the one that you actually need to be looking at for your own perspective.

But the third is the question. If this is such a crucial component of what we now

understand as national and – and societal security, where is the investment? We may talk about this in august settings like this from a strategic perspective, but talk to any municipality in Canada and ask them what their cyber defence posture is, and you'll have a blank stare. And yet governance hits the population of any country at the municipal level. It's where people live, where they pay taxes, where they get services, where the biggest impact will happen. If I want to take down the Canadian National Defence Department, I'm not going to attack their network; I'm going to attack the city of Ottawa because that's where their employees live.

Lyse Doucet: Very good – very good points. I think what's just – would you – you had – did you have your hand up? Just very, very quickly because we just have four minutes left. It'd better be good because –

Question: (Off microphone) quick one. Richard Spencer, Secretary of the US Navy. So we went through --

Lyse Doucet: (Off microphone)

Question: -- three very meaningful exfiltrations over the last 18 months, and we whistled in a cyber study on ourselves, for those people who've gone through near-death experiences with a cyber exfiltration, both corporate and government. And we've come up the curve quickly, but we have a long way to go. One, it's culture. It's not investment in dollars. You've got the get the culture right inside the organization so people know what cyber hygiene is.

But my question, as we went down the line here, you cannot have good cyber defence without having an offensive edge. Because it's like sharpening the edge on one side. The velocity is so quick you can't focus on defence only. In a free environment, free countries, how do you have the discussion to get the authorities to go offensive?

Lyse Doucet: Very good question. OK, James, you'll take the question about – there's Peter MacKay's question about China, since it was yours.

James Appathurai: Sure. Thanks. I don't know if this is yet working. OK. I – I – maybe I wasn't clear. What I was trying to say was the threat of military attack by China, in the context of the war question, was off the table for NATO anyway. We just don't see that, don't plan for it, don't consider it realistic. But we're absolutely recognizing that, when it comes to China's rise, that represents obviously opportunities but also challenges, and some of those challenges include some of the issues you raised: the canoe basically, including Chinese acquisition of strategic infrastructure, including IT infrastructure, but of course the security of our systems.

So I'm not going to talk about one particular company because NATO doesn't have a po—position on that. But as I mentioned, we have set these baseline standards, one of which is you have to have, or look at having, trusted providers. And so all of our countries are going to look at that, and they have to make their own national

assessment about it.

Lyse Doucet: That's – that's Huawei coming into the mix, which we don't have time to discuss here, but I think --

James Appathurai: Potentially.

Lyse Doucet: Yeah. OK.

James Appathurai: I'd just say one more sentence, coming back to that question. The German government came and briefed us on their cyber security. It is extremely well advanced, the thinking behind it. And one of the things they do is go to the municipal level, to local level. And for people who are making IT acquisitions in a local government, they say this is what you need to watch for. So everybody knows. They're not – you're not there to tell them what to do. They've already been educated.

Lyse Doucet: Shelly, do you go down to – in Canada you got to go to the federal level, the provincial level, municipal level. Is it that – is it going all the way down?

Shelly Bruce: Yeah. The – we have a very concerted outreach program, and we are meeting at all of those tables, as well as sectoral leads. It's very important that we have that conversation and knit that fabric together so that they feel comfortable and know who to reach out to. Some of this is just knowing who to call if they have an issue. So it goes back to the – the Norwegian question earlier too. You have to build that up, and it needs to be robust and – and pretty fluid.

Lyse Doucet: Hmm. Minister, on the offensive, not (crosstalk) --

Andrii Zagorodniuk: On – no, not on the offensive. I just wanted to mention one thing, is that in information campaigns and in information warfare, a critical thing is awareness, as was just mentioned. But the awareness works. Like, it's – it's a complex thing. So one of them is understanding that you can only use credible sources of information. And – because (inaudible) feed, for example, and social media, you know, the information from The Economist and – and some completely unknown place appears pretty much on the same screen, one after another.

And when you – when we started talking about the – understanding that sometimes it's not even a fake news or it's not even the – a complete – a complete fake, which also happen, but also it's just adjusting the – the way the real news are presented and then over and over again being reposted. And then at the end, it – it's given a completely different focus. And people's opinion are created in a – in – they're shaped, you know.

Lyse Doucet: OK.

Andrii Zagorodniuk: So people have to be aware of this and just understand that this is happening, like, all the time right now. Yeah.

Lyse Doucet: Golnaz? Just a – which – do you want to make a last – I know bit bits – be – as a journalist, you don't have governmental or corporate --

Golnaz Esfandiari: No, I – I mean, I – I (crosstalk) --

Lyse Doucet: -- responsibility, but it's something that's part of your daily life.

Golnaz Esfandiari: -- have a question for --

Lyse Doucet: Yes.

Golnaz Esfandiari: -- for a tech company. For --

Lyse Doucet: Yes.

Golnaz Esfandiari: -- for countries such as the US, other countries, what are they planning to do in case of shutdowns in other countries or in Iran? You know, the US keeps saying that we stand with the Iranian people. The US Ambassador to Germany just a few days ago said that the US has the aba—ability to restore the Internet for the Iranian people. And I thought wow, that's great. But then some people who are, like, tech experts said that's not possible, that they need to have some kind of – do it with the – some domestic servers inside the country, which is not going to work with Iran because we don't have any relation. So that's my question. That's my concern.

Lyse Doucet: Hmm. It's interesting because you began by saying that the Iranian government has been preparing for this for ten years. Well, the question that would be has the American government been preparing for that possibility in Iran for – for ten years so that you're at the same place and at the (crosstalk) --

Golnaz Esfandiari: And actually, some tech experts believe that the US sanctions have helped Iranian government bring down the – shut down the Internet. Because, because of the sanctions, all these tech companies have been pushing out Iranian people. So – and – and Iranian servers. So people have been forced to bring the servers and the companies inside the country, so it's been easier for the government to shut down the Internet and rely on its halal Internet or Intranet.

Lyse Doucet: OK. We could – this conversation could go on and one. I'm going to do just quick fire. Discipline's part of democracy. We're all going to go on the offence, one quick word from each of you, giving advice to all of us. If you could do one thing starting today, what would it be? Just bullets.

Shelly Bruce: I would say know exactly what information you care about and make sure you have a plan to protect it. And if something goes wrong, know what you're going to do to be resilient and recover from that.

Lyse Doucet: Golnaz?

Golnaz Esfandiari: But be committed to Internet freedom.

Lyse Doucet: James?

James Appathurai: Design a real government-industry program of cooperation.

Lyse Doucet: Minister?

Andrii Zagorodniuk: Clearly un—identify risks and – and name things as they are. So if somebody's launching the cyber, the whole world—attacks over and over again, the whole world should know about that and do something. So if – a world of freedom has to be kind of united against – against the state-inspired actions. Because it's – it's – it shouldn't be acceptable. And it is right now.

Lyse Doucet: Yes. Ladies and gentlemen, please join me in thanking our great panel, and thank you to – to all of you. (Applause).

-30-