KEN WEINSTEIN: Well, good afternoon. And welcome to the Hudson Institute. Hudson Institute's mission is to promote U.S. international leadership and global engagement for a secure, free and prosperous future. I am Ken Weinstein, president and CEO of Hudson Institute. And I am absolutely delighted to welcome everyone here to the - and those watching online - to the 2019 Abe Fellow's global forum, which focuses today on cybersecurity, the internet, global competition and national security. The Abe Fellowship, which you will hear more about shortly, is named, of course, in memory of Abe-san Shintaro, the legendary Japanese foreign minister who did so much for U.S.-Japan relations. And this fellowship has gathered a highly select group of extraordinary experts for three decades of important policy work between our two countries.

We at Hudson are honored to be able to co-host this event with our good friends at the Center for Global Partnerships at the Japan Foundation and the welcoming executive director Junichi Chano to the podium shortly and also, the Social Science Research Council. I want to thank Ron Kassimir, the vice president for programs, and Linda Grove, who's the consulting director of the Tokyo office of the Council from which you will be hearing shortly. The SSRC and CGP are the joint sponsors of the Abe Fellowship. Now, for us at Hudson Institute, today's event is - combines two major and important themes that have been critical to Hudson throughout our 57-year history - policy work at the intersection of technology, policy and strategy and trying to think through what the future might look like to promote a better future, particularly at a time of rapid technological change, which affects the strategic landscape. And secondly, our deep love for Japan and for the U.S.-Japan relationship. Our founder, Herman Kahn was, of course, the pioneer - the first man to predict that Japan would be the world's second largest economy, which he did in 1962. And Herman, of course, knew Shintaro Abe well. And we at Hudson have had a long relationship with the prime minister, Abe - the prime minister, Abe, the son of Shintaro Abe. And he, in fact, presided over the grand opening of our Washington offices - these very offices in March of 2016. Today, much of our work is in the area of cybersecurity, 5G, AI, quantum machine learning, global supply chain challenges, as well as in the area of great power competition. Pleased to say that some of our work has become signature work that has shaped and informed US policy and also policy in Japan.

Today, we will have major specialists discussing these issues, noting how critically important it is for our two countries to work together as we enter the next phase of the information revolution. I think all of us had hoped that the Internet would lead to free and open societies. But instead, in some ways, as we've seen, as authoritarian regimes have come to understand the need for information dominance among their own peoples and particularly, using this dominance as a means to monitor their own citizens and to protect themselves from their own citizens, it's become all the more important that we examine these issues strategically, both to open up the Internet, which the U.S. government agency for - U.S. Agency for global media government agency, which I - whose board of advisers I chair here in Washington, promoted an open and free internet through various VPNs and other tools. But the challenges go beyond that. Maintaining the qualitative advantage is key as we move to the next phase of the Internet, of mobile telephony, 5G connectivity, as authoritarian regimes seek information advantage gleaned from following not just the movements of people in their own countries, but the movements of our own citizens' financial transactions, hacking into health insurance companies, hacking into presidential personnel systems. There are major opportunities we as people of Japan and people of the United States together need to face together. And looking forward to an interesting conversation. And on that note, let me now have the pleasure of welcoming to the
podium my friend, Junichi Chano, the executive director of the Japan Foundation for Global Partnership. Thank you very much.

(APPLAUSE)

JUNICHI CHANO: Thank you very much, Ken. And good afternoon ladies and gentlemen and all other guests. Thank you very much for coming out this afternoon. My name is Junichi Chano. I am the executive director of the Japan Foundation Center for Global Partnership. Let me start out by thanking others from the institute and its president Ken Weinstein for hosting this incredibly timely event. I would also like to thank our partner in the Abe Fellowship, the Social Science Research Council for intellectual input and coordination for today’s seminar on cybersecurity. We are truly appreciative of this close collaboration to bring such a singularly appropriate issue to fruition at this contentious time. Just to give you a brief introduction about us - the Japan Foundation was established in 1972 with a special legislation to conduct Japan’s cultural exchange with the world. There are currently 25 offices in 24 countries. And the Center for Global Partnership was established within the Japan Foundation in April, 1991, as a dedicated unit to promote U.S.-Japan intellectual as well as grassroots exchanges.

You might recall that the 1980s were a tumultuous time for Japan and the United States. It was during this acrimonious economic interlude the late Japanese foreign minister Shintaro Abe - who is, of course, the father of the current prime minister, Shinzo Abe - strongly conceived the necessity for a mechanism to ensure the two countries continued to forge scholarly (ph), people to people and other forms of dialogue irrespective of the political times. And as a matter of fact, Foreign Minister Shintaro Abe in the past announced this concept back in 1990, when he was in Washington, D.C., to commemorate the 30th anniversary of the 1960 revision of the U.S.-Japan security pact. The leadership of the U.S. government and those who were engaged in the bilateral relations in private and nonprofit sectors at the time were extremely supportive of his idea, which ended up with the establishment of the CGP a year later. So based on this tradition, the CGP remains dedicated to promoting the global U.S.-Japan partnership and nurturing the next generation of public intellectuals and leaders necessary to sustain this particular partnership. So in order to carry out this mission, the CGP supports the Abe Fellowship Program and the policy-oriented research grant and other initiatives.

Three years ago, in 2016, the CGP and the Abe Fellowship celebrated its 25th anniversary. We are much delighted to have supported more than 400 Abe fellows over the past 28 years. This diverse network of policy scholars and the practitioners has been and will continue to be a growing asset for the U.S.-Japan bilateral relations and beyond. So to this end, the Abe global forum is designed to bring Abe fellows' research and expertise on pressing issues of global concern to much broader audiences. We have had events in California, Texas and New York on topics like innovation policy in science and technology and climate change. Now, given its prevalence (ph) in news headlines in recent years, probably, I don't have to remind this audience about the importance and relevance of cybersecurity on both personal and the national spheres. And as technology increasingly becoming part of our everyday lives, cybersecurity has likewise become a vital concern. The issues of a particular concern include both technical and policy-oriented discussions, the enhancement of our resilience of the Internet against the bot nets and other of these threats, the Democratic Defense Against Disinformation, based on the notion of data free flow with trust and the rise of so-called techno-nationalism, to name a few.
So drawing on the research of Abe fellows, this session will examine how these complex issues are being discussed in the United States, Japan and other countries. The Japan-U.S. relationship has evolved to become a vitally important partnership, both regionally and globally. Numerous issues would benefit profoundly from Japan and the U.S. merging our intellectual capabilities and diplomatic efforts together, and such is a very issue we intend to explore here this afternoon - cybersecurity and national security. So it gives me great pleasure to have such a prominent lineup of international scholars from Abe community and Hudson Institute to discuss these issues with us today. So on behalf of the - all the staff of the CGP and SSRC, thank you very much again for coming out today to engage in robust conversation on topics of importance for all of us. So thank you, and please enjoy the afternoon. Thanks.

(APPLAUSE)

THOMAS DUESTERBERG: Good afternoon. I'm Tom Duesterberg. I'm a senior fellow here at Hudson, and I have the pleasure of being the moderator of the discussion today. Just for information purposes, we are going to have presentations of papers that have been written by our four panelists. They're extremely distinguished panelists. It's a heady, timely topic, so I'm not going to waste your time by speaking off the top of my head here. We will have presentations - short presentations by each of our speakers. Then we will go into a discussion amongst ourselves and open it to the audience for questions. Following the end of the program, we invite you all to stay around for a reception just outside of this room.

So we're going to start with Professor Paul Evans. He's been a professor at The University of British Columbia since 1999 teaching Asian and Transpacific affairs. He's the director emeritus of the Institute of Asian Research. Between - Paul's had a distinguished career as an academic and in public affairs. Between 2005 and 2008, he was on leave from British Columbia to serve as the president of the executive committee of the Asia Pacific Foundation of Canada. He's a regional specialist specializing in Asian research. His first book was on the great Harvard pioneer of Chinese history, John King Fairbank. He was also the co-founder of the Council on Security Cooperation in the Asia Pacific and the Canadian Consortium on Human Security and the Canada-Korea Forum. Today, he's going to summarize his paper on techno-nationalism and some of the impacts of the rising tide of techno-nationalism, especially on the supply chains that have developed over the last 40 years between - in the global economy. Professor, thank you.

PAUL EVANS: In business. Is my voice - OK, great. Well, that's - well, let me start with the customary thanks to the Abe Fellowship Program and the SSRC for taking a chance on me 22 years ago. I'd been a prof at University of Toronto, York University, and then was at Harvard. And the Abe Fellowship gave me the opportunity to - as a Canadian American hybrid to spend time continuing my time at Harvard but also to be based in Japan and to spend one week each month during my fellowship in Beijing, where we were able to do some very interesting cooperative work involving Japan, China and the United States and Canada. So thank you for taking a chance on a strange kind of guy who didn't fit the normal definition. And thanks, too, to the Hudson Institute for the president and others helping us pull this together. Sitting as I do mainly in Vancouver, we hear about the Hudson Institute and are impressed by the research that is done here and particularly because of recent activities involving the Hudson Institute and Chinese counterparts. Whether that dialogue is an easy one or a hard one - I'm guessing it's a hard one - but it has been a distinguishing feature of a group that has tried to make connections across differences in a serious way. And for that, big applause and big appreciation. We're not sure if the Hudson Institute is best remembered for the speech by Vice President Pence in
October, which we think is probably a little better known than the dialogue activities with the Chinese. But they're both part of a picture and, again, congratulations and appreciation. I'm embarrassed. I don't have a paper. And for an academic to say that - difficult. I'm in hot water to begin with.

What I have been working on in the last two years, mainly with officials in Ottawa, in Singapore and several other smaller and middle-power countries about this era of what I think many of us are now calling the era of techno-nationalism. That - we're going to be talking about risks in cybersecurity, many of the challenges that are out there that need responses by individual countries, by individual groups and collectively. But if it would be all right for me to use my 10 or so minutes to talk about techno-nationalism as it's playing out now. And I want to define it in a very specific way because we've been in a situation in international relations where governments for a very long time have been concerned about protections of their societies, of their governments from technologies from abroad. But it strikes me we're in a very different moment than five years ago or 10 years ago or through a longer time. And we're in a different moment because on the edge of the fourth industrial revolution, as technologies are not just they're about communications but, in fact, about defining the way societies and economies are going to be migrating in future and are racing each other to get to that future, suddenly, techno-nationalism means something a little bit different. And what I have in mind in that is that difference.

Techno-nationalism is about areas of an economy or a society that are securitized. And by that, what I mean is that areas that used to be defined as principally of commercial or technical interest - science, broad movement - are increasingly securitized as they become seen as matters of national power, and that not just in defense against things that were challenges to domestic security, not just things that were challenges to defense, dual-use activities, techno-nationalism is about the definition of sectors that are going to be important to the future world economy. And that they are matters of national power and will be securitized, not just in defense but also in the suppression or restriction of those technologies in other locations. And I think it's that era of techno-nationalism that - this era of techno-nationalism is a little bit different than anything we've seen before. And as I've read some of the work from the Hudson Institute, Council on Foreign Relations, a variety of other places in the United States, plus what's going on inside government, I think everyone in this room agrees we're into a very special era on these matters that is compounded by the fact of growing U.S.-China - whether it's called strategic competition or strategic rivalry.

So that combination of techno-nationalism, China and the United States is a subject that's not just on a lot of Canadian minds - and obviously, Chinese and American - but Japanese and others around the world. It is not difficult to go anywhere in Southeast Asia, Northeast Asia or North America and simply use the phrase techno-nationalism to - and U.S.-China relations to begin something that's really at the heart of contemporary policy debates. I'm not, today, going to dwell on what techno-nationalism with Chinese characteristics looks like. I imagine everyone in the room is familiar with made in China 2025, the techniques and the priority areas, several of them - 11, 12, 13, depending on how you count them - where the Chinese state has said that our leadership role in these areas is a national priority. It's a matter of national power and national survival and getting ahead in an international division of labor. This is a strategic objective. And the games that are played, the techniques that are used by China - negative, positive - are an important subject that we need to look at in detail.
But I'd say that what has changed with techno-nationalism in China in the last decade and particularly the five - last five years, is that five years ago, when I would speak with Americans or Canadians or Japanese, say, what do you think of the rise of China? Well, people had a lot of - some saw it positive but on unbalanced. We also saw a lot of concerns. But there was a feeling that China could not innovate in the areas on the cutting edge of technologies in a variety of sectors. Viewed now a few years later, it's a view that it is a China that can innovate, not just imitate, not just steal, but in a variety of areas is moving into the forefront of where technologies are going in a wide range of these new, let me loosely call them, fourth industrial revolution sectors - and that they are able to innovate precisely because of what we thought were their limitations in past. And that has to do with the Chinese Communist Party, authoritarianism and an educational system that, again, was seen to imitate but not innovate. I think the atmosphere now is very different and that it has caused deep concerns in this country and many other countries about how we appreciate that.

What I did want to do, though, was speak a little bit further with an American audience on the matter of techno-nationalism with American characteristics and why some of us in multiple countries are both curious, concerned and sometimes worried about where the United States is moving in its techno-nationalism, which is not just about the development of new technologies in the United States and with friends and in an international space but the limitations and restrictions on Chinese development in those areas, both in this country and internationally. I'd like to give just a quick case study to open the discussion on the subject of Huawei and 5G technologies; a subject that is deeply debated inside Canada and in this country, of course, but also in Japan and others. And from - if I can use an American basketball metaphor, even though the world champions are from Toronto...

(EVANS) It would be that, vis-a-vis, Huawei, as an example of a particular kind of Chinese company that is on the cutting edge of a set of technologies that are related to 5G but could go well beyond, that there is a full court press against Huawei, not only in this country - it's on the entity list, the restrictions on it - but also a pressures by your government for other countries to join the limitation ban on Huawei 5G activities. And in Canada, there's no country more so than Canada that is caught right in the crosshairs of this through the arrest of the Huawei CFO, Madame Meng Wanzhou, in Vancouver on an extradition request from the United States. As your government has gone after a Huawei employee rather than the company itself, we're caught up in the midst of a major diplomatic rift with China because of that extradition or house arrest in Vancouver but also in the retaliation by China on the arrest of two Canadians - two Michaels - and some other economic kind of sanctions.

So right now, we're right in the midst of major - my aunts, my uncles, my cousins all have heard the name Huawei for the first time. They have heard this name Madame Meng, but they don't know much about. But it is top of mind, a country we're fighting with - we're in a deep diplomatic conflict with at this moment, the deepest since we had diplomatic relations established in 1970. But this - the issue that's beneath the surface, though - beyond extradition treaty with the United States and how it might need to be adjusted - is the issue of the 5G decision and where Canada is going to go with that decision. Let me just say that it is being buffeted by three forces. One of those forces is the technical and security issues involved in working with Huawei. They are very complicated. And the mitigation techniques, the risk assessments, what could be done to
mitigate them if we move ahead - big technical debates - no clear understanding but a smart discussion.

But our smart discussion is overshadowed by two other factors. One of those is the public opinion on both China and on Huawei - that is stone cold. A country that had been pretty deeply committed to engagement with China is now maybe engagement but not engagement as it has been in past. And public attitudes are extremely negative. So that's part of the picture for any politician that has to make the decision. I'd like to say to an American audience that there is a third force. And that's the force of the U.S. government in encouragement, in browbeating, in threats in working with Canadians if we don't go along with a Huawei ban. And this is something that is happening in a variety of countries. Whether it's the right way for your state craft to have developed on this - hard for me to say. But there is a feeling that to go against the United States in a Huawei ban - we can debate what ban means. But to go against the United States may - whatever it may be in Canadian national interest, our overriding interest is the maintenance of security arrangements with the United States. That's not to say that the - the point is, it's not based on the logic of the proposition itself of working with Huawei but the reality of great power of geopolitics and the intensity and the credibility of American pressure. Where that decision's going to come out - invite me back in November after our election on October 21, and I can tell you.

Well, let me finish, if I could, by saying that in this caught in between United States and China in technology nationalism, that there - it has an impact on governments, where we're going. Nobody wants to get caught in the middle of this. We don't want to get caught in the middle of something that is either decoupling at one end or a simple openness to what China is doing. Where is the middle? And one group - and I will finish with this - that is caught smack in the middle of this is our universities. And the universities - this is not only about student recruitment from China, not only about fields where we're trying to recalibrate our diplomatic - I'm sorry - our academic exchanges; it's principally in the areas of the sciences. And this is the area where it is very unclear to our researchers whether they can do work on Huawei - Huawei funds research in Canada; in fact, a lot of it - how far we can accept it. And I want to - there's a big debate about this internally.

But one of the factors that I want to emphasize to our American friends is that there are extraterritorial implications to how you are moving on research and other limitations that spill over for us. And a very practical example is that in our collaborations with scholars at University of California, Berkeley, they are unwilling to work with Canadian institutions and are unable to work with Canadian institutions that take funding from Huawei. So if you - (laughter) you start looking at the implications of what decoupling and restrictions might look like, our universities - the tension between those who see open science as the objective and others who are dealing with real national security issues, how we connect those is really a hot topic in our world.

And I might end on just one hopeful note that in this pretty gloomy conflict that is emerging, this competition that is emerging - how to compete with China rather than against China. And I think that at least some of us hope there are ways where, I think in the American parlance in science and technology, we need to define small gardens and put very high walls around them in areas that we will not cooperate with China. And in other words, to keep the door open, you close some windows. That, I think we all agree to, we have to do. But the issue is, where are those gardens? How big are those grounds - gardens? Excuse me. And we do see forces in the United States that see this as much bigger than a Huawei or a 5G issue. But the whole issue of
China's involvement and that of other countries in these new technologies of the fourth industrial revolution that we're looking very carefully to see where you're going and how far we can cooperate in that and how far we have to go an independent path. On behalf of Canada - I wish I could say on Japan - thanks so much for the opportunity to be here today.

: (APPLAUSE)

DUESTERBERG: OK. Thank you, Paul. And our next speaker is from Japan. Motohiro Tsuchiya is professor of the Graduate School of Media and Governance at Keio University and deputy director of the Keio University Global Research Institute. Tsuchiya has had a long career at Keio, having been educated there up through the Ph.D. level. He's the - an expert in national security and cybersecurity. He is the co-author of more than 20 books, including "Cybersecurity: Public Sector Threats and Responses" He's interested in the impact of the information revolution on international relations, regulations regarding telecommunications and the Internet, and global governments and information technologies, as well as cybersecurity. Please welcome professor Tsuchiya.

: (APPLAUSE)

MOTOHIRO TSUCHIYA: Thank you very much. I'm very glad to be back to Washington, D.C. So I was actually a Abe Fellow 18 years ago. I spent one year in Washington, D.C. So Thomas (unintelligible) - he is also Abe Fellow - he helped me to find an apartment in (unintelligible) Virginia. So I had a very good memory in Washington, D.C. But 18 years ago, it was the time of 9/11, so I was very shocked. On that day, I was in San Francisco for a conference, so I couldn't go back to Washington for a week. And I was watching TV, and I was reading newspaper. And so I realized that bad guys are using the Internet. So that's a big change for me. So I was just looking at the brighter side of the Internet at that time - until that time. But I changed my topics. I started looking at the darker side. That's why I'm doing cybersecurity these days. So I want to talk about what Japan is doing on cybersecurity these days. So I'm not - I learned - using English more than 35 years, but I'm still not confident in my English, so I want to use the slide actually.

So I am a guest editorialist at Nihon Keizai Shinbun - Nikkei - in Japan, so I searched articles on Nikkei. So this is a number of articles on cyberattacks on Nikkei. So the first big change was Mitsubishi Heavy Industries in 2011. So they were compromised by possibly China, and 83 servers - computers were hacked, and we lost some technology information. So MHI says it is not critical information at all, but we were very much surprised. So MHI is the biggest military contractor in Japan. The next one is Huawei. So Huawei is a big issue now, but several years ago, it was also a big issue between China and the United States. And so Edward Snowden came up in 2013. So these kinds of reports were bigger in Japan, too. After that, Sony Pictures was hacked in November 2014. So Sony Pictures Entertainment is a American company, so Sony brands goes back to Japan. So Japanese people were very upset with this cyberattack. And next one - the biggest one was Japan Pension Service, actually. So more than 1.25 million pension records were lost from the agency. So Japan is an aging society these days, so a lot of older people are very angry. So - where's my money? Where's my pension records? It was kind of a political scandal.

After that - so U.S. election was also widely covered in Japan, too - and WannaCry incident happened 2017. So these kinds of reports are affecting our perspective on cybersecurity in Japan. And whom do we care? So here are articles covering China, DPRK - North Korea - and
Russia. At first, China was our possible enemy, so a lot of articles are covering cyberattack on China. But after that so Japan Pension Service - after the Japan Pension Service incident, U.S. election was becoming a national issue. So Russia is intervened - interfered on U.S. election. But Russia has not interfered Japanese elections so far. But we are expecting a national referendum to change the constitution, so we are worrying about it. So what's a topic we are worrying about? At first, we were talking about Tokyo Olympic Games next year. So I started looking at the darker side. That's why I'm doing cybersecurity these days. So I want to talk about what Japan is doing on cybersecurity these days. So I'm not - I learned using English more than 35 years, but I'm still not confident in my English, so I want to use the slide, actually. So I am a guest editorialist at the Nihon Keizai Shinbun - Nikkei - in Japan.

So I searched articles on Nikkei. So this is a number of articles on cyberattacks on Nikkei. So first, a big change was Mitsubishi Heavy Industries in 2011. So they were compromised by possibly China, and 83 servers, computers, were hacked, and we lost some technology information. So MHI says it is not critical information at all, but we were very much surprised. So MHI is the biggest military contractor in Japan. So the next one is Huawei. So Huawei is a bigger issue now, but so several years ago, it was also a big issue between China and the United States. And so Edward Snowden came up in 2013. So these kinds of reports were bigger in Japan, too. After that, Sony Pictures was hacked in November, 2014. So Sony Pictures Entertainment is a American company, but Sony brands goes back to Japan, so Japanese people were very upset with this cyberattack. And next one - the biggest one was Japan Pension Service, actually. So more than 1.25 million pension records were lost from the agency. So Japan is an aging society these days, so a lot of older people are very angry. So where's my money? Where's my pension records? Well, it was kind of a political scandal. After that - so U.S. election was also widely covered in Japan, too, and WannaCry incident happened in 2017. So these kinds of reports are affecting our perspective on cybersecurity in Japan. And whom do we care? So here are articles covering China, DPRK - North Korea - and Russia.

At first, China was our possible enemy, so a lot of articles covering cyberattack on China. But after that - so Japan Pension Service - after the Japan Pension Service incident, so U.S. election was becoming a national issue. So Russia is - intervened, interfered U.S. election. But Russia has not interfered Japanese elections so far. But we are expecting a national referendum to change the constitution, so we are worrying about it. So what's a topic we are worrying about? At first, we were talking about Tokyo Olympic Games next year. So it might be hacked. It might be disrupted by cyberattacks. But recently, we are focusing on election national referendum intervention might happen in the future. And so we are closely watching at - Taiwan presidential election expected next January. So it might be a big issue for us. But I went to Taiwan twice this year, and they were talking about possible intervention from China these days - and not only in cyberspace but in the physical space, too. So United States and Japan are sharing concerns. So after Tokyo Olympic Games - the summer games will be in Paris, but in 2028 - so United States, Los Angeles will host Olympic Games. So we are sharing concerns. And so you will have a U.S. presidential election next year. And after that, we might have a national referendum for the changing of the constitution. So we are sharing concerns these days.

And what might happen during the Olympic Games? A lot of things are of concern. So first one is fake ticket. So a lot of people try to get tickets. Well, we might have fewer audience in the stadium because of the cyberattacks, cyber operations, and maybe overbooking or small
booking of hotels on the other accommodation in Tokyo area. Or we might have a blackout in Tokyo area. It's really, really hot, so you'll be stuck in a very crowded train. It's a nightmare. So you don't want it. So - but we are worrying about these kind of things. And so in the final phase, we might lose the police, self-defense force or government functions in Japan, in Tokyo and in other parts of the - in other parts of Japan. So these things must be cared in the government preparedness for Olympic Games. So the Japanese government is preparing a lot of money for security of Tokyo Olympic Games and the Paralympic Games. We successfully finished G-20 summit in Japan earlier this year. But we are facing - the Rugby World Cup is coming later this month. And after that, we will have Olympic Games. So we have many, many exercises these days. But we cannot guarantee 100% security, so we have to prepare for something might happen. So what we are doing - so last year, 2018, the Japanese government organized a council for National Defense Program Guidelines. So this is a first meeting of the council. I hope you recognize my face. But just in case, I will zoom so you will see my face.

(LAUGHTER)

TSUCHIYA: Actually - so I was not picked up because I'm a good expert of cybersecurity. The reason is that our older generation don't understand cybersecurity in Japan. Because I was here 18 years ago; I started researching on cybersecurity 18 years ago; it's a good advantage for me. So after coming back to Tokyo, so everybody said, oh, it's not good topic. Why? So - bad guys are using the Internet. I said, really? Bad guys are using the Internet. But people didn't believe me. So one big figure to international relations - he said so to me in a reception, oh, that's a bad topic. Why? So - bad guys are using the Internet. I said, really? Bad guys are using the Internet. But people didn't believe me. So one big figure to international relations - he said so to me in a reception, oh, that's a bad topic. You should not do it. But after that, I said, oh, I will definitely do it. So now I have an advantage. So that's why I was picked up in the council. Well, this last December, we concluded that National Defense Program Guidelines. So we have to strengthen our security in cyberspace and outer space, too. So we called it multi-domain defense force. So we have self-defense forces in Navy, ground force and the air force. And we are trying to have a new force for outer space, new - I'm sorry, not force - unit for outer space. And we have already a cyber defense unit under the self-defense forces.

We have to strengthen these kind of units and forces. In the National Defense Program Guidelines, we set a fundamentally strengthened cyber defense capability, including capability to disrupt ongoing attack against Japan or pronounced use of cyberspace for the attack. This is not fancy for the U.S. people, American people, but it's a big step for us. Before this Defense Program Guidelines, we couldn't launch a cyberattack in any case. We were just focusing on defense - defense only. But it says we can do a counterstrike. It's a big step for us. But in that case, we have to do attribution very well. So we might think that cyberattacks came from China, but real attack might be North Korean people inside China. So if we do a counterstrike against China, what would happen? So it's a big nightmare for us, so we have to have strengthened our cyber intelligence capabilities. In the later part of the guidelines, it says self-defense force will liberate this capability in all domains, including cyber. We have all domains' ISO capabilities. We have to strengthen our capabilities, but we have a problem. It's another constitutional problem.

So Article 9 of the Japanese constitution prohibits using force for offensive purposes, but Article 21 says we have to respect people's communications privacy, so that's why we don't have an NSA, National Security type agency in Japan. We have national - we have Ministry of Defense Unit focusing on wireless communications. We can tap wireless communication from North Korea, China, Russia, but we cannot tap wired communication inside Japan. So we have to be
careful to monitor people’s communication, but we have to have some kind of limited capabilities to monitor our communications to stop cyber operations, cyberattacks, but we are not allowed to do so. That’s a big problem these days. So I want to quote James Clapper’s words. At the Pentagon, I had often heard the military truism that every nation is preparing to really fight its last war. When was Japan’s last war? It was World War II. There was no cyber operations, cyberattacks. We have to think the future, so we have to prepare for the future. It’s quite a difficult task for us.

So in conclusion, Japan and the United States are sharing our cyber concerns. We have - I hope we can work together. And second - so Japan sets up a multi-domain defense force. We are trying to strengthen our forces in every domain. And finally, Japan strengthened cyber capabilities, including ISO, and we have to do it very quick. So defense program guidelines is planned for 10 years, but 10 years too long. So Olympic Games come next year, so we have to be very quick. We have to work together with the United States. I want to stop here. Thank you very much.

(APPLAUSE)

WEINSTEIN: So we’re honored to have, as our next speaker from an American perspective, Dorothea LaChon Abraham. Excuse me. She is an associate professor of information systems and operations information systems department of William and Mary’s Raymond Mason School of Business in beautiful Williamsburg, Va. She’s a graduate of West Point and went on to get a PhD in management information systems from the University of Georgia. After her service in the military, she worked as a systems analyst for American Management Systems in Norfolk, Va. Her research interests include wireless, ubiquitous computing, organizational decision-making for information systems and technology and health care informatics - all incredibly important applications of information technology.

She was the recipient of a Fulbright Research Award to Japan in 2008 and 2009, which must have been an interesting time to be in Japan. She studied health care information technology and served as a visiting assistant professor at Keio University, which is another theme of our program today. She’s also been recognized as a teacher as the David and Carolyn Wakefield Distinguished Associate Professor of Business from 2013 to 2016. Her current research is partly focused on cyber security strategies in Japan, the U.K. and the United States and comparisons between those. So, LaChon, nice to have you.

(APPLAUSE)

DOROTHEA LACHON ABRAHAM: Good afternoon. I’m more of a recent Abe fellow, and I’d like to thank the Abe Global Fellow program as well as Hudson Institute for allowing me to share some of the insights that I’ve garnered thus far as well as Tsuchiya-sensei for his guidance in this particular area. Let’s see here. Thank you. OK. I’ll try to get through a number of these topics today as I go through. There have been some that have covered, so I’ll skip through a few of those, but I think they’re incredibly important topics to cover when we’re talking about cyber capabilities. But I’d like to start out with discussing kind of - what are the common adversaries? And building off of what Tsuchiya-sensei has provided, Japan, U.S. and U.K. are - share common adversaries in cyberspace that work to weaken our national defense, illegally acquire our IP - intellectual property - destabilize our global alliances and disrupt supply chains. Since 2017, as was discussed, international malware by nation-state actors have amassed
almost 1% of the global GDP in losses, and these losses due to cyberattacks have been increasing in Japan, the U.S. - Japan, U.K. and U.S. respectively since that time.

More attacks are being realized now in critical infrastructure, particularly public government, telecom health, academic, manufacturing, power utility, transportation are the primary sectors that we're concerned about, especially with the Tokyo Olympics right around the corner in Japan. But these are also critical sectors that have been impacted in both the U.S. and U.K. The Mirai botnet attacks targeting Internet of Things devices, many of which have been rushed to market without cybersecurity engineering baked into their designs, are now a particular concern for Japan with the expected flood of these devices during the Tokyo Olympics. China and Russia lead in offensive attacks against all three countries. And as you can see over there, Japan is limited again by some of its pacifist constitutional issues that have restricted its ability to do counterattacks.

But Japan is critical as an ally in the information supply chain and defense capabilities in the Asia-Pacific region. Japanese companies also are prime vendors in the U.K.'s defense information infrastructure. A recent cyberattack by Russia on a U.S. defense contractor operating in Japan demonstrates that, while Japan was not directly the target, Japan's networks were attacked in an attempt to gain access to U.S. trade secrets and possible network disruption. This scenario could be replicated easily in which domestic networks in any of the three countries that are allied and do operations extensively in the Asia-Pacific area together or over networks are used to engage with a vendor supplying any one of the other nations. Thus, all countries have a responsibility to become more accountable allies in building their cyber capacity.

So what are these capabilities that we're talking about? Cyberspace accountability for nations can include developing comparable security and resiliency and attribution. These capabilities are critical for national security. While cybersecurity is foundational to protect assets and information from being attacked in the first place, cyber resiliency, which is a theme across all the strategies, concerns the assurances that a nation will be able to protect its critical infrastructures to remain effective through an attack. So it's about enduring the inevitable attack. Attribution of responsible attackers is a capability enabled by threat intelligence analysis, a multiple-source information to learn tactics, techniques and procedures used by attackers. The information enhances the security and resiliency and overall the national security. Transparency of these aforementioned capabilities, propensity for risk by each nation and the cultures are actually challenges to national cyber strategies, being comparable to protect our tightly woven digital economies.

But luckily, when we look at the national cybersecurity strategies across Japan, U.S. and U.K., they're pretty similar in terms of what the intent is. And organizing around a risk management approach in particular for securing critical infrastructure seems to be the theme. The U.S. and U.K. articulate deterrents while continuing innovations in offensive capabilities. But this requires attribution capability. Japan now only - has openly espoused deterrents as a strategic goal, even in light of its pacifist constitution in response to these increased attacks that we've been talking about and potential attacks on other critical infrastructure such as telecom, power and utility, medical and transportation, which are vital to the operations of Tokyo 2020 Olympics. And so indeed, the Olympics is a driving force of Japan's strategy - or was - in securing and making services in these sectors particularly resilient. All strategies note the need to strengthen engagement with the business ecosystem since the critical infrastructure's owned and operated
by a private sector in each country. The cyber authorities interviewed thus far across U.K. and U.S. note sufficient federal cyber budgets. But some in the GOJ personnel within the ministries themselves suggest that Japan needs to substantially increase in scale, especially to meet its goals for the Tokyo Olympics in terms of its budget, which is about a tenth of the U.S. budget for cyber. Each nation's cybersecurity authorities seek to operationalize the strategies and collaborate with each other but do indicate that there are differences in some key areas, like threat intelligence analysis. There are constraints with the legal frameworks and some fragmentation actually across the cyber authorities that complicate issues with collaboration.

Here are schematics, which is a little difficult to read there, on the U.S. and U.K. authorities. As we know, they share identification of coordinating authorities, which DHS serves in the U.S. and the National Cyber Center serves for the U.K. The U.S. and U.K. have distinct responsibilities. But there is a bit more overlap between the authorities in the U.K. for defensive operations. Direct communication platforms exist. And this is key between the U.S. and U.K. for sharing information between the authorities domestically and between the two countries. Much of the lessons learned from the terrorist attacks of 9/11 about what should be done more effectively in counterterrorism information sharing has been applied in the context of cybersecurity across the two nations. While some cybersecurity fragmentation does exist in the U.S. and U.K., these issues are readily being worked out. For example, in the U.S., the NSA's new cybersecurity directorate will unify NSA's foreign intelligence and cyber defense missions to reduce risk to national security systems and the defense industrial base, in particular. And that was just a recent occurrence.

A challenge for all cyber authorities in each country is that the defense industrial base is compromised - comprised of many private-sector suppliers who transmit across computer networks of managed services or managed service providers, MSPs. But these are not owned by government, and there's a desire for more regulation to ensure cybersecurity. So these cyber authorities that I've been speaking with sometimes have noted challenges by lack of legal authority to conduct as thorough analysis as needed domestically and with each other when laws do not enforce private-sector cooperation. Looking at Japan's cyber authority, the cyber responsibilities are coordinated by the National center of Incident readiness and Strategy for Cybersecurity, NISC. It was established in 2005, but it's actually not a ministry-level entity as of yet. NISC does have direct consult with the prime minister on all cyber-related matters.

However, Kenzo Fujisue, who's a member of the council - House of Councillors that I've been engaging with, is strongly advocating a need to boost NISC's authority, by first establishing in law for its undisputed authority for coordinating policy on cybersecurity and resiliency in critical infrastructure sectors to plan for preventing outages on critical systems. He suggests renaming National Cyber Command - or renaming it as the National Cyber Command. And its responsibilities would then become kind of a mix of what DHS, USCYBERCOM and the NCSC in the U.K. has as roles. The second thing he's noted about NISC, or he's proposing, is making part of its staff permanent, particularly the senior leaders. And that's because it's a needed necessity for continuity on cyber issues. It needs to increase the number of staff overall that it has. And it only currently has 150 personnel. And the staff are nomadic. So in that, I mean they're tasked to NISC, which is the primary coordinating authority on cyber, for about only two years. And they come from posts in other ministries - the NPA, National Police Agency, and private sector. But it is very apparent that many of these personnel do not have extensive cyber experience.
Thus, it's imperative to build the cyber acumen for the NISC workforce. Increasing its budget also is an imperative because it is gravely below that of the U.S. and U.K. in terms of what it has to do in order to protect and build guidance and governance for national interests. These factors would increase NISC's ability to conduct governance. But it takes lawful changes. When we talk about legal frameworks, Japan is unique among the three countries in having a cybersecurity law. Japan's Article IX does not prevent Japan, as we discussed before, from conducting attribution analysis on known attacks, levying sanctions or other diplomatic methods. But naming and shaming as we do in the U.S. and U.K. is not part of the culture. Some political officials have advocated for elevating cyberattacks on critical infrastructure within Japanese laws and approving a defense trade act to strengthen Japan's cyber defenses. As far as laws applying to the public sector, Japan currently does not have an equivalent of what we have here in the U.S. - The Foreign Investment Risk Review Modernization Act - that can be leveraged to make activities transparent of private-sector entities with foreign companies or academic institutions, particularly for safeguarding shared networks against attacks.

The U.S. and U.K. typically apply current laws on counter-terrorism and dual-use technologies, which enable attribution activities that lead to indictments and prosecutions for cybercrimes of individuals that may or may not be hacked by nation states. The EU's General Data Protection Regulation, which is actually absorbed into the U.K.'s data protection laws, can be used in posed fines for data breaches of customer-related data that impacts companies in all countries. Also, regulated sectors like health care or finance can impose fines or retribution, but it's not uniform across all sectors in the three countries, and the regulations don't apply to intellectual property theft or network disruptions for critical national functions. All countries pursue some form of diplomatic actions against bad actors, but it's not always been uniform until the unilateral banning of Huawei. Also in the countries, there isn't law encouragement - basically law or encouragement by the cyber authorities to share blacklisted company information received from the U.S. and U.K. with Japanese businesses for fear of economic retribution on Japanese companies.

So they actually are able to receive blacklisted information like the OFAC list from the U.S. in those that are established in the U.K. But it's not being shared with businesses in Japan. Also, investigative authorities interviewed in the U.S. note that a challenge is that there aren't laws exacting punitive damages to companies or government entities for not complying with investigative authorities regarding cyberattacks. And government and private sector agencies don't always have the same view of threats posed by nation-states cyberhacking equally, which impacts reporting to investigative authorities and willingness to cooperate to build threat intelligence. And this is something that was shared sentiment across the NPA, FBI and investigative authorities in the U.K. So in talking about threat intelligence and how it relates to attribution, the U.S. and the U.K. robustly share threat intelligence information as part of the Five Eyes, including Australia, Canada and New Zealand. As of December 2018, Japan has committed to engage more effectively with the Five Eyes and increase capabilities to assess multisource threat intelligence, which up until now has not been a particular capability of Japan. However, the U.S. and U.K. have a more direct capability to share classified information compared to Japan. Interviews reveal that Japan's platform sharing currently does not allow direct exchange for classified information with allies. They, in fact, connect through proxies, which is impacting, potentially, Japan being able to get timely information to critical forensic data when it's needed for exchanges. There are also issues in comparable data classification schemes.
So these are issues that are being explored currently by the appropriate authorities, but it is - it does produce a time delay between the countries in being able to share the true forensic data that Japan needs in order to do attribution. However, the Information Sharing and Analysis Centers are robustly sharing unclassified industry threat and mitigation information in critical infrastructure sectors in all three countries, and it's become kind of the de facto information sharing platform for the domestic entities for cyber authorities in Japan. But there should be some wrangling of the cyber assets used in each country in how they are validated or the information used for threat assessments for each country to ensure their methods are normalized. This will aid in normalizing cyber capabilities, at least at the national level, across governments to improve threat assessment and capabilities for attribution internationally.

There's another particular point that is made in all the strategies and that's improving cybersecurity in the private sector. It's a key tenant in each country's strategy. However, as you can see, some of these figures - and I know it's a packed slide - they note a disparity in cyber leadership between the Japanese, U.S. and U.K. companies, which does impact how the private sector can be used as or incorporated in collaboration to protect against cyberattacks.

The U.S. and U.K.'s chief information security officers may be more prevalent within companies, but they still have many reservations about their organization's propensity for cybersecurity and resiliency. The chart notes a lack of concern for suppliers' cybersecurity in particular in Japan compared to the U.S. and U.K. companies. The Japanese cybersecurity guidance for business leadership is a new attempt to boost the focus on suppliers, particularly for the defense industrial base, with guidance on the use of NSS (ph) risk management framework as a baseline. And this is urging the Japanese business leaders to prioritize assets for protection and resiliency. Kenzo Fujisue, who is also, I noted, in the House of Councillors, is pushing for legislation requiring Japanese companies to disclose their cybersecurity postures on their financial statements. This is something that we should also consider in the U.S. and the U.K.

The GOJ will reduce companies' corporate taxes in organizations if they can prove that their IT investments include cybersecurity measures. Again, these are - this is something that maybe the U.S. and U.K. can also do, and especially for academic institutions doing defense-related work as well as anyone in the DBI - or the defense industrial base.

Also, there is a push to have companies submit to audits for certified auditors - or by certified auditors instead of what's currently happening in the U.S. and U.K. as far as reported - self-reported cyber assessments. The development of a cybersecurity and resiliency and maturity model is needed to gauge posture levels as a basis to award any of the incentives, which is something we don't currently have in any of the countries. As you can see, even on this short list and what has been discussed so far, there is a lot of collaboration that's happening internationally, and the dialogue continues. The topics range from legal frameworks to technical oversight to encouraging the business ecosystems that span military and civilian engagements, as well as workforce developments to meet the grave global shortage of demand - skills for cyber. So the question is, can existing collaboration frameworks lay a foundation for stronger shared accountability and resilience in cyberspace between the countries? And in conclusion, I think they can, but they may be more effective to do so in a new trilateral cooperative agreement, something shorter than a - less extensive than its treaty (ph), but that formalizes the combined intent of those prior international collaborations and addresses some of the gaps.

So what are some of the gaps? Transparency and more accountability in policy mandating supplier risk management. There should be methods for supplier assessment and certifications
of vendor networks to create a trusted provider pool for primary, secondary and tertiary bidders that would benefit all countries. And this is particularly so for the critical infrastructure and the defense industrial base vendors. There are also some policy and legislation that the U.S. is currently pursuing for risk management that can be used as a base. Second, our technology device and service providers need to bake in security standards from the outset and governments mandate legislation for this. Third - creation of some global cybersecurity resiliency model as a metric for governance to gauge postures, aid organizations to know what to implement to improve postures to reduce risk. We don't have something that would allow us to currently do that, and it's - again, particularly for the defense industrial base. So this model could be used as a basis for metrics for implementing the incentives, developing laws around network and communication transparency that ease efforts in countries collaborating for attribution purposes.

And it might be something as simple as mandating protections of web logs for forensic data. Increasing threat intelligence capacity with near point-to-point information exchange of classified information is a must and using a common lexicon that all three countries can share, as well as creating normalized cyber assets is also something that could be part of this trilateral cooperative. Finally, focusing on workforce development in areas where the three countries have low to medium expertise and high future demand. These are areas like secure cloud computing, AI machine learning, technology product, security engineering design, cybersecurity risk quantification and - that are amongst some of the other skills. So in this manner, I believe a trilateral collaborative agreement between Japan, U.S. and U.K. can support collective accountability in cyberspace. Thank you for your attention.

(APPLAUSE)

DUESTERBERG: So to continue the sports metaphor which we started out with, our cleanup hitter today is Dr. Patrick Cronin from the Hudson Institute. Patrick hulls the institute’s chair in Asia Pacific security. He’s had a long and distinguished career since completing his education at the great University of Florida and St. Antony’s College at Oxford. Patrick’s had positions in government and academia, private institutions. Among these are the U.S. Institute of Peace, the CSIS, National Defense University - where he was senior director for the Institute for National Strategic Studies. Patrick, his approach - he's an expert on China and East Asia in general - Japan. His approach, I would characterize, is that of something like grand strategy. And today he's going to be our cleanup hitter and talk about global competition for information security.

(APPLAUSE)

PATRICK CRONIN: Tom, thank you very much. And what an honor to be added to this distinguished panel and this distinguished event. When I was offered an invitation to speak on cyber challenges, the Internet and global competition and national security, I wanted to say something original and something that related to my ongoing research, which is looking largely at China’s political warfare campaign, for lack of a better phrase, in maritime Asia. And this led me to the thesis of the global competition for information superiority. So bear with me for another 10 minutes, and then we have Q&A to follow. So this is the first time I've actually read my own remarks that I wrote yesterday, so let me read my remarks, and I apologize for that. If resurgent major power rivalry can be reduced to a single phenomenon, surely it is the quest for information superiority. Because our livelihoods, the way we interact with others and our national security are increasingly and inextricably linked to information, our desire for
information security inevitably drives a competition for information superiority. It is not sufficient to think about the Internet and cyber challenges. We must enlarge our minds and be attentive to the wider global competition for information superiority.

So let me expand on this argument by making four interrelated points regarding the history of information, the value of big data, the defense implications of information and the looming threat to the public square. In the time period we have, I'm just giving you illustrations. First, let me add to the historical context to cybersecurity. Tsuchiya was right to say that Japan last war - they didn't have cybersecurity. But, really, information security is not new. Even just thinking about the British experience before the last war and in between the wars - it's very instructive, I would argue. Because this is the history of signals intelligence, SIGINT. After World War I, the British established a global peacetime code-breaking organization - probably with Commonwealth help there, Paul - designed to intercept and decode diplomatic cryptosystems. This interwar SIGINT agency, the Government Code and Cipher School, better known as CG&CS, was the precursor to the post-World War II GCHQ. So from wiretapping stations in Hong Kong and Shanghai, the British GC&CS intercepted communications detailing secret Soviet-backed organizations in China.

In the 1920s, the intercepts enabled Chiang Kai-shek to deliver an early blow to the communist insurgency in China, as well as humiliating Moscow. After raiding the Soviet Embassy in Beijing, Chiang's intelligence chief, Dai Li, published a book of extracts from the communications of Soviet spies. So predating Snowden and WikiLeaks by 80 years, Dai Li went on to evolve the clandestine investigations section into the innocuous-sounding Investigations and Statistics Bureau. So my point is that accumulating dossiers and statistics is another way of amassing big data, and so I turn to my second point regarding the value of big data. Big data and information power may well determine which country controls the commanding heights of the 21st-century global economy. We have embarked, as Paul noted earlier, on the fourth Industrial Revolution. The digital revolution is permeating all aspects of our lives and international relations.

If the first Industrial Revolution used water and steam power to mechanize production, and the second used electric power to create mass production, and the third used electronics and information technology to automate production, the fourth is characterized by a fusion of technologies that is blurring the lines between the physical, digital and biological spheres. With so much at stake, major powers do not want to be left behind in the race for information-centric technologies such as artificial intelligence, the Internet of Things, 3D printing, quantum computing, et cetera. Information-centric technologies are vital to economic clout and preeminence. That is why, 2015, China issued the 10-year state industrial strategy, Made in China 2025, earlier referenced, as a roadmap for ensuring Beijing would be the world beater in next-generation information technology and telecommunication, AI, and other high-tech industries. The tussle over 5G telecommunications encapsulates the struggle for economic preeminence embedded in information technologies. Huawei is on its way to achieving dominance in various countries and regions, including most recently in Russian and Eurasian 5G. In the Indo-Pacific, 5G projects planned for Cambodia, Singapore and South Korea will expand Huawei's access to their critical infrastructure and potentially the data that passes through it. Huawei relies on products, pricing and various state inducements from the Belt and Road Initiative to, in the case of Russia, playing to Russian pride. Huawei has come a long way. Ren Zhengfei founded the company 32 ago, four years after leaving the People's Liberation Army, setting up shop in Shenzhen's Special Economic Zone adjacent to Hong Kong.
Huawei epitomizes Beijing's approach to profiting from and buying the rest of the world. China is accumulating through all means the biggest collection of data and using that to advance its state-designed quest for economic dominance. That is why Japan has more at risk in the Olympics than just cybersecurity narrowly defined. Bringing in China's technologies and allowing it to vacuum up personal data is just one more way to accumulate big data for profit and power tomorrow. This leads me to my third point, namely that AI helps to underscore why digital technologies are vital dual-use investments, driving not just economic growth but also today's and tomorrow's military systems. Three - information power could determine which country enjoys military primacy. China's desire to rule the world and AI by 2030 is both a bold ambition and a threat that cannot be ignored by businesses or governments. As one Chinese writer wrote a couple of years ago, if successful, Beijing's moonshot initiative has the potential to be a game changer, not just for Chinese society but for global geopolitics, as well. And, he added, while so much of the world today lacks clear direction, China has an edge in its ability to combine strong, top-down government directive with - direction with vibrant, grassroots-level innovation. Or as Eric Schmidt, then-chairman of Google's parent company, Alphabet, told an audience of Americans a couple years ago, the future will belong to countries that can surf the technological tide wave - tidal wave of artificial intelligence, and while China's efforts appear up to the challenge, the United States is swimming in the wrong direction.

China technology specialist Elsa Kania has captured as well as anyone Xi Jinping's gambit for becoming world-class military power by leveraging all of these technologies. As she wrote recently, the PLA aspires not only to equal but also to surpass the U.S. military by seizing the initiative in the course of the ongoing revolution in military affairs being catalyzed by today's advances in emerging technologies. Chinese military strategists anticipate a transformation in the form and character of conflict, which is seen as evolving from today's informatized warfare to future intelligentized warfare. And I've seen this specifically in the Spratly Islands in the South China Sea. We could talk about that in Q&A, if you wish. PLA may have offset U.S. military power if successful in advancing innovation and leapfrogging ahead in the course of this transformation. The advent of AI on the future battlefield might disrupt the balance of power in ways that risk jeopardizing strategic stability and undermining deterrence in U.S.-China relationship. Information-driven economic development is dual-use and is simultaneously aimed at achieving defense primacy in the Indo-Pacific, if not beyond, and it is fed off of information collection, which brings me to my fourth and final point - that security in the public square in the digital age is a wicked problem for democracies - Canada, Japan, the United States, for starters.

In the 2018 book "The Square And The Tower: Networks And Power From The Freemasons To Facebook," Niall Ferguson writes, China's leaders seem much more adept at webcraft than American counterparts. This is seen in myriad ways as the Chinese Communist Party is able to exploit our networked age. The Great Firewall of China, surveillance state facial recognition and social credit ratings give the upper hand to centralized power in Beijing. The Belt and Road Initiative is proving a better brand than FOIP, the Free and Open Indo-Pacific, and the CCP's propaganda machinery is unrelenting at crafting its narrative, with some of the latest themes being that America is breaking down the rules-based system and is the major source of global instability. They are turning the American reaction to China's exploitation of rules in the digital age on its head and against us. Interference in democracy in our networked age is a growing problem. Our public square is open and our people free, and China and others are exploiting that. New Zealander Anne-Marie Brady, Australian Clive Hamilton and others have written
extensively about this concerning and even alarming multifaceted campaign led by organizations such as the United Front Work Department.

I already mentioned by association the Taiwan election in January is certain to be buffeted with interference, and our own election next year could well be targeted. And because we care about privacy and freedom and autocratic states are primarily focused on the survival of an authoritarian system of governance, it is difficult to protect freedom and privacy while combating unwanted external influence. China's authoritarian governance and system of so-called state capitalism employ information to reinforce a set of values antithetical to the post-war liberal international order championed by the United States, Japan and Canada, I would add. As one Japanese commentator wrote recently about China's export of everything from its social credit scoring system to surveillance state technology, quote, "China's Orwellian vision of the future has huge implications for how its battle with the U.S. for global hegemony will play out. If many Asian nations opt for authoritarianism, the foundations of the U.S. liberal order will gradually erode." So to sum up my argument, the Internet, global competition and national security are intertwined in the 21st century. Not only must countries like the United States, Japan and Canada play a leading role in combating this threat, they must also help fashion responses that balance security with democratic freedoms. Achieving this balance in the midst of a surging global competition for information power and information superiority should be among our highest priorities. Thank you.

(APLAUSE)

WEINSTEIN: Good. OK, we're going to move into a question and answer period here. I'm going to start off with a very general sort of question. Then I'm going to turn over to the audience, so please get your questions ready. But one of the themes that has come up here in almost each of the presentations was the need for international cooperation in setting the rules for this new world that we're - of information security that we're living in. One specific question is - and many of you have touched on it - who's going to set those rules? If we were the Europeans, we would say this ought to be done using the - what they call the liberal international order represented by, for instance, the World Trade Organization. If you ask Bob Lighthizer, the trade representative of the United States, he would say there is no international organization that is going to tell the United States what its national - basic national security interests are. So I would ask each of the members of the panel to comment on who should be making the rules that can overlap national security, economic security and cybersecurity. Who would like to start this? Is it the WTO? Is it a trilateral group? Is it Western, like-minded nations?

TSUCHIYA: So I'm running - I'm trying to organize a CJK track two dialogue - CJK; China, Japan and South Korea. So we will have the first round this year, and so we are trying to have a track two dialogue, but it's quite difficult. So we are trying to - I'm trying to persuade so we have to have this kind of agreement in the final stages of the dialogue, but we cannot agree. It's a track two in just three countries. It's quite difficult. And so you are familiar with the U.N. GGE framework, a group of governmental experts. So I think 20, 25 countries are arguing how to organize a global governance of cyberspace. It's quite difficult, so we are divided. And so China and Russia are trying to divide the Internet itself. So they are warning about the U.S. intervention into their systems. So they are trying to say set up Chinese Internet or Russian Internet. So we are in the face of, say, divided Internet in the future.
Well, one thing positive is that cyberspace is organized by geeks. It's a kind of republic of geeks. So they are talking each other. They are trying to maintain the real, physical space of the Internet. So for example, my - one of my students is working for JPCERT. CERT is a computer emergency response team. So they are easy to talk to the counterparts all over the world - CNCERT or KLCERT (ph). So if we find something wrong in the server in Japan, it's getting DDoS attacks. And so command and control site might be in China. And so we make - so JPCERT go out and make a phone call to CNCERT. Hey, we are getting DDoS attacks from China. Could you stop that site? So it works. So geeks can talk each very easily. But political leaders - very difficult, even academics.

DUESTERBERG: OK, would anybody else like to dive in on that? Paul? I'm sorry.

ABRAHAM: I just want to say, to focus on all of those areas, I don't think anything's going to get accomplished any time soon. And we need speed to scale, to deal with these attacks. Why not start with the technical oversight first, with the standards organizations like ISO or the ones that have been established that are developing standards to - for cyber asset creation and for mitigation techniques like - that are risk management oriented? So I think saying that we're going to accomplish all of those different areas at the same time is unrealistic. And what we need is - definitely get that community of geeks online, as well as with our international standards organizations, to come up with cataloguing, what our cyber assets? What are the critical functions that each country needs to secure, and how can we develop cyber assets to particularly support endurance and resiliency and security for those?

DUESTERBERG: Thank you. Dr. Evans?

EVANS: No, we - before coming here, we were in Palo Alto for a meeting organized by the EastWest Institute. And your question, Tom, was exactly what they've had a multiyear project - and that's what can be done. As I think Chon has said, it is in pieces rather than one grand move. And the issues that were being tackled there related to attribution issues and norm building for what's right and what's wrong, recognizing it's extremely difficult to build consensus or even a clear statement of what the problem - these are wicked problems, in terms of their technological complexity but also the politics. But I would say, Tom, your - I think one of the issues, when we discuss with our American friends on this matter, is we are going to need different kinds of venues for this discussion. Sometimes it's among the like-minded, the friendly states, Five Eyes groups. Sometimes it's going to be among those who are not the like-minded. And bringing the non-like-minded in is becoming increasingly complicated.

That's partly the China story, if I can be direct. But it's also a U.S. story as well and how far the United States would like to work towards collaborative solutions on these problems that run across the like-minded and the non-like-minded, as you said and as some of my Chinese friends implicitly will argue, look - we're not going to do anything that is going to undercut our capability to be, if not the leader, a leader in these fields going forward. Some things we can restrict. But how far we can expect American leadership in using multilateral processes, trying to insert themselves in and making some concessions around superiority - I think that's one of the hardest questions. Pat and I, for years, have argued about a country being the leader or a leader. My sense is China wants to be a leader; the United States still feels it's essential to be the leader. And therein lies a big issue in this country.

CRONIN: Let me respond to that because, I mean, the way I read what the Chinese are saying is they want to be the leader. That's the stated goal of the CCP. The United States, on the other
hand, in the National Security Strategy that was issued, the defense strategy, early last year by
the administration actually recognized that the United States no longer enjoys primacy. And so
while some would argue that we still want primacy, and there's a debate that's ongoing that Paul
knows well and will continue to go well after this panel, we have diminished power. We
recognize that. And so, clearly, there are going to be compromise. This is a bounded
competition with China. And this is a huge area of governance, a gap that we have. So the
same reason I argue that information is so key to the 21st century, the governance challenge is
huge. It's going to take a long time. It will take multiple different attempts. Accountability,
transparency are going to be very important to this like-minded group trying to hold up a high
standard for where we want to go with this.

EVANS: Can I ask one more thing? I'm sorry to - Cronin and I have debated these things for 20
years, and he's one of the most intelligent and thoughtful people who I love to disagree with. It's
always a pleasure, and I learned something. But I wanted - you used the phrase moonshot in
your...

CRONIN: I was quoting. That was quoting the Chinese...

EVANS: Yeah, yeah, yeah, yeah.

CRONIN: ...Edward...

EVANS: The meeting we just attended with the East Asia Institute was also about a moonshot,
but an American-led moonshot. And the argument is that in the fourth industrial revolution, you
have to have government leadership in setting a strategic framework to accomplish goals. Now
China knows how to do that in a particular way. It might not be perfect, but they have a system.
The moonshot that was being advocated by - and I was delighted that it was across partisan
group, both Republican and Democrat, involving some people in your administration now on
how the United States can play a special role in organizing private sector actors and
incentivizing them to tackle some of the problems. Moonshot means sending things to the
moon, the big picture. And in - the United States is a country that has not been averse to
government leadership in key areas - Manhattan Project, space projects. It's not the way the
Chinese do it. But how United States can play a lead in using private sector forces, that's
something many of our countries would like to work with.

CRONIN: And don't want to dominate this with Tom, so - but if you...

EVANS: Say nice things about me.

(LAUGHTER)

CRONIN: I totally agree with Paul on this point because we are creating new metrics of power.
In this economic competition, in an information age of the 21st century, it will be private sector
largely driven. And so we have to figure out how to unleash that, catalyze that. So government
has a role to catalyze this, to incentivize, to set boundaries. But ultimately, it's going to have to
be this new constellation with new metrics of power. And China's appealing to the region,
offering goods, offering public goods. So it's not all bad. It just comes with huge strings attached
and huge risks, I would argue.
DUESTERBERG: OK. Well, let's turn to the audience. I'm sure there are many questions. Why don't we go to the gentleman in the third row? And we have a microphone. Could you state your name and affiliation? And also, make it a question and not a long statement. Thank you.

HIRO MATSURA: Thank you. I am Hiro Matsura (ph) from Japan, and I'm just visiting for the summertime. I have a question to Professor Abraham. I think your theme has been interesting. You tried to assess the capabilities and the problem of three countries - Japan, United States and Britain - and tried to focus on some need for trilateral cooperation But I wanted to re-understand your rationale, why you may focus on this particular trilateral cooperation, possibility of the trilateral cooperation. It is that this particular one is one of the possible many one - why you just put priority on this particular trilateral cooperation. Thinking that Japan's cyber capability and labor of government centralization in this field, maybe Japan is lagging behind more than 10 years.

Well, Japanese government is very good at in documentation for the national cybersecurity. But as you have already mentioned that the United States and United Kingdom have long history and legacy of the second war. And then you have a very close collaboration - collaborative relationship in the intelligence as a core member of the Five Eyes. But Japan is not prepared to have this kind of - well, Japan cannot get into the core of this Five Eyes. So given that, why do you put the priority on the possible trilateral cooperation, why you just picked up that possible one as such? Or you just include this particular case because you have to include the case of Japan because you are on the upper fellowship.

ABRAHAM: No, it's - in fact, the primary reason is because Japan, even though we don't have a direct defense relationship like U.S. and Japan does for Asia-Pacific region, Japanese companies actually provide the industrial base for the Defence Information Infrastructure for the U.K. And it also - so that's one component of it. And when that attack that happened last June, which was by a Russian actor that was going after U.S. IP but did so through Japanese networks, that's basically an indicator of how because of that particular - and I won't divulge the name of that particular vendor, but it was a primary vendor for the U.K. and the U.S. And they share networks. They share information. And so there's a trilateral relationship with these vendors that the countries, if they don't have the same capabilities and security measures that are in place, it could expose vulnerabilities of all three countries.

So that was a case that really kind of made it apparent that there are these extenuating circumstances and linkages that we may not see readily between the countries but that it's exacerbated when you have a cyberattack. So that was my rationale for going with those three. And then also, the U.S. and U.K., as you noted and we've talked about, has an extensive intelligence capacity or assessment capacity, something that can be leveraged by Japan. That does not have the capabilities currently to absorb the amount of information to do the assessment with all the multi-source - their intelligence that it could have. And the U.S. and U.K. have a very mature system for doing so. So why not leverage those capabilities and help Japan build in this threat intelligence analysis area?

DUESTERBERG: OK, who else?

TSUCHIYA: May I?

DUESTERBERG: Sure.
TSUCHIYA: Very quickly. So if you put the United States center, so who is a partner on the Atlantic side? It’s the U.K. No explanation. But who is a partner on the Pacific side? So you're looking at maybe Singapore, South Korea or other countries. But Japan could be one of the best partners. And so U.K. is approaching Japan these days. So maybe two years ago, Prime Minister May came to Japan. And she said, so the United Kingdom will help Japanese cybersecurity because they had Olympic Games in London in 2012, and they are helping us so much. So U.K., Japan is getting closer these days. So what we can do? So we can contain erasure in geopolitical sense. So China is there. Russia is there. North Korea is there. Iran is there. So we can contain those countries with the partnerships.

ABRAHAM: And this relationship actually has extended from the maritime connections between U.K., U.S. and Japan and the Asia-Pacific region being that channel. So from the need to secure a maritime operations, you have connected networks that are sharing information between the three countries that need to have cybersecurity as well. So it’s very critical for these three countries to have comparable capabilities.

DUESTERBERG: Let's go to the lady in the front row here.

LIZ KIM: My name's Liz Kim (ph). I'm a reporter with Voice of America Korean Service. My question might sound a little bit narrow, but I was wondering how each of you assessed North Korea's capability in cyberspace since there have been a lot of reports on North Korea's heist of cryptocurrency these days. And I was also wondering if you believe North Korea's denial of the heist.

CRONIN: Sure. Well, maybe North Korea didn't make $2 billion off the cryptocurrency heist, but they made a lot of money. And I think the point is we need to keep following just how quickly North Korea adapts to both new technologies, especially in cyberspace, as well as the work around sanctions. So the more pressure we can agree on with sanctions, you can be sure that North Korea is not stopping. They're just finding a different path to raise money through a largely illicit economy. So this is a - it's a serious problem. They've got a serious capability, and they are maybe the most likely to disrupt the 2020 Olympics as well.

EVANS: North Korea makes China look good in comparison.

CRONIN: Yes, that's true.

DUESTERBERG: Let's go to this gentleman in the front row here.

RICHARD COLEMAN: Hi. Richard Coleman (ph). I'm retired from Customs and Border Protection. We used to worry about counterfeit electronics getting into critical infrastructure. And now we're bypassing that into the issue here. My question is, and it's a fairly political, technical question, there is apparently one person in Washington who doesn't believe anything that the four experts have told us about cyberattacks. With the coming election in the United States, is there anything that can be done to protect this - our elections at the state level? Now their stuff, presumably, is 4 years old - their software and whatever protection. With the state of the art of ransomware, which has already scored big hits in the United States, is there anything after the fact that you can recommend to remedy our vulnerability there? Or are we basically screwed?

CRONIN: Well, I would just advertise the organization Secure Democracy, which is a bipartisan group that is geared up to deal with not just Russia, but also China now and their election - electronic interference and broader interference in our election next year. They're doing very
good bipartisan work. And they deserve - their recommendations are thoughtful and deserve to be looked at. And they're online.

TSUCHIYA: Luckily, Japan is still using paper ballots.

(LAUGHTER)

DUESTERBERG: OK, time, I think, for one more question - gentleman in the second row here.

DAVE RABINOWITZ: All right. Thank you. I'm Dave Rabinowitz (ph). It's been mentioned that geeks created cyberspace. Basically, geeks are running it and all that. I'm just wondering, why are there no geeks on the stage? They're the ones who know what's going on.

DUESTERBERG: Dr. Abraham is the closest we have to a real expert.

EVANS: A real geek.

DUESTERBERG: So would you like to - would you like to take that one on?

ABRAHAM: They're out preparing technical solutions and don't have - no, but you're right. You're right. They're - I was at a conference for Sans. Are you familiar with Sans? It's a credentialing organization, probably largest internationally for cyber personnel. And a comment was made that we have a lot of frequent flyers in the cyber community but no pilots. And that - and your comment is well taken because a lot of the policy that's being driven is not being driven by the technical experts. And I think that's what we were talking about earlier, is that we need to get them more engaged in the conversation. They have the tools. There are tools out there to assess, to mitigate, to remedy our issues. But we have impediments with legal authorities that don't allow certain technologies to be implemented. We have also just a overall kind of perspective in our manufacturing process for our devices for everything right now that puts national security and cybersecurity interests at the end of the manufacturing process. That should be moved to the beginning. That's what China does. Everything that China produces and uses, domestically, it's gone through audit for cyber. It builds to the cyber specifications that are already identified prior to the development and manufacturing of a device getting to market.

We don't do that. We build things, and we put a lot of time and energy into technology. But the cybersecurity portion of it is an afterthought. And if we get our technologists involved in the manufacturing process to specify how to change this - it's really a mindset - change this culture, then maybe we can also, you know, improve not only a cybersecurity but also boost their - or raise their capacity to inform our policy as well. But if you have an administration who, you know, fires its own CISO for - and subjugates the cybersecurity personnel that are - have the relative acumen, then how can we make that something - you know, raise it to the level of importance that it needs to have?

EVANS: If I could add - I don't think all geeks are born equal or think the same thing.

ABRAHAM: Right.

EVANS: You know, if we start looking at the range in our imagination of what a geek is, it's a guy - a man or a woman who is in love with the technology, usually in love with freedom, and wanting to break barriers down, create new things, operating somewhat independently. First, most geeks that mattered are tied into real organizations and used one way or another. Secondly, as I have met Chinese geeks, they're not exactly identical to my California geek
friends in what they feel their responsibilities are to the state and what they feel their responsibilities are as an actor to serve the state. And on occasion, when I've had the unfortunate opportunities to talk with people who are pretty technologically savvy in using information for purposes of racist or supremacist activities, for people who are on the wrong side of terrorism, a coalition of geeks in the world - some of them are good ones in this process, but some of them aren't.

**TSUCHIYA:** So Jun Murai, he’s my boss at the graduate school. He's called father of the Japanese Internet. He imported Internet technology into Japan. And he and I were sharing the membership of the government council maybe seven years ago. And we were always arguing in the council. So I said, this is a council for thinking about national security, for cybersecurity. But he always says, Internet is global; it's not national. So we have to connect the Internet beyond borders. So the mindsets are very, very different. And my first experience to the geek community is 2002, while I was a Abe fellow, I went to Utah. And there here IETF meeting - Internet Engineering Task Force meeting - in February. It's very cold outside, a lot of snow. But they are wearing short pants and ponytail and T-shirts with a logo and something geeky - worse, actually. And so they were sitting on the ground in a very fancy hotel, and they are typing, all - bah, bah, bah, bah (ph). So their mindsets are very, very different. So Washington people don't understand what they are thinking, actually.

(LAUGHTER)

**TSUCHIYA:** So - I don't understand. So we have to think about - we have to try to understand each other.

**DUESTERBERG:** OK, listen - I - very interesting discussion. But I think we’ve reached a point where we should allow our sponsor from the Social Science Research Corporation (ph), Ron Kassimir, to give some concluding remarks. And he will be followed by Ken Weinstein, our president and CEO. And we can continue the discussions during the reception between 5 and 6. And please take advantage of the presence of these really distinguished speakers, and save your questions for a personal conversation. So Ron.

(APPLAUSE)

**RON KASSIMIR:** So it's never a good thing to stand in the way between a great panel and a reception. And so I will try to be brief and mostly give a few thank-yous. Really, deep appreciation to the panelists, both our - the Abe fellows and Patrick for a really stimulating discussion that I hope we will continue in a more informal way over the - during the reception. I'd also like to thank President Weinstein and his colleagues here at the Hudson Institute for being both such great hosts but also for being engaged interlocutors with these issues. And of course, I'd like to thank Junichi Chano and his colleagues at The Japan Foundation's Center for Global Partnership for their partnership with the SSRC now 28 years with the Abe Fellowship Program - 400 hundred fellows supported over that time and counting. And also for developing the Abe Global Forum, which this is an event of and is a really great way to bring the knowledge that's being produced by the fellows to a wider audience, beyond the academy or beyond their own fields and institutions. So it's a really exciting innovation in the Abe program. And thank you all for being such great contributors to it.

For those of you who don't know much about the SSRC, we're now a 96-year-old private nonprofit foundation, so we'll be around - our centenary is coming up. We're starting to think
about that. And over all that time, we have, as our major mission, promoted social science research through a range of mechanisms - fellowships and capacity-building, deepening the craft of social science research, building research networks across disciplines on major public issues and communicating new understandings to a wide range of stakeholders. And perhaps most broadly, we build bridges within the research community and between it and policymakers, the media and the philanthropic world. So happy - if anyone’s interested to hear more about the SSRC, we can talk at the reception. Just before I conclude, I did want to mention two things that we’re doing at the council that are touched on in some - some in very direct, some in indirect ways, with the discussion we’ve had here today.

First, we have a relatively new social data initiative that looks into the potentials and perils of data and has overseen a fellowship program on the ways in which social media has influenced democratic elections and democratic processes. It features a very unique and very complex partnership between eight foundations and Facebook. And again, if you’re interested, I’m happy to tell you more. Second, we have a program on media and democracy that connects scholars - and convenes scholars to look at how media shapes and affects democratic institutions - all forms of media - shapes democratic institutions and democratic cultures. Next month, we’re going to launch an online research platform that will map in, close to real time, research on disinformation and its potential impact on politics around the world. So if that's something you're following, I hope that - I think this will be a really great resource to give for scholars, but also for practitioners who are interested in these issues, access to the latest debates and latest findings from - on the impact of disinformation. I’d be happy to connect any of you to my colleagues who are working on those programs. So in closing, let me again repeat my thanks for the extraordinary quality of the conversation today on something that really does matter to all of us. And I really appreciate the - not just the panelists but the great questions we had in the Q&A. It's really a pleasure and a privilege to be here with you all. Thanks.

(APPLAUSE)

WEINSTEIN: I'm definitely the last person between you folks and some wonderful food and drinks out in the lobby. Let me just again thank our partners at the Center for Global Philanthropy, at The Japan Foundation, Social Science Research Council. Let me thank the panelists. This was an extraordinary, open, diverse, divergent discussion about critical issues on what are, frankly, the - probably the largest policy challenges that the U.S.-Japan alliance and our alliance partners, including in Canada, face. And it was a very rich discussion. But from my standpoint, the part that I enjoyed the most were the reflections of our Abe fellows on looking back at just how much their experiences as Abe fellows transformed their lives and transformed their professional careers, as I unfortunately was not smart enough to do Asia policy. I did my Ph.D. in political philosophy, specialized not in the 21st century but in the 17th. And I looked back at the numerous grants that I received from the government of France, and they were really transformative for me - contributed to a much deeper understanding.

So I really want to just thank both the SSRC and The Japan Foundation for the extraordinary opportunity you've given to these people who've become major leaders in their field. I want to thank my Hudson colleagues as well for their contributions. And please step out into the lobby, and let's enjoy a reception and the opportunity to get to know each other better. Thank you, everybody, and I want to thank the Hudson Institute team as well for their hard work in pulling this event together. Thank you.