MACDONALD-LAURIER INSTITUTE

OCTOBER 2021

Securing Cyberspace: How we can protect against digital threats to a free and open Indo-Pacific

The COVID-19 pandemic has only heightened geostrategic competition, with a rise in tensions most acute in the Indo-Pacific. Security challenges are dynamic in this new era and not confined to the traditional domains of conflict. Indo-Pacific states are amongst the leaders of this digital age, spurring the growth of technological developments in a range of areas, including 5G and artificial intelligence.

The malign use of cyber capabilities has also been on frequent display. Several key elections, including ones in the United States and Taiwan, have demonstrated how certain actors are looking to disrupt and interfere with democratic processes. Misinformation and information warfare, in addition to other cyber-attacks, present a significant risk to a free and open Indo-Pacific and beyond.

In this context, Canada still lacks a well-considered and clearly articulated framework for addressing immediate security needs and planning for longer-term requirements. A cybersecurity gap insidiously and routinely undermines Canadian safety, security, and prosperity. Canada needs a coherent vision and comprehensive policy for cybersecurity that actively and aggressively deters aggression and defends our interests.

To shed light on these issues, MLI hosted an event with experts from like-minded countries to discuss the cybersecurity challenges facing the Indo-Pacific. Speakers at this event included: Ambassador Kawamura Yashuhisa, Japan's ambassador to Canada; Richard Fadden, former national security advisor to

the prime minister of Canada; Motohiro Tsuchiya, dean and professor of Faculty and Policy Management at Keio University in Japan; Ainikki Riikonen, research assistant at the Center for a New American Security's Technology and National Security Program; Rafal Rohozinski, founder of the SecDev group; and Bart Hogeveen, head of cyber capacity building at Australian Strategic Policy Institute's International Cyber Policy Centre.

We are pleased to release an edited transcript of the presentations and discussion from this event.

J. Berkshire Miller:

Welcome and thank you for joining us. My name is Jonathan Berkshire Miller and I am director and senior fellow of the Indo-Pacific program at the Macdonald Laurier Institute. It is a great pleasure to be your moderator for what I am sure will be another engaging discussion on a crucially important challenge facing the Indo-Pacific region.

As many of you know, the Macdonald-Laurier Institute has been placing a good deal of attention on the importance of the Indo-Pacific and its nexus with Canada's own foreign policy interests.

Over the past year, we have hosted events and given a platform to thought leaders across the region, highlighting the key stakes in the region and outlining the imperative for Canada to bolster its own engagement.

This session will be focusing in particular on cyber security in the Indo-Pacific. We are delighted to have a top cast of experts here from Australia, Japan, the United States, and Canada to shed light on these issues.

Traditional security and the potential for conflict are evolving in marked ways during the cyber age. Security challenges are dynamic in this new area and not defined in the traditional domains of security which have established forms of conflict avoidance and de-escalation, even if they don't always work. The take-away is that while there are some rules of the road and established practices in many spheres of traditional conflict , when it comes to cyber security challenges and threats, the landscape is much muddier, more opaque, and potentially dangerous.

States in the Indo-Pacific are amongst the leaders of this digital age, helping to lead the growth of technological developments in a range of areas including next generation networks like 5G and artificial intelligence.

China, especially, has been spending hundreds of billions of dollars developing its digital infrastructure and aggressively moving to export this technology to foreign countries in its periphery and

globally. But these challenges are not just limited to China. As I believe our speakers will delve into later today, challenges are arising from other state actors such as Russia and North Korea, in addition to the rise of cybercriminals and terrorist groups that are not always state directed.

The malign use of cyber capabilities has been on display increasingly over the past few years. Several key elections including ones in the United States and Taiwan have demonstrated that certain actors are looking to disrupt and interfere with the democratic process. Misinformation and disinformation warfare, in additional to other cyberattacks, present a significant risk to a free and open Indo-Pacific and challenge the rules-based order beyond this region too.

In this context, Canada lacks a well-considered and clearly articulated framework for addressing immediate security needs and planning for longer term requirements. At issue is a cyber security gap that undermines Canadian safety, security, and prosperity. Simply put, Canada needs a coherent vision and a comprehensive policy for cyber security that actively and unapologetically deters aggression and defends our interests. More importantly, this strategic planning needs to be done in concert with key allies. Those allies include our traditional Five Eyes partners (the United States, the United Kingdom, Australia, and New Zealand), but also the "Plus" partners, such as Japan, along with other key countries in Europe such as Germany, France, and the Netherlands.

On that note I would like to proceed to hand the virtual floor over to his Excellency, Ambassador Kawamura Yashuhisa, Japan's ambassador to Canada, who has graciously agreed to provide some opening remarks for this panel discussion. Before coming to Canada, Ambassador Kawamura served as ambassador and deputy representative of Japan to the United Nations between 2017-2019. He has also served in a range of other senior roles in Japan's foreign ministry. He continues to be a good friend and a strong proponent of strengthening Canada/Japan relations, both on the official track, but also through his robust and keen engagement with public policy institutes such as the Macdonald-Laurier Institute.

Japan is clearly one of the most important friends we have in the Indo-Pacific and has been increasingly working collaboratively with like-minded partners to maintain a free and open Indo-Pacific. We are very much looking forward to hearing from the ambassador on some of his perspectives from Japan on this very important topic.

Ambassador, the virtual floor is yours.

Ambassador Kawamura Yashuhisa:

Thank you Mr. Miller. I would like to thank MLI for inviting me to this very important webinar. Webinars like this and working from home are examples of the new normal brought on by COVID-19. The communication system plays a big role today and is anticipated to advance to become part of our social infrastructure. 5G, for example, is now being introduced internationally and is expected to help provide various social services.

While we live in a world where people increasingly depend upon information and the communication technology infrastructure, the news also reports the rapid increase in cybercrimes caused by the misuse of cyberspace information and communication technology. Cyber security needs to be urgently ensured. The Canadian Centre for Cyber Security also points out in its National Cyber Threat Assessment 2020 that the number of cyber threat actors is rising and state-sponsored actors will almost certainly continue to conduct commercial espionage against business, academia, and governments to steal intellectual property and proprietary information.

Japan has made an effort to build confidence by conducting cyber security dialogues with 14 nations.

Webinars like today's, which will be an opportunity to discuss the issue of cyber security with experts from different countries, are therefore crucial, not only for Canada, but for all of us. I am going to talk about the actions Japan has taken to realize a free, fair, and safe cyberspace. There are three pillars.

The first pillar is the promotion of the rule of law. Actions taken in cyberspace are often categorized as anonymous. These spaces need to be underpinned by international cooperation and international order. In 2014, Japan joined a United Nations group of governments or experts and has actively participated in discussions to promote a rules-based cyberspace, for example by promoting discussions about the application of international law to cyberspace and the development of non-binding norms in cyberspace. Japan has also been an active member of the UN open-ended working group on cyber security and participated in the preparation of the consensus report on rules in cyberspace,

which was adopted unanimously in March. In the G7, Japan has been actively involved in discussions to promote rules-based cyberspace. For example, at the Hiroshima Summit in 2016, which was Prime Minister Trudeau's first G7 meeting, the Hiroshima G7 Principle and Actions on Cyber was endorsed. It affirmed that the openness, interoperability, reliability, and security of the Internet would enhance the common values of the G7, such as freedom, democracy, and human rights. From this point of view, a free and open Pacific region would aim to secure peace and prosperity in the region and abroad through the realization of a rules-based order in the region. Japan is also increasing its cooperation on cyber security matters with the US, Australia, India, the UK, and other like-minded partners.

The second pillar is the development of confidence-building measures. To avoid any escalation of tensions in cyberspace caused by miscalculations and misunderstandings, it is important to deepen the understanding of each other's domestic laws, regulations, policies, strategies, and perceptions of governments. Japan has made an effort to build confidence by conducting cyber security dialogues with 14 nations and regions including bilateral dialogues with the US, UK, France, Australia, and India, trilateral dialogues with China, the Republic of Korea, and the United States, and dialogues with ASEAN and the EU.

The third pillar is cooperation and capacity-building in cyberspace. There is always a risk of cyber attacks coming through countries that do not have enough awareness or the capacity to ensure cyber security – a so-called security hole. This security hole can be a risk factor for the entire world. In response, Japan has been building capacity and providing assistance for human resource development in various countries. For example, the ASEAN-Japan cyber security policy meeting has been held annually since 2009. The ASEAN-Japan Cyber Security Capacity Building Center was established in Thailand to provide technical assistance, including cyber exercises, joint awareness, capacity building, and mutual notification for incidents. Cyberspace and information and communication technology are changing daily and in order to build and maintain a free, fair, and safe cyberspace, the international community needs to keep making an effort. I have just talked about Japan's actions to give one example of such an effort.

I am looking forward to listening to the discussion today among experts from various countries on the latest cyber risks to which the world is exposed and how the international community needs to respond to them.

J. Berkshire Miller:

Many thanks, Ambassador. I was very impressed with some of the approaches that you have mentioned about how Japan is working not just multilaterally, but also bilaterally and unilaterally.

I would like to move on and open our panel discussion. We have speakers here from Japan, Canada, Australia, and the United States. To kick off the first discussion, I would like to welcome Richard Fadden, Canada's National Security Advisor to the Prime Minister from 2015-2016. Before that, Mr. Fadden had a range of senior roles in the Canadian Public Service including as Deputy Minister of National Defence, Deputy Minister of Citizenship Immigration Canada, and Director of the Canadian Security Intelligence Service. He currently holds a range of academic and think tank roles and is a Senior Advisor at the Macdonald-Laurier Institute.

Richard Fadden:

It's a real pleasure to be able to participate in this webinar on a topic that is vital today – and I suspect is going to stay that way for a while. Let me start by saying that my remarks are going to be to some degree motivated by my experience both in foreign affairs and in national security and I've tried to weld these together. One of the conclusions that I've come to in the course of my work is that very few issues can be dealt with outside of context. There are some aspects of the cyber problem that can be dealt with by experts of one sort or the other, but if we are going to talk about dealing with cyber threats at large, either across the planet or in the Indo-Pacific, we need to look at the context and look at some basic principles and some basic truths. So I am going to start with some of those and then work my way through to something more relevant.

Some basic thoughts: One, no country has a full grip on cyber security. I would note that this has aspects – concerns – both in the public and the private sectors of those countries and I will come back to that. No country alone can attain full cyber security short of returning to the pre-digital age. That does not mean that nothing has been done, either in Canada or in other countries, but in most cases it's incomplete and it's not comprehensive. Everybody is suffering from a security gap and if we don't admit this from the very beginning I think we are going to have a challenge. Why? Because of the rapid rate of change, aggressive adversaries, the nature of the worldwide web, the Internet, and the challenges of international cooperation. That's where I would like to start now in a little more focused way.

Cyber threats of one sort or another affect national security; they affect the sovereignty of states, and they affect the reputation of states. I think we need to admit that like all other national security challenges, we can't ignore these, but we also can not expect that they will be dealt with like we would, say, tourism. They are sensitive; countries don't generally like to talk about these things. In the absence of a more basic broad relationship, countries are not going to cooperate easily beyond a certain level (I'm generalizing on cyber security), absent a more general relationship that has been built up over the years and that encompasses political, economic, trade, tourism, and whatever kinds of issues that we might want to mention.

One of the things I noted in particular when I dealt with national security issues was that it does take a while, no matter how well intentioned people are, to develop a measure of trust, so that countries can start dealing with each other with some of their secrets – and in the cyber security area there are some secrets. Of course, they are not entirely secret, and I suspect that my Canadian colleague will talk about some of those "secrets" that exist in the private sector.

No country alone can attain full cyber security short of returning to the pre-digital age.

I want to stress again that part of our challenge in this area of cooperating between the nations of the Indo-Pacific is to develop longstanding or more in-depth relationships, which will allow us to talk about a topic that is really quite sensitive for most countries, and we need to do this consciously.

Let me turn to Canada. We are not a country that is inclined to great public policy statements, with marching bands and whatnot. That's not critical in and of itself, if we articulate principles or if we have a framework. But in the case, for example, of national security policy in Canada, our strategy dates from Prime Minister Martin's time, which in cyber years is ancient history. We need a new policy, dealing not only with national security more broadly, but one that deals with cyber in particular. We do have defined cyber objectives. They deal with the federal infrastructure in a number of critical areas. We do collaborate within the Five Eyes,

NATO, and with a variety of other countries, but we have not even been able to take a decision on whether or not we are going to allow Huawei, a Chinese company, from involving itself in the development of our 5G infrastructure. So, while we are doing a whole variety of things, we don't seem to be able to galvanize ourselves as a country to develop a comprehensive approach in dealing with cyber issues.

I think Canada has another challenge in dealing with how we might work together with the countries of the Indo-Pacific – and that is we don't have that many substantive, effective, active, strategic relationships in the area. We, of course, have Australia. In the case of Japan, out of deference to the ambassador who is talking to us, we do have a formal strategic relationship. You know, vice-ministers meet, ministers talk every now and again, and we have short visits, but the relationship is not one that is animated by a week-by-week or day-by-day sense of commitment and collaboration. We need to put some meat on the bones.

In dealing with a topic like cyber, which involves a fair bit of sensitivity, it's relatively easy for people like ourselves to say, well, let's just collaborate – public sector and private sector – but there is a strong ingrained view in most governments that you don't share too many of your own problems or too many of the potential solutions without some measure of a long-term relationship. I think that is something that we need to do much, much more aggressively. Canada has very good diplomatic relations with most of the countries of the Indo-Pacific, but they are traditional in the sense that we sort of chug along on a file-by-file basis. We have periodic ministerial visits, but they are not as intense as they need to be. Canada has the additional problem of balancing out its interests in the Indo-Pacific and Europe, and I think that that is going to be a problem that will be with us for a very long time, but I would argue that we will suffer the consequences if we ignore the Indo-Pacific.

Let me summarize by saying that single countries are not going to deal effectively with the cyber challenge. We need to find a way to collaborate. That collaboration needs to be built on solid relationships, either within government or the private sector, and if we can't get governments to move as quickly as we can, there is no reason why the private sector companies, corporations, think tanks, and universities can't build relationships that might help. So again, context is important in many respects, which doesn't preclude our dealing with sub-elements of the cyber issue, but unless countries find a way of deepening their relationships so that they can deal with sensitive national security issues more ef-

fectively than we sometimes can now, I'm not sure we are going to be able to push forward very effectively in dealing with the challenges of the Indo-Pacific on the cyber front.

J. Berkshire Miller:

There are two very important take-aways from your remarks, Dick. The first is the idea that cyber security gaps and vulnerabilities are not unique to one country. There might be differences between different partners, but essentially all countries have these challenges and need to work together. The second point (and one very important for today's discussion) goes along with some of things I've been saying for a while about us having to have a stronger strategy for the Indo-Pacific and for specific partners in that region in the sense that we shouldn't be looking at the cyber security issue in a fish bowl. The idea shouldn't just be that we need to improve cyber security on an ad hoc basis. Cyber security needs to be a part of a bigger package that is a strategic relationship with some of the key countries in this region; obviously Japan is one of the important ones, but not a relationship exclusively with Japan.

I would like to now move to our second Japanese colleague, Dr. Motohiro Tsuchiya, dean and professor of Faculty and Policy Management at Keio University in Japan. He is interested in the impact of information technologies on international affairs and is focused on cyber security. He is one of Japan's top cyber experts, often advises the government, and is a very frequent guest on these panels.

Motohiro Tsuchiya:

Two-and-a-half years ago, in December 2018, Prime Minister Shinzo Abe's cabinet approved Japan's National Defence Program Guidelines (NDPG). It aimed to set up Japanese defence policy for the next 10 years. I was involved in drafting it. We discussed cross-domain warfare (or multi-domain operations). We are adding new domains to the existing ones: the fourth domain is outer space, and the fifth is cyberspace, and the Japanese government added another one, electromagnetic space. So, with the physical domains of air, land, and sea, we now have six domains in total. Future conflict might break out across these domains, so it might be more difficult to respond to such threats and risks.

Japan was following a defence-only policy in cyberspace, but the NDPG gave us a new idea. So in dealing with an emergency, if somebody were to attack us in cyberspace, we might launch a counter-strike in cyberspace. Contemplating such a response

might be quite natural for Canada and other countries, but Japan was not considering such a policy. We were just sticking to a defence-only policy. But now, after the National Defence Program Guidelines, we can make use of cyberspace. It's quite new for us. The NDPG does not say what kind of measure we can use to protect Japan's cyberspace, but launching a counter-strike is one of them. That is the first step for cyber defence for Japan.

In the same year, 2018, several months before the NDPG, the Japanese government published a cyber security strategy to prepare for Tokyo 2020. It is scheduled to be revised after the Olympic games are over. The National Center of Incident Readiness and Strategy for Cyber Security (NISC), has tentatively proposed the next draft of our cyber security strategy, which is to be finalized later this week. The core idea of the new strategy is cyber security for all. Of course it should be for all except the bad guys! During the pandemic, we in Japan realized that we are lagging behind in terms of digital transformation, or DX.

In dealing with an emergency, if somebody were to attack us in cyberspace, we might launch a counter-strike in cyberspace.

For example, Tokyo's metropolitan government is counting and releasing the number of COVID-19 cases every day, but we now realize that they are collecting data by fax machine from sub-municipalities. The numbers are collected by fax and input by hand. They miscounted many times.

Anyway, we have many, many problems in our IT system. The government has also said that we have to seek DX and cyber security at the same time – DX with cyber security. The next draft of the cyber security strategy says it will heighten the priority of cyber security in diplomacy and national security. We will make an effort, first, to promote the rule of law, as the ambassador says, then second, to raise defence power and situational awareness, and finally to strengthen international cooperation and collaboration.

Inside Japan, the government will establish a new agency for digital issues and digital transformation. I still don't know it's official name in English; today I will simply call it the Digital Agency. It will focus on the issues that will make Japan more digitally friend-

ly. The agency will work with cyber security strategy headquarters, which is in charge of cyber security, and also with the National Security Council. So the Digital Agency and the headquarters will try to make Japan more secure in cyberspace.

In short, Japan is ready to cooperate and collaborate with like-minded countries, including Canada. Some people have suggested that we might be able to join the so-called Five Eyes countries. I'm not stuck on the idea. Now we have the Quad framework that centres around Japan, the US, Australia, and India. I want to strengthen and expand the Quad framework with Canada, the UK, and other partners. So we say, cyber security for all – not only inside Japan, but with the international partners. Cyber security for all, except the bad guys.

J. Berkshire Miller:

Your remarks are really interesting, informative, and provide a warm-up for some of the discussion later on. One interesting point was that from a diplomatic perspective, the upcoming cyber security strategy will have a significant national focus and will be an important part of Japan's diplomacy. Perhaps we can get into this later in the question period, but maybe this can be looked at from the perspective of the US/Japan alliance. I believe that in 2019 the US and Japan said that in certain situations, perhaps a cyber attack could be considered covered under the US/Japan security treaty, which seemed to be a pretty important development.

Our next panelist is Ainikki Riikonen, a research assistant for the Technology and National Security Program at the Center for a New American Security in Washington, DC. Her research focuses on emerging technologies, particularly AI and information systems, and in addition to publishing in an array of prestigious outlets, Ainikki formerly worked in the United States Department of Defence.

Ainikki Riikonen:

Thanks so much to MLI for hosting today. If I could look into the future, I would guess that over time, the United States is going to take a much more expansive perspective on cyber threats – and even what they are. Overall, it is going to become more challenging to look at threats to information security within the narrow frame of what we like to call hacking, and over time countries will need to adapt to the diversification of ways that adversaries can steal information or disrupt network access. There are two trends that I would like to talk about today.

The first one is the observable trend of malicious actors moving upstream and conducting cyber operations through supply chains. What I mean by that is a software supply chain attack that occurs when a threat actor compromises a third party that provides some kind of software services to the target. Prominent examples of this include the Solar Winds hack (attributed to Russia), and the Microsoft Exchange hack at about the same time (attributed to China). A couple of years ago, Operation Cloud Hopper, pretty notorious, was also attributed to China's government. In that case they used cloud service providers as a jumping off point to get to target companies. In these cases, a malicious actor hacked into one technology company and then got access to a great many more possible targets, potentially even thousands more.

On 5G, the Five Eyes have had some debates on the reliability of vendors such as Huawei.

One of the challenges here is that the traditional view of perimeter defence is evolving towards what we call Zero Trust Architecture, as it seems that you can't trust even legitimate sources for software updates as much as you used to. What this also means is that a breach into one network, one company, or one organization, could indicate a breach into another. It highlights the importance of disclosure requirements and information sharing. In the US recently, the Department of Homeland Security issued new reporting requirements for pipeline companies in particular; I think that this is an overall trend we need to watch going forward – that government institutions will require even private entities to share what they know.

The second trend is that there are supply chain risks outside of hacking, and in some cases the adversary is actually becoming the supply chain, whether as a software provider or provider of network services more broadly. Globally there is a demand for digital services, whether in 5G space, online banking, smart cities, or industrial technologies – and yet you have initiatives like the Digital Silk Road and the Belt and Road Space Information Quarter, which may unfortunately increase the reliance of some states on entities that are subject to the influence of China's government. This gets back to the debates we've heard in Washington, DC, about whether they a back door or a front door. In some cases,

those are both vulnerabilities, but there is a diverse set of ways to mitigate them.

There are some interesting opportunities for international cooperation. For instance, on 5G, the Five Eyes have had some debates on the reliability of vendors such as Huawei. These debates impact everyone else as well. There is also some interesting news out of Ethiopia. Ethiopia is assessing 5G vendors at the moment, and they seem interested in a Vodafone-led group that might get funding from the US Development Finance Corporation. While it is not really in the traditional cyber bucket to think about using tools traditionally reserved for development to empower nations to secure their networks, I think it's a really critical area and will be a really interesting avenue for international cooperation.

Overall, information sharing will continue to be important for cooperation, as will adapting to new means of cyber operations, new trends, and likely software supply chain issues. It will become increasingly important to prioritize finding solutions to information security threats that are outside of our traditional conception of hacking. Our adversaries are continuously innovating – and so should we.

J. Berkshire Miller:

Thanks very much Ainikki. One of your interesting points was the importance of information sharing networks and that we should think of the Five Eyes Plus as well. There are different members there and if we enlarge the scope of the Pluses more, we'll have different networks, different diplomatic partners, and different strengths in those relationships that might allow us more access to broaden that network. As you said, a lot of these issues aren't isolated to five or six or 10 or 20 countries; it's a global issue and I think we need to start thinking about it in that way.

Our next panelist is Rafal Rohozinski, who again will be very well known to many people on this topic. He is a prolific writer on these topics. He is the founder of the SecDev group, where he leads its geopolitical digital risk practice. Prior to founding SecDev, he advised the United Nations and other organizations in more than 37 countries and directed the Advanced Network Research Group at the University of Cambridge?

Rafal Rohozinski:

In order not to violently agree with everything that's been said earlier, let me just step back a little bit to grasp why we should be looking at cyber security from a strategic perspective and why it may be that it sort of sits outside the established bounds a bit.

To begin, the Internet is 52 years old. In historical terms, this is just the blink of an eye, and yet in those 52 years we've seen more than two-thirds of the world's population join this infrastructure that now underlies most of the economic, political, and social events and relationships around the planet.

Two-thirds of those who are now presently working and making the Internet into this economic powerhouse driving development worldwide are under the age of 35 and about 50 percent of those are under 25. The vast majority of new users aren't coming from developed economies – they are actually coming from developing economies, or economies that are transitioning, such as those in Asia. This represents huge a democratic bubble of creativity that has largely been using this resource to interact unmediated by the kinds of institutions that have for the most part shaped people's relationships, not just professionally, but around their concept of identity and their relationship to civic duty and other relationships. We've seen the consequences of that in the last two decades with the rise and the power of non-state actors. Transnational terrorist groups have emerged that leverage recruitment from the Internet and that mobilize populations, sometimes towards genocide, such as we saw in Myanmar, propelled by the fact that this medium has made itself so available to everyone.

Transnational terrorist groups have emerged that leverage recruitment from the Internet.

The challenge with cyberspace is that this fundamental reordering of the relationship between institutions and states is something that institutions – at all levels – have been very poor at being able to adapt to. Those are institutions within countries, and international institutions, too. The challenge, of course, is that at the moment the world has been divided into two camps. There are those that feel that the Internet should remain open and largely unfettered by regulation because that is where, for the most part, creativity and economic value will come from. And there are those countries that want a resovereignization of cyberspace. In other words, they want the reimposition of national rules as the way in which we can find the most stability, the most security, as communities and nations around the world.

The absence of being able to find a consensus between the two sides, or at least a workable consensus, has meant the emergence of the dark side of the Internet: actors that are able to exploit jurisdictional hiding. Sometimes the intentional support of nation states or simply our ability to operate across this largely borderless environment in the absence of states being able to leverage institutional-based means to deal with them has led to a global cyber crime and criminality problem that has proven very difficult to deal with.

It's also clear that cyberspace is a major strategic disruptor of the way that we see security framed through a traditional national security lens, including the application of armed force. For those of you have read Elliot Ackerman and Admiral Stravridis' latest book, *2034: A Novel of the Next World War*, the potential impact of cyber as a means of ending the kind of investment that groupings such as NATO have put into industrial war fighting is fairly significant and being taken remarkably seriously.

It is also a dangerous time. As part of an engagement I am involved in, a trilateral 1.5 dialogue between China, Russia, and the US on the military uses of cyberspace, the Russian Federation has made the point that they see the strategic response to threats as being from cyber to nuclear and from nuclear to cyber. This means that they don't necessarily differentiate between the two and see both as being part of the same level of response available to a state in order to deal with what they see as their national issues.

But Asia is important in this calculus. Asia is where the new Internet and the new rules of the Internet will be built. It has more than half – 60 percent – of the world's population and what is predicted to be 40 percent of the smart city market by 2015. The sheer volume of humanity and technology that will require creative solutions using cyber is going to be significant. Invariably it will be within this mass of humanity that the new rules of the game will be written. We've already seen that in part with China's Belt and Road Initiative, the export of smart city technology, smart city surveillance technologies, and the growing rush by China and its partners in terms of setting global norms over the resovereignization of cyberspace. In fact, we can almost say that the great game is on in terms of seeing which competing set of norms and rules will be the one that will happen in the future.

What does this mean for Canada? For Canada there should be a couple of key take-aways. The first is that cyber is not something that can be solved with the sheer force of a single nation state. It's going to require international cooperation. In fact, it's going to require a doubling down on the very kind of globalization that we've

seen as threatening coming from the cyber domain. It means that Canada has to up its game. We need to start thinking like some of the countries that have recognized that interdependence is where true security can be found. We perhaps need to look at setting up institutions that will aggregate across the whole of government with the ability to effectively communicate our interests across the social, political, and economic domains.

Digital Canada is maybe not a concept that we should discard out of hand, as an institution like that could bring together the capabilities that are currently scattered across several government departments. We need to start taking digital diplomacy seriously and appointing digital ambassadors, in the way that Australia and Estonia have. Most of all, we need to start thinking outside of the box in terms of how we can come up with a global system of norms that addresses and bridges the gulf that presently exists between the like-minded and the non-like-minded. As the ambassador has indicted in his talks, the GGE (Group of Governmental Experts) has just concluded its work and the report – the consensual report this time – is to be released in a few weeks. Hopefully that will give us a path towards this more consensual and interdependent future.

J. Berkshire Miller:

I very much enjoyed your comments, especially the idea that we need more whole-of-government cooperation on this and your suggestion on the need for a digital ambassador. Also, I think you made a really important point about resovereignization of the Internet and the digital sphere.

Our next panelist, Bart Hogeveen, is leading cyber capacity building efforts at the Australian Strategic Policies Institute. For the last couple of years he has been working on initiatives to formulate regional frameworks for stability in cyberspace, in particular in areas of confidence-building measures in the endorsement of norms and responsible behaviour with a focus on South East Asia.

Bart Hogeveen:

I was asked to reflect on Australia's perspective on regional cyber security challenges, in particular regarding the Indo-Pacific. Indo-Pacific is the new buzz word today, including in cyber town.

Let me take you first to February 2019. That was when Australia's Prime Minister Scott Morrison announced in a press briefing that Australia's political parties, all three of them, had suffered cyber attacks alongside the computer network of Parliament House, by

what he called a sophisticated state actor. At the same time, he was not able, or not willing to provide many details, nor the name of that suspected state actor. The common opinion was quite undivided. It was surely Chinese state intelligence. The sophisticated attack had used a suite of malware and techniques not yet detectable by malware detection companies. Those skills are only present in a few countries, specifically, Russia, North Korea, UK, Israel, China, and the US. But really, only one state would have the capability and the extensive tract record necessary to conduct such an operation in Australia against an institution of critical national importance. At least that was the dominate argument then, and still is today.

Later in June 2019, a highly professional group again gained access, this time to student and staff data from the Australia National University, one of the country's premier universities where many prime ministers and political leaders studied and a key institution for science and technology research.

Australia has not really experienced major cyber havoc as other countries have.

Finally, in June 2020, the prime minister again warned the nation of what he called an ongoing campaign of cyber attacks targeting all levels of government, essential services, and businesses. Again, no culprit was mentioned, but he cautioned everyone to be alert and to shore up their defences.

Australia is sometimes referred to as the lucky country, although not always for the best of reasons. But really, on the cyber front, I would argue that Australia has been quite lucky indeed. While much more is happening on the continent to businesses, as the previous speaker alluded to, the number of cyber incidents of a national security and state sponsored nature can really be counted on the fingers of one hand. In fact, so far Australia has not really experienced major cyber havoc as other countries have, quite recently in the US, for instance. That is causing some complacency. Generally speaking, we could say that some cyber security practices in government, amongst businesses, and in society, are far from perfect, or even meeting the standards of a mature digital economy. It seems like the lived experience of a real incident seems to be quite critical given that the digital domain is so intan-

gible, in particular for policy-makers and political leaders, but also within intelligence circles.

Moving to strategy and policy, as some of you may have seen, Australia issued a new National Cyber security study last year in August. When I say "national strategy," I should probably say, "an Australian government strategy," or if I want to be really critical, "a strategy by the Department of Home Affairs and Defence." That's really a first point of critique. It's not really a truly national strategy despite best efforts to include industry, and not a third party's views, as per the comment made by Jonathan earlier. In fact, at the moment, Australia's national cyber security goes hand in hand with the defence strategic update that was launched just a month earlier. That strategy explicitly declares Australia's ability and willingness to project military power. It really centres around the ideas of the need to be self-reliant and ready for high intensity operations, as well as different grades of conflict.

The common thread in both strategies is quite clear and it's also the elephant in the room. We are talking about cyber security in the Indo-Pacific that is aimed at protecting Australia from a growing threat from China, any number of threats, or at least a defence against a Chinese Communist Party (CCP) that is increasingly assertive, if not aggressive, in its behaviour towards other countries in the Indo-Pacific and also towards Australia, including in the digital domain and predominantly in the digital domain. Added to that is, of course, the risk of a deepening China-US competition in the technology area or even the risk of technological decoupling.

Australia's answer in all of this has been to shore up our national defence and further improve our defence agency's response capabilities. Cyber security, both the Defence Security Update and the National Cyber Security Strategy, contained commitments for two main investments. One was a A$50 billion investment in cyber information and warfare capabilities spread over 10 years, but still a substantial investment. And A$1.6 billion, again over 10 years, for Australia's Signals Directorate. I think it is difficult for Five Eyes countries that that kind of cyber security role is so closely linked to intelligence and the intelligence role, but this is definitely not the case in many of the countries in our neighbourhood, and definitely not in our immediate neighbourhood when we look at Asia or even the Pacific. The issue about the militarization of cyberspace and the cyber security function is something that has been brought up quite often in conversations with partners, but is usually internally and domestically focused.

On the external affairs side, the tone is markedly different, even from the prime minister. Let me quote him during the Defence

Strategic update. He said, "It's not just China or the United States that will determine whether our region, the Indo-Pacific, stays on path for free and open trade, investment and cooperation that has underpinned stability and prosperity, the people-to-people relationships that bind our region together. Japan, India, the Republic of Korea, the countries of South-East Asia, Indonesia, Malaysia, Singapore, Vietnam and the Pacific all have agency, choices to make, parts to play, and of course so does Australia." Surprisingly, he didn't mention Canada. So the tone of Australia's new international engagement strategy for cyber and critical technology, launched just last month, shows a far more balanced Australia, and an Australia that is moving beyond cyber and increasingly starting to include considerations of the use and adoption of technologies and the state's use of new technologies.

Australia has been quite active in international attribution efforts after a few major incidents.

The international strategy you will read and hear is that there is a recognition that there is a competition between major powers, i.e., the US and China, and the risk of that decoupling. There is also the other angle, which is that technology and cyber-enabled technologies provide increasing economic productivity that allows us to have effective responses to humanitarian crisis. There is also a drive for substantial development. That's particularly relevant in our case for our neighbours in the South Pacific.

Initially, I was going to introduce four domains, but I added a fifth one. One is where we see a deepening and increasing level of operational partnerships – in our case of the Australian Cyber Security Centre, or the Signals Intelligence Service with regional counterparts. There is a partnership with instant response centres in the South Pacific, there is APCERT (Asia-Pacific Computer Emergency Response Team), with a key role also for Japan and increasingly bilateral channels with Indonesia, with Singapore, Malaysia, Vietnam, Thailand, India, etc. So that's really the operational side of cyber security.

On top of that, there is a regional approach. On that, we really have to credit our colleague from Japan for their leadership role in keeping the discussion going on confidence-building mea-

sures. There still might be an issue with looking at cyber security issues through the conventional ways of dealing with regional security issues, but I think we really see that cyber and information and communications technology issues are being brought into the conventional and regular ways of dealing with regional security issues. This is in fact an acceptance and a constructive way to deal with cyber security, but still is a very new topic for many countries in the region.

One further point: Australia has been quite active in international attribution efforts after a few major incidents, in particular ones that have been attributed to the Russian Federation, where an international coalition is built around public attribution. I think we see that more and more, countries tend to build international coalitions when they want to provide a deterrent effect, which they do partly through attribution.

The Quad has already been mentioned; it is an extremely important factor for Australia: the partnership with India, the US, and Japan, as the liberal democracies in the Indo-Pacific.

Finally, I must highlight the work of the GGE. Despite the criticism about a lack of a Canadian strategy, the Canadian delegation has played a key role in the UN open-ended working group that wrapped up earlier this year. Japan also played a massively important role in the conclusion of the other UN cyber group that concluded last week. So all in all, there are different pockets of areas where international cooperation is increasing. Australia, with its partners in the Indo-Pacific, is trying to play an active and constructive role in all of that, and the more conjoined efforts, the better.

J. Berkshire Miller:

Many thanks, Bart. You made a lot of really excellent points and we can learn a lot from the examples of the specific threats that Australia faces. I also enjoyed your discussion on capacity builders. I think that is crucial when we are talking about this region. It's not just what the Five Eyes and the Five Eyes Plus are doing on cyber, but what is happening in the whole region – South Asia and beyond.

I will move now to the moderated discussion. I will try to be brief. I do plan on abusing moderator's position a little to ask a few questions, but I know the audience has been very interested in this discussion and have posted a number of interesting questions. So let me kick off by truncating a couple of questions into one that touches on the threats and the vulnerabilities that states

are facing in the cyber realm. I want you to think about this very quickly. Give me about a 60-90 second answer. I want to hear your thoughts on the top one, two, or three threats in cyber terms right now in this region and what are the main vulnerabilities. Also, from a 10 to 15-year horizon, what do you foresee as the main threats and vulnerabilities that may not be addressed in that period? I'm going to start off with Rafal.

Rafal Rohozinski:

I would summarize this in kind a trite way and it's not unique to the region. The Internet was built for resilience; it was not built for security. Fundamentally, we have built a whole antithesis of dependencies in economic and in social terms, as well as in management of cities, on a technology that cannot be secured. So really, the only way of being able to secure it in the absence of being able to reinvent it technically is to find international consensus. This where the hard part is going to come in. China, Russia – if you like, the non-like-minded – have a particular strong vision on how they see this technology evolving and the kinds of social and political controls that need to be put on it. The like-minded can see this as antithetical to the rule of law and democratic principles that we see imbued in this technology and somehow enhancing it. The reality is we need a break-through moment.

That doesn't mean that we need the Internet to be under a global government or that we need to re-invent the International Telecommunications Union (ITU) to provide that kind of framework, but it does mean we need to start thinking creatively about how we will accommodate this resovereignization of space, so there is a shared interest around protecting it. Maybe a good model might be something like ICAO (International Civil Aviation Organization) which is one of the quieter UN agencies that allows air traffic and other global infrastructure to operate with minimal friction (of course, setting aside Belarus for the moment). But I definitely think the question that we are going to have to find consensus on in the next 10 to 15 years is how we move towards an institutional framework that accommodates resovereignization while at the same time preserving the basic intraoperative ability of the Internet, recognizing its fundamental insecurity and the need for enduring security.

J. Berkshire Miller:

Ainikki, do you have thoughts on this?

Ainikki Riikonen:

I would say supply chain is one area and standards is the other.

Thinking about supply chains, who owns the digital backbone, who is providing your networks, your applications, your services, even things in the app store, that may have their own back doors depending on who is collecting the data? I think it plays into this notion of the grey zone. It's not just hackers out there, hackers versus defenders, but also legitimate organizations in play that have their own interests or are susceptible to certain influences.

The other one is standards. As Rafal mentioned, the Internet is 52 years old or so, but it's not always going to look the way that it does now. Huawei and certain Chinese government entities put forward a proposal for new IP, looking at what new standards might look like, that theoretically might give a little bit more control to governments – for better or worse, probably worse. I think it will take looking at things pretty holistically in the long-term, not in terms of the bugs in our systems, but systemically at what might evolve in the future and how can we get ahead of the curve.

J. Berkshire Miller:

I'm going to segue to Dick now about international cooperation, following a couple of points that Rafal and Ainikki made. Bodies like the G7 and others have so much on their plate, so many different issues that they are tackling. I would agree that this would be a logical space for the G7 to start putting some more attention, but on the international cooperation side, how much traction do you think will be able to move on this?

Richard Fadden:

On threats and vulnerabilities, I think the thing that worries me the most is the possible impact of all these threats on emerging democracies in the Indo-Pacific. Not every country in that area is a settled democracy with a long tradition (some are; some aren't), and the issue of misinformation, malinformation, and playing on democracy is really important.

The other area that one of my co-panelists mentioned that I think that we need to worry about more and more is non-state actors mucking about in this area. The growth of criminal activity is being significantly underplayed today, generally speaking, and it's one area where I do think it's easier to promote international cooperation because in the case of criminal activity, there is usually a criminal statute or procedures and there are police that can deal with it. That's one area where we should build a banner and start making a fuss about it.

Fifteen years from now, I can see going to Rafal's concerns – the world developing into two spheres dealing with the worldwide

web, with the Internet. I really do hope that we can find a way to find a consensus on the rules that will allow the free and open use of the Internet, but I'm not so sure we are going to succeed, at least not in the short-term. I think part of the issue is we may have to deal not only in the area of cyber, but in other areas with spheres, and develop a coalition of the willing outside of existing organizations.

I don't think the G7 is the right forum to deal with this. They have too much on their list right now and I don't think that's the right grouping. The G20 is not really proven to be very effective. I would argue that three or four countries, possibly those represented here, should sit down and come up with a list of 20 countries or so and try and do something in a new coalition of the willing. I don't think, with great respect to Rafal, that a United Nations specialized agency model is going to work here. I wish he was right, but I don't think he is.

J. Berkshire Miller:

Motohiro Tsuchiya, your thoughts.

Motohiro Tsuchiya:

In terms of cyber security, people tend to talk about the software side, but I want to focus on the physical side. Japan is an island country, so we depend on submarine cables, undersea cables. Ninety-nine percent of the international digital traffic goes through submarine cables. If you look at the submarine cable market, there are three big companies: Japan's NEC Corporation, America's SubCom, and Europe's ASN (Alcatel Submarine Networks). These three companies occupy more than 90 percent of Japan's market for undersea cables, but a Chinese company, East Micronesia Cable, is trying to penetrate into the market. The Chinese company bid was 20 percent lower than other three companies. We worry about the Chinese government subsidy to the project. Ainikki talked about supply chain. This submarine cable is another supply chain risk. We have cables and we have some dry components on land, and we need stable computerized machines to connect these cables, and we have to be prepared for future attacks on those cables and those machines connected to the cables. We have to think about it. Australia is also an island country, so Australia is also dependent on undersea cables. We have to think about how we connect. We are now connected to Canada via the Transpacific Cable. We are dependent on those cables, but how can we trust these cable systems? That is the threats I see for the next 10 years.

J. Berkshire Miller:

You've made a very important point on submarine cables, Motohiro Tsuchiya. It is something that is often neglected, but is a very significant issue. Bart the last 60 seconds is yours for this round.

Rahima Mahmut:

We still do not fully understand the nature of the cyber security threats and incidents that we see happening. I think that if we were to do an analysis, we'd find that a lot of focus is on state-based or state-sponsored attacks or incidents or infiltrations, but by far the majority is of a criminal nature. I think we will see more and more attention going into kind of the cyber requirement that will fight the organized crime area, which is still very much our policy angle. I do agree that there are greater chances of international cooperation in that field, rather than in the international peace and security field.

The other thing when talking about international collaboration – there is a bit of irony in all of the initiatives that we talked about, and we are fighting a bit of an uphill battle here. If In reality, we see that even our own countries are moving more into this information space on cyber security issues. The same for the UN group that was just mentioned. The Group of Governmental Experts started off as initiatives begun by the Russians and then a couple of years later are being perceived as American initiatives. We are probably seeing the same tendency with the western countries fighting back against suggestions for a new international legal instrument to deal with cyber security, whereas we see more and more from different sides the call to come up with something that is binding – a binding instrument to guide state affairs.

J. Berkshire Miller:

Thanks very much, Bart. I'm going to move back to Rafal for a quick point.

Rafal Rohozinski:

I wanted to go back to something that Dick said about the emergence of spheres of influence and this is a really important point that we need to consider. Underlying the disruptive aspect of cyberspace is strategic competition, and one of the ways that strategic competition in cyberspace is being played out is through what is known as the vulnerabilities equities process, which basically means that countries stockpile vulnerabilities as part of a hedge that will become useful tools for resolving interstate issues.

The challenge of that, of course, is that having this kind of arms race occurring runs completely opposite to a need to creating predictability among countries, which is really the route basis of cooperation. My point here is not that I advocate for an UN agency to somehow take over the regulation of cyberspace because I think as Dick does, that this is not likely to happen. In the interest of keeping your friends close but your enemies closer, finding some kind of a mechanism through which you can activate discussions and we can find a minimum threshold of security that is acceptable to all that at least takes this hidden process of stockpiling vulnerabilities and makes it more of an overt process that we've had with other arms controls regimens, is probably worthwhile, as opposed to simply not having that process and living with a gross strategic insecurity indefinitely.

J. Berkshire Miller:

I would like to move on now to the audience questions. Getting back to the point of frameworks to deal with some of these challenges going forward, we talked obviously of the large, multilateral scale of the United Nations, but several of you mentioned the Five Eyes. The Quadrilateral Security Dialogue or Quad has also come up. From a Canadian perspective, would these frameworks make sense for us, in addition to working in the multilateral sphere in other forums? Would the Five Eyes construct and potentially the Quad make sense for us? Related to this, one of our audience members has been asking about New Zealand and its future in the Five Eyes, and particularly its relationship with China. Can we dovetail some of these points together and look at whether the Five Eyes is an area that makes sense going forward on this particular issue, and whether the Five Eyes Plus idea holds any merit? I will start with Dick on this because he has had so much experience as a practitioner in this field. Dick, what are your thoughts on the Five Eyes taking a leading role on this, or is it just one small part of the puzzle?

Richard Fadden:

I think it's one small part of the puzzle. We have to remember that the Five Eyes are an intelligence alliance. It has been expanding in other areas to deal with immigration and whatnot, but it is an alliance where there is trust and a longstanding relationship, as I talked about in my initial comments. I think we should continue to work within the Five Eyes.

Having said this, there is a real concern within the Five Eyes. I was on another webinar not too long ago about letting this intelligence alliance become a jack-of-all-trades. My solution is to

take the Five Eyes and add five or six countries, much like the G7 became the G10 and the G20, and build that coalition up. Don't ignore the Five Eyes, but most of what it does is done in secret, and I do agree with others who articulate the view we have to stop being so secretive about a lot of things that we do in this area. I think it would be great if Canada was invited to join the Quad, and if given an invitation, that we accept, because it would mean the allocation of resources and intellectual capacity to be a real partner.

Back to the issue that I was raising earlier, we still have the challenge in Canada of balancing off the Indo-Pacific with Europe and Russia and all the problems there, and fundamentally, to state the obvious, we are still next door to the United Sates. The issue of dealing with North America as an entity is also very important. Having said all of this, I do agree entirely with Rafal, if you can get a dialogue going, if you can build even a partial consensus on any of these issues, go for it.

J. Berkshire Miller:

Excellent! Bart, can I have your thoughts from Australia on the visibility of the Quad being an area to work on this, and also, as Australia is a member of the Five Eyes, what could its potential role be? Do you have any other bright ideas on areas to address this?

Bart Hogeveen:

To the point that was raised about New Zealand, I think the reality of it lies pretty much with what Dick just mentioned, that the position of New Zealand was defined by its intelligence sharing alliance. There is less likeness between the Five Eyes partners than has been reported in some media outlets. That said, I think all of the Five Eyes partners, with New Zealand being one of them and Australia being one of them, are trying to grapple with the changes of the geopolitical reality in the Indo-Pacific. What we see from an Australian perspective is that there are various forums where strategic security issues are being discussed and corporate measures are being initiated and being discussed. The Five Eyes is one such centre in our relations in what I would call the first-class military and cyber nations. But in addition to that, the Quad has become very important in Australia's discourse in the region, but also in Australia's Regional Forum, the recent partnership on artificial intelligence. You see the different networks and regimens of international collaboration being established and expanding, and they will all develop into some kind of overlaying network of networks in terms of international diplomacy and international affairs.

J. Berkshire Miller:

Thanks, Bart. Ainikki?

Ainikki Riikonen:

Firstly, I want to agree with the point that this is an area where we can't be too secretive. Part of this is because the private sector is so involved. I think it's hard to do cyber defence when so much of the information you need and so many of the targets of cyber operations include the private sector. That would be my bid for coming out of the shadows. In terms of particular groupings, I really like the concept of the D10 (Democratic 10) or the Tech 12 or Tech 10, or however many numbers it settles on, because it's not just about intelligence operations, it's also about development tools, looking at how you proliferate standards for assessing risk – whether that's political risk, technical risks, or financial risks. Given the interconnectedness, it doesn't make sense to keep all of these things pooled within a small group of countries because vulnerability is scaled worldwide, so it's better to be more open than not.

J. Berkshire Miller:

That's a really good point that hinges well off the one Dick made earlier on whether the G7 and other organizations are the appropriate bodies for this. We need to get a bit more creative and focus on this particular issue itself rather than relying on pre-existing bodies. Motohiro Tsuchiya, do you have some thoughts on this?

Motohiro Tsuchiya:

After the Second World War, Japan lost most of its intelligence capabilities. Some people say that now we want to join the Five Eyes, but I'm skeptical. People say we need to do so in order to share information, share intelligence with other partners on intelligence activities and undertake information exchange. But if we don't have enough information, enough intelligence to exchange, we will not be able to receive good intelligence from you and other partners. So why we don't have such capabilities? Because Article 21 of the Japanese Constitution says that we have to respect people's secrecy of communications. That's why we don't have powerful intelligence agencies in Japan. We don't have a Japanese version of the US National Security Agency (NSA). So we are dependent on NSA, the US government, under the Japan/US Security Treaty. We have to raise our capabilities in intelligence and cyber security. If we don't, we will not be a good partner when we're in Five Eyes or other intelligence arrangements. We have to raise our capabilities first, then we want to have a better relationship with other partners.

J. Berkshire Miller:

Rafal, you have the last word.

Rafal Rohozinski:

During my opening remarks, I made the point that we need to look at the internet and these technologies as a generic infrastructure and that it's something that really cannot be segmented between one group of countries and another group because ultimately what we are is so much more than what separates us. That creates a bit of a conundrum because this idea of a D10, or clusters of countries that share interests, only works as much as those countries can insulate and defend what values they have from the rest. That's clearly something that has proven impractical, both because of the strategic calculus that I talked about earlier, as well as the grey zone that exists in cyberspace. We have to get used to the fact that cyber in of itself is a little bit like biosecurity. It's a bit of an all-or-nothing game and in that all-or-nothing game, that international consensus, the allusive international consensus, is really critical.

The critique I would make for the like-minded is that for the last 15 years, our position – this is really the position of both the Five Eyes and the G7, the democratic countries, if you like – has been, don't change anything, the Internet has to stay the same. Of course, that has not really rung true for countries that have been caught up in the way that the Internet has changed drastically. Look at places that Myanmar – any country where all of a sudden politics has been up-ended because of a young generation coming online. In all of these countries, rule-setting has become a priority. When automobiles were first introduced onto the roadways of the United Kingdom, in the early part of the last century, guess who was responsible for making the rules? The automobile association, because at that time, it was seen that only drivers would have the means of being able to determine what rules worked best. Well, our concept of governance is kind of stuck in that era and until the like-minded are able to recognize that the rules that will apply to everyone have to be the rules that will be accepted by everyone, and to change our dialogue and change our narrative from defending our past to looking at the future, we run the risk of both spheres in the way that Dick has outlined them, as well as an unhealthy competition and insecurity that will persist.

J. Berkshire Miller:

That's a great ending point. The audience has had a number of really interesting questions here that I haven't been able to ask. We have a good basis here to continue this discussion in a future

webinar. I would like to thank everybody here on the panel for joining in, and of course the audience members for their great questions. One point that I wanted to close on is one that several of you made during the course of this webinar: the importance of not looking at cyber issues in isolation. Dick made this point at the beginning and others made it as well about interconnectedness. From a Canadian perspective, it strikes me that we need to be thinking on a couple wave lengths. Number one: we need to be beefing up our game strategically on cyber security issues. Number two: we need to be doing that same thing when it comes to the Indo-Pacific region. One in isolation will not be sufficient, so we need a clear, robust growing of our partnerships in the Indo-Pacific. That will help some of the direction that we have on cyber security with some of the key partners in this region. It's not going to be sufficient just to draft a cyber security strategy and assume that some of our partners in this region will immediately become our closest partners on this. We have to build those relationships up hand-in-hand.

So again, a very interesting discussion and I thank you all for joining, and of course thank you to the audience.

constructive important forward-thinking excellent insightful high-quality active

Ideas change the world

WHAT PEOPLE ARE SAYING ABOUT **MLI**

The Right Honourable
Paul Martin

I want to congratulate the **Macdonald-Laurier Institute** for 10 years of excellent service to Canada. The Institute's commitment to public policy innovation has put them on the cutting edge of many of the country's most pressing policy debates. The Institute works in a persistent and constructive way to present new and insightful ideas about how to best achieve Canada's potential and to produce a better and more just country. Canada is better for the forward-thinking, research-based perspectives that the **Macdonald-Laurier Institute** brings to our most critical issues.

The Honourable
Jody Wilson-Raybould

The **Macdonald-Laurier Institute** has been active in the field of Indigenous public policy, building a fine tradition of working with Indigenous organizations, promoting Indigenous thinkers and encouraging innovative, Indigenous-led solutions to the challenges of 21st century Canada. I congratulate **MLI** on its 10 productive and constructive years and look forward to continuing to learn more about the Institute's fine work in the field.

The Honourable
Irwin Cotler

May I congratulate **MLI** for a decade of exemplary leadership on national and international issues. Through high-quality research and analysis, **MLI** has made a significant contribution to Canadian public discourse and policy development. With the global resurgence of authoritarianism and illiberal populism, such work is as timely as it is important. I wish you continued success in the years to come.

The Honourable
Pierre Poilievre

The **Macdonald-Laurier Institute** has produced countless works of scholarship that solve today's problems with the wisdom of our political ancestors. If we listen to the **Institute**'s advice, we can fulfill Laurier's dream of a country where freedom is its nationality.

MACDONALD-LAURIER INSTITUTE

TRUE NORTH IN CANADIAN PUBLIC POLICY

323 Chapel Street, Suite 300,
Ottawa, Ontario K1N 7Z2
613-482-8327 • info@macdonaldlaurier.ca

@MLInstitute
facebook.com/MacdonaldLaurierInstitute
youtube.com/MLInstitute
linkedin.com/company/macdonald-laurier-institute