SSRC

ABE GLOBAL | 安倍 ABE FELLOWSHIP PROGRAM

CGP The Japan Foundation Center for Global Partnership

CYBER CHALLENGES: THE INTERNET, GLOBAL COMPETITION, AND NATIONAL SECURITY

ABE GLOBAL | WASHINGTON, DC

SEPTEMBER 5, 2019
HUDSON INSTITUTE
WASHINGTON, DC

安倍 ABE FELLOWSHIP PROGRAM

The Abe Fellowship Program encourages international multidisciplinary research on topics of pressing global concern. The program fosters the development of a new generation of researchers interested in policy-relevant topics and willing to become key members of a bilateral and global research network. In partnership with the SSRC, the Japan Foundation Center for Global Partnership (CGP) established the Abe Fellowship Program as its flagship program in 1991. The Abe Fellowship Program now includes three core elements: the Abe Fellowship, the Abe Fellowship for Journalists, and the Abe Fellows Global Forum (Abe Global).

The Abe Fellowship Program, named after former foreign minister Shintaro Abe, is a critical hub for researchers engaged in US-Japan dialogue and cooperation and continues to facilitate valuable policy-relevant research on pivotal issues facing Japan and the United States. The program has supported over 400 Abe Fellows who make active contributions across the academic and policy worlds not only in the United States and Japan, but throughout the world.

ABE GLOBAL | 安倍 ABE FELLOWSHIP PROGRAM

ABE FELLOWS GLOBAL FORUM

An initiative of the Abe Fellowship Program, the Abe Fellows Global Forum (Abe Global) brings Abe Fellow research and expertise on pressing issues of global concern to broader audiences. Abe Global hosts events each year in partnership with academic and civic organizations throughout the United States.

Cyber Challenges: The Internet, Global Competition, and National Security

ABE GLOBAL | WASHINGTON, DC

Overview

"Information" has become an integral part of our daily lives. We have all become accustomed to the use of apps that ease daily life, and rarely stop to think of the masses of big data that have made them so effective. At the same time, there are worries every time a government, or a company, or an internet server reports a breach of its databases, exposing the private data of millions of people. The worries about information extend from the most intimate personal concerns, to the grand strategies related to national security and defense. While governments have increasingly fine-grained tools for identifying and gathering information on individuals, at the same time, they struggle to defend their systems against attacks from rival powers. As states move to introduce new 5G technology, the commercial interests of tech companies have become entangled with nationalist interests of states, and legitimate concerns about cyber security. These issues are of particular concern in Japan as it prepares to host the Rugby World Cup and the 2020 Olympics; will current cyber security institutions be strong enough to protect such global events? Drawing on the research of Abe fellows this session will

Abe Global | Washington, DC: Thomas J. Duesterberg, Paul Evans, Motohiro Tsuchiya, Dorothea "LaChon" Abraham, Patrick Cronin

examine how these issues are being discussed in the US, Japan, and other parts of Asia, and what new institutions have been developed to deal with the increasingly contentious world of information.

Over nearly three decades, the Abe Fellowship Program has supported several fellows whose research projects discuss the repercussions and benefits of how changing technology has allowed for the increased capacity to create, store, and trade information and data. For Abe Global 2019, three Abe fellows and other experts addressed multi-national cybersecurity coalitions, strategies, and cyber-resilient methods critical to sustaining national functions in inevitable attacks; US-China trade war and techno-nationalism's implications for suppliers, customers, and the global supply chains; and Japan's 2018 National Defense Program Guidelines which focus on Multi-Domain Operations including cyberspace, outer space and electromagnetic space.

Two panelists from the DC event also participated in the EastWest Institute's Global Cooperation in Cyberspace Progress Roundtable - Palo Alto 2019 as part of Abe Global 2019.

Table of Contents

Opening Remarks

September 5, 2019

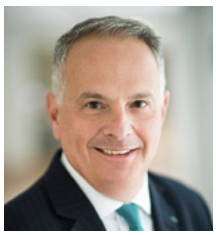
Ken Weinstein

Hudson Institute

Well, good afternoon. And welcome to Hudson Institute. Hudson Institute's mission is to promote US 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—and those watching online—to the 2019 Abe Fellows 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 US-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 cohost this event with our good friends at the Japan Foundation Center for Global Partnerships, whose executive director, Junichi Chano, I will be welcoming 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 whom you will be hearing shortly. The SSRC and CGP are the joint sponsors of the Abe Fellowship Program.



Ken Weinstein is president and chief executive officer of Hudson Institute, and the inaugural holder of the Walter P. Stern Chair. He joined the Institute in 1991 and was appointed CEO in June 2005. He was named president and CEO in March 2011. Dr. Weinstein is chairman of the Broadcasting Board of Governors, the oversight body for US Agency for Global Media, whose entities include the Voice of America, Radio Free Europe/Radio Liberty, Radio Free Asia and Middle East Broadcasting. Weinstein also serves on the Advisory Committee on Trade Policy and Negotiations, which provides counsel on trade agreements to the United States Trade Representative. He previously served on the National Humanities Council, the governing body of the National Endowment for the Humanities. Dr. Weinstein earned his BA in general studies in the humanities from the University of Chicago, DEA in Soviet and Eastern European studies from Institut d'Etudes Politiques de Paris, and PhD in government from Harvard University.

Now, for us at Hudson Institute, today's event combines two major and important themes that have been critical to Hudson throughout our fifty-seven-year history. The first is 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 one; this is particularly important at a time of rapid technological change, which affects the strategic landscape. The second is our deep love for Japan and for the US-Japan relationship. Our founder, Herman Kahn, was, of course, the pioneer—the first man to predict, in 1962, that Japan would be the world's second largest economy. Herman, of course, knew Shintaro Abe well; and we at Hudson have had a long relationship with the prime minister, Abe-san Shinzo, the son of Shintaro Abe. In fact, he presided over the grand opening of our Washington offices—these very offices—in March of 2016.

Much of our work is in the area of cybersecurity, 5G, AI, quantum machine learning, and global supply chain challenges, as well as in the area of great-power competition. I'm 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 the Internet would lead to free and open societies. Instead, in some ways, as we've seen, authoritarian regimes have come to understand the need for information dominance among their own peoples and have come to use 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, and the US Agency for Global Media—whose board of advisers I chair here in Washington—promotes an open and free Internet through the use of 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, and5G 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 and [from] hacking into health insurance companies and presidential personnel systems.

There are major opportunities we, as people of Japan and people of the United States, need to face together, and I look forward to an interesting conversation. 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.

Opening Remarks

September 5, 2019

Junichi Chano

Japan Foundation Center for Global Partnership

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 of today's seminar on cybersecurity. We are truly appreciative of this close collaboration to bring discussion of 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 special legislation to conduct Japan's cultural exchange with the world. There are currently twenty-five offices in twenty-four countries. And the Center for Global Partnership was established within the Japan Foundation in April 1991 as a dedicated unit to promote US-Japan intellectual, as well as grassroots, exchanges.

Junichi Chano was the executive director of the Japan Foundation Center for Global Partnership (CGP) from May 2014 through December 2019. Prior to taking charge of CGP, he served as director general of the Japan Foundation New York, where he oversaw the foundation's cultural exchange programs to the United States. Chano joined the Japan Foundation in 1982 and initially served as deputy director of the Bangkok Office. In 1996, he was appointed director of CGP in New York to manage institutional grant and fellowship programs which supported US-Japan policy-oriented research and dialogue initiatives. His other positions at the Japan Foundation included managing director for Japanese Studies and Intellectual Exchange Department (2007-2008), managing director for Financial Affairs Department (2008-2010), and special assistant to the president (2010-2011). Junichi Chano received his MA in governmental administration from the University of Pennsylvania, and BA in sociology from Doshisha University, where he currently serves as a visiting professor. In 2011-2013, he was affiliated with Johns Hopkins University's School of Advanced and International Studies (SAIS) as a visiting scholar. He is well connected with academics, policymakers, journalists, and foundation officials in both countries, and seeks to further solidify intellectual linkage and exchange between the United States and Japan.

You might recall that the 1980s were a tumultuous time for Japan and the United States. It was during this acrimonious economic interlude that the late Japanese foreign minister, Shintaro Abe—who was, of course, the father of the current prime minister, Shinzo Abe— strongly conceived of the necessity for a mechanism to ensure the two countries continued to forge scholarly, people to people, and other forms of dialogue, irrespective of the political times. And, as a matter of fact, Foreign Minister Shintaro Abe announced this concept back in 1990, when he was in Washington, DC, to commemorate the thirtieth anniversary of the 1960 revision of the US-Japan security pact. The leadership of the US government and those who were engaged in the bilateral relations in private and nonprofit sectors at the time were extremely supportive of Foreign Minister Abe's idea, which led to the establishment of the CGP a year later.

Based on this tradition, the CGP remains dedicated to promoting the global US-Japan partnership and nurturing the next generation of public intellectuals and leaders necessary to sustain this particular partnership. In order to carry out this mission, the CGP supports the Abe Fellowship Program, policy-oriented research grants, and other initiatives.

Three years ago, in 2016, the CGP and the Abe Fellowship celebrated their tweny-fifth anniversary. We are much delighted to have supported more than four hundred Abe Fellows over the past twenty-eight years. This diverse network of policy scholars and practitioners has been and will continue to be a growing asset for US-Japan bilateral relations.

To this end, the Abe Fellows 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, Georgia, and New York on topics like innovation policy in science and technology and climate change.

Now, given its prevalence in news headlines in recent years, I probably don't have to remind this audience about the importance and relevance of cybersecurity in both the personal and national spheres. As technology has increasingly become part of our everyday lives, cybersecurity has likewise become a vital concern. The issues of particular concern include both technical and policy-oriented discussions, the enhancement of the resilience of the Internet against botnets and other such threats, the Democratic Defense Against Disinformation, based on the notion of the free flow of data free with trust, and the rise of so-called technonationalism, to name a few.

Drawing on the research of Abe Fellows, this forum will examine how these complex issues are being discussed in the United States, Japan, and other countries. The Japan-US relationship has evolved to become a vitally important partnership, both regionally and globally. Numerous issues would benefit profoundly from Japan and the United States merging our intellectual capabilities and diplomatic efforts, and such an issue is the very one 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 the Abe community and Hudson Institute to discuss these issues with us today. On behalf of 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. Thank you, and please enjoy the afternoon.

Comparing National Cyber Capabilities and Strategies of Japan, the United States, and the United Kingdom

Dorothea LaChon Abraham

William & Mary

Introduction

Japan, the United States, and the United Kingdom share common adversaries in cyberspace. The United States attributes to China intellectual property (IP) losses of an estimated $20 billion–$30 billion annually through cyber espionage,[1] while the global annual cost of cybercrime is estimated at 1 percent of global gross domestic product (GDP).[2]

In comparison to other sectors, like finance, vital infrastructure such as that supporting government, health, and education services typically lacks advanced safeguards. Security budgets are inadequate, and in-house cybersecurity professionals are in short supply. The telecommunications infrastructure relies on components and data across a global supply chain of varying security provenance and quality, which introduces the challenge of dealing with embedded threats in shared critical infrastructure (CI) and is itself a marker for understanding the principal differences in rulemaking and cyber resilience among nation states.

Against these challenges, harmonized cybersecurity strategies can form part of a foundation of shared global defense, although this foundation can provide only a "common operating framework" because cybersecurity priorities are not globally uniform among governments. The effectiveness of national cybersecurity strategies is shaped by, first, the capacity of a nation state to enforce laws, engage

Dorothea LaChon Abraham (2017 Abe Fellow) is an associate professor in the Mason School of Business at William & Mary in Williamsburg, Virginia, where her research and teaching involve business intelligence, cyber and information security, data management, and health information management. She is a graduate of the US Military Academy at West Point, has a PhD in Management Information Systems from the University of Georgia, and a MBA from Old Dominion University in Norfolk, Virginia. Chon is a lieutenant colonel in the United States Air Force Reserve based at the Pentagon in the Chief Data Office. She also is a 2008 Fulbright Scholar to Japan and a recent Abe Fellow. She engages in applied research to deliver practical insights to organizational leaders, managers, and frontline personnel. Additionally, she co-authored a 2018 book titled *Hacking Healthcare: Understanding Real World Threats*.

in the international sphere, and prosecute cybercriminals across jurisdictions; second, national technical oversight of information assets, information sharing, standards, and interoperability; and, third, cultures surrounding cybersecurity among government and business leadership.

For my research, I have conducted interviews with cybersecurity professionals in the United States, Japan, and the UK, complemented by literature review and analysis of comparable national frameworks, to consider the cybersecurity strategies of these three countries with regard to these measures. My investigation examines, first, differences in legal authority, technical oversight, and business ecosystem engagement capabilities; second, effects of different capabilities on the cybersecurity national strategy for each country in terms of defensive and offensive operations, prioritization of industry sectors to protect, responsibility designations among government and private sector entities, and how information is shared among all stakeholders; and, third, the implications of differences in cybersecurity national capabilities for international collaboration in cyber defense.

Common Adversaries

Japan, the United States, and the UK share common adversaries in cyberspace that work to weaken national defense, illegally acquire IP, destabilize global alliances, and disrupt supply chains (see table 1). IP theft is not a new challenge for governments, but the problem has been exacerbated markedly by the advent of the digital economy, with some countries effectively enjoying a research and development (R&D) subsidy at the cost of global innovation.[3] According to the Center for Strategic and International Studies (CSIS), the annual loss of United States IP through global theft likely reaches an estimated $600 billion annually. Of this, Chinese cyber espionage accounts for $20 billion–$30 billion per year.[4] Following the widespread, high-profile cyberattacks of 2017, renewed calls for an international response[5] to shared threats placed cyber among the top five global risks for 2018[6] and 2019.[7]

Losses due to cyberattacks are increasing in Japan, the United States, and the United Kingdom, with attacks on public, government, and critical infrastructure. 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 of particular concern for Japan, with a flood of these devices expected during the Tokyo Olympics. And while Japan was not directly the target of a recent cyberattack by Russia on a US defense contractor operating there, its networks were attacked in an attempt to gain access to US trade secrets. Domestic networks of any of the three countries are at risk if used to engage with a vendor supplying any one of the other nations; this highlights the need for shared responsibility in improving accountability.

Table 1. Timeline of Selected Cyberattacks and Attributions in Japan, the United States, and the United Kingdom

August–December 2011	Mitsubishi Heavy Industries, IHI Corporation, Kawasaki Heavy Industries, and Japan Aerospace Exploration Agency discover malware and an advanced persistent threat (APT) in their systems.[a]
September 2012	Japan's government agencies are targeted following acquisition of Senkaku/Diaoyu Islands.[b]
June 2015	Targeted attack on Japan Pension Service affects data for 1.25 million people.
November 2015	Distributed Denial of Service (DDoS) generates 12-hour disruption to the IT systems of the Tokyo Organizing Committee of the Olympic and Paralympic Games.
November 2016	Attack on the National Defense Academy of Japan and National Defense Medical College seeks machines to use as a gateway to the Defense Information Infrastructure.[c]
May 2017	Total cost of the NotPetya attacks of 2017 to Maersk and others estimated at least $543 million;[d] WannaCry affects at least 100 countries, global costs estimated at $7.4 billion;[e] 600 organizations across Japan are affected, including Hitachi and hospitals.
December 2017	United States formally attributes WannaCry to North Korea.[f]
February 2018	UK formally attributes the June 2017 NotPetya attacks to Russia;[g] analysts identify Russian cyber operations as a feature of state-led organized crime.[h]
March 2018	United States publicly and formally attributes attacks targeting energy and critical infrastructure to Russia.[i]
April 2018	Reports emerge of Chinese state-sponsored hacking groups targeting Japan's defense companies, seeking information on Japan's policies toward North Korea.
October 2018	United States indicts a Chinese intelligence officer for economic espionage, including theft of IP from US aerospace companies.[j]
December 2018	UK assesses with highest level of probability that the group APT10 has acted on behalf of the Chinese government to launch systematic campaigns targeting IP and commercial data in Europe, Asia, and the United States.[k]

a P. Kallender, "Japan, the Ministry of Defense and Cyber-Security," RUSI Journal 159, no. 1 (2014): 94–103, DOI: 10.1080/03071847.2014.895264.

b P. Kallender and C.W. Hughes, "Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace," Journal of Strategic Studies 40, no. 1–2 (2017): 118–45, DOI: 10.1080/01402390.2016.1233493.

c Hiroyuki Arie, "Japan's Approach to Tackling Cybersecurity Challenges," Japan Industry News, January 17, 2017, https://www.japanindustrynews.com/?s=Japan%E2%80%99s+Approach+to+Tackling+Cybersecurity+Challenges&submit=Search.

d "NotPetya's Fiscal Impact: $592.5 Million and Growing," Cybereason, September 6, 2017, https://www.cybereason.com/blog/blog-notpetyas-fiscal-impact-592-5-million-and-growing.

e Reuters, "Global Cyber Attack Could Spur $53 Billion in Losses: Lloyd"s of London," July 17, 2017, https://www.reuters.com/article/us-cyber-lloyds-report/global-cyber-attack-could-spur-53-billion-in-losses-lloyds-of-london-idUSKBN1A20AB.

f The White House, "Press Briefing on the Attribution of the WannaCry Malware Attack to North Korea," December 2017, https://www.whitehouse.gov/briefings-statements/press-briefing-on-the-attribution-of-the-wannacry-malware-attack-to-north-korea-121917/.

g UK Foreign and Commonwealth Office, National Cyber Security Centre, "Foreign Office Minister Condemns Russia for NotPetya Attacks," February 15, 2018, https://www.gov.uk/government/news/foreign-office-minister-condemns-russia-for-notpetya-attacks.

h James Sullivan, "Russian Cyber Operations: State-Led Organised Crime," RUSI, November 28, 2018, https://rusi.org/commentary/russian-cyber-operations-state-led-organised-crime.

i US Department of Homeland Security, "Computer Emergency Readiness Team, Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors," Alert TA18-074A, March 15, 2018, https://www.us-cert.gov/ncas/alerts/TA18-074A.

j US Department of Justice, "Chinese Intelligence Officer Charged with Economic Espionage Involving Theft of Trade Secrets from Leading US Aviation Companies," press release 18-1318, October 10, 2018, https://www.justice.gov/opa/pr/chinese-intelligence-officer-charged-economic-espionage-involving-theft-trade-secrets-leading.

k UK Foreign and Commonwealth Office, National Cyber Security Centre, "UK and Allies Reveal Global Scale of Chinese Cyber Campaign," December 20, 2018, https://www.gov.uk/government/news/uk-and-allies-reveal-global-scale-of-chinese-cyber-campaign.

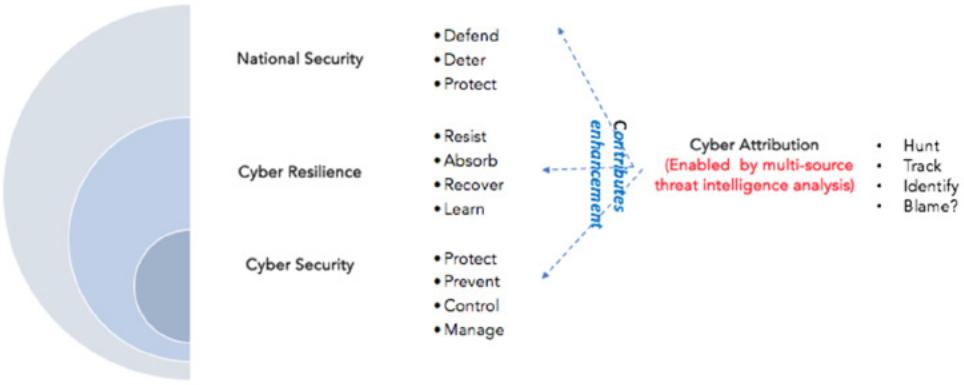
In terms of cyber risks to critical infrastructure, the United States identifies sixteen national CI sectors,[8] similar to the thirteen each identified in the UK[9] and Japan.[10] In April 2019, the Cybersecurity and Infrastructure Security Agency (CISA, under the US Department of Homeland Security National Risk Management Center) released details of US National Critical Functions,[11] which broadly comprise four activities: "*connect*," "*distribute*," "*manage*," and "*supply*"—that is, the full range of activities required to sustain "business as usual" at the scale of a nation state. This development in the US approach is key to reevaluating how we conceptualize accountability and cyber resilience, because it considers capabilities across sectors rather than stove piping across industries. Similarly, the UK has concluded that a *critical systems* approach should extend into the supply chains that support the UK critical infrastructure. This complements the defense mission, because it is action oriented—that is, it considers the tasks that every part of the system needs to

focus on, whatever its business role, to harden the critical systems and information flow for resiliency. The US CISA is advising Japan's National Information Security Center (NISC) on how on how to organize cyber resiliency activities using the critical national functions approach.

Cyber Strategies and National Capabilities

Achieving national cyberspace accountability includes developing comparable security, resiliency, and attribution capabilities in a whole-of-society framework that contributes to national security (figure 1). While cybersecurity is foundational to protecting assets from an attack happening in the first place, cyber resiliency provides assurance that critical infrastructure will remain effective and operational even while under attack. Attribution supports security and resiliency by drawing on threat intelligence analysis, using multiple sources to learn the tactics, techniques, and procedures used by adversaries.

Figure 1. Accountability: A Whole-of-Society Task



National cyber strategies. Securing cyberspace requires collaboration among companies and nation states if all are to enjoy the benefits of the digital economy. Set against this challenge are fundamental differences in our perspectives as nation states on the task of "national security." All strategies note the need to strengthen engagement with the business ecosystem, since much of the critical infrastructure in each country is owned and operated by the private sector.

Japan has now openly espoused deterrence as a strategic goal. Japan's Cybersecurity Policy for Critical Infrastructure Protection sees an equal division of labor between government and the private sector.[12] The UK approach to cybersecurity is inherited from the national security strategy of "defend, deter, develop"—that is, it seeks to enable cyber defense, deter attack, and invest in R&D to enhance cyber resilience,

with overall emphasis on improving risk management and devolving responsibility to individual companies.[13] The United States and the United Kingdom articulate deterrence while continuing innovations in offensive capabilities, which requires attribution capability.

Cyber authorities. In the United States, the Department of Justice and the Federal Bureau of Investigation (FBI) assume responsibility for domestic cybersecurity, including investigation and law enforcement. The Department of Defense (DoD) and National Security Agency (NSA) are responsible for national defense and securing the United States in international cyberspace, with the Department of Homeland Security (DHS) performing a coordinating role. In Japan, cybersecurity responsibilities are coordinated by the NISC, established in 2005. Direct communication platforms exist between the United States and the United Kingdom for sharing information among authorities. A challenge for cyber authorities across all three countries is that the defense industrial base comprises many private sector suppliers who transmit across computer networks of managed service providers (MSPs) not owned by government. Fragmentation of cyber authority in the United States and the United Kingdom is being addressed; for example, in the United States, NSA's new Cybersecurity Directorate will unify NSA's foreign intelligence and cyber defense missions to reduce risks to national security systems and the defense industrial base.

In national cybersecurity, governments face a challenge and a choice: to develop a single agency that "owns" cyber on behalf of the nation (and develop a talent base to support it) or to require departments and sectors to adhere to national laws and

frameworks, consistently and effectively. The challenge with the first method is to develop a model that has the buy-in of the private sector (particularly in the example of the UK) while reconciling different operational cultures; with the second, it is to devise an incentives and fines structure that is enforceable on a meaningful scale and within a meaningful time frame. Interviews conducted for my research have suggested that the Japan Computer Emergency Response Team (JPCERT) could be formalized within the government. This move presents a continuity and corporate knowledge management challenge, however, that is readily compared with the UK experience of setting up the National Cyber Security Centre (NCSC).[14]

Strategic culture. Comparing cyber capabilities is important to understanding power relationships between nation states,[15] but comparative research in national cyber resilience cultures is at a nascent stage. I suggest that national cyber resilience culture is subject to three influences: perceived threats and security priority; laws and authorities; and information-sharing culture. In the United States, we are particularly concerned about the threat to our economy from cyber economic espionage, notably from China. The UK focus is on countering financial crimes, countering the cyber threat from Russia, and mitigating threats to critical national infrastructure. Japan's focus is currently on the security of society and on mitigating threats to national security around the occasion of the Olympic and Paralympic Games.[16]

The role of the private sector. Irrespective of differences in national strategic cultures, improving cybersecurity in the private sector is a key tenet of each country's strategy. Possible strategies include tax breaks, cyber discounts, cyber maturity certifications, and the creation of a trusted vendor pool status. About half of Japanese companies conduct cybersecurity risk assessments, compared to roughly 80 percent in the United States and 65 percent in Europe. Similarly, only 27 percent of Japanese companies have a chief information security officer (CISO), compared with 78 percent of US and 67 percent of European companies.

Legal Frameworks

In 2012, Japan acknowledged cyberspace as an operational domain under international law[17] and, in 2018, the National Defense Program Guidelines recognized "space, cyberspace and the electromagnetic spectrum," across which Japan should expand capabilities in "cross-domain warfare."[18] Japan's view is that "the rule of law should also be maintained in cyberspace, [and] existing international law is also applied in cyberspace."[19] Similarly, the UK view is that "international law should apply in cyber as in other realms, and [we] will work with others to ensure this."[20] Japan is unique among the three countries considered in this research

in having a Cybersecurity Law. While its Article 9 does not prevent Japan from conducting attribution analysis on known attacks, levying sanctions, or applying other diplomatic methods, naming and shaming is not part of Japan's culture.

In the United States, cybercrimes are generally prosecuted under Title 18 of the US Code.[21] The complete criminal law with respect to cybercrimes is set out by the US Department of Justice,[22] which also advises on how and where investigation teams may operate.[23] The US Federal Acquisition Regulation[24] and supplementary regulations cover many of the contracts that directly affect the country's critical infrastructure.[25] Individual states and cities also have their own laws.[26,27,28] In keeping with its culture of "fine and punish," the United States is the most effective of the three countries considered in this analysis in utilizing the rule of law to deter IP theft.[29]

By 2018, most countries had enacted some form of cybersecurity legislation,[30] but laws are of limited value if the ability to enforce them is weak and attribution and prosecution takes months or years. In Japan, some have advocated for elevating the seriousness of cyberattacks on critical infrastructure within Japanese law and approving a defense trade secret act (equivalent to the US Foreign Investment Risk Review Modernization Act) to strengthen Japan's cyber defenses. The United States and the United Kingdom also utilize controls on dual-use technologies (UK), asset-freezing targets (UK), and Securities and Exchange Commission (SEC) control lists (United States). The practice of blacklisting is effective in the United States, while in Japan agencies do not share blacklisted company information with Japanese businesses for fear of economic retribution on Japanese companies. Japan acknowledges US blacklists but shies from imposing them on its own business ecosystem or enforcing a fine structure. Similarly, the UK is effective in monitoring and sanctioning suspect entities, particularly in the financial services industry, but the broader corporate environment remains open to foreign manipulation.

Challenges to Collaboration on Attribution Analysis and Threat Intelligence

In the United States, the principal platforms for threat intelligence sharing are provided by the DHS and the FBI.[31] The FBI Internet Crime Complaint Center (IC3) provides the public with a mechanism for reporting suspected Internet crime, while its Cyber Action Team (established in 2006) provides a rapid response unit—although the FBI is limited to investigation, and its remit does not extend to informing the affected company or companies. The Industrial Control Systems-Cyber Emergency Response Team (ICS-CERT)[32] provides threat advisories. Departments also rely on commercial providers for threat intelligence. In Japan, myriad actors and contested jurisdictions have, by necessity, produced some cooperation. The National Police

Agency (NPA) operates probably the largest ecosystem (an estimated 2,000 businesses are using it), but it is more for outreach.

In all three countries, Information Sharing and Analysis Centers (ISACs) robustly share unclassified industry threat and mitigation information in critical infrastructure sectors. The United States and United Kingdom share threat intelligence information as part of the Five Eyes alliance for signals intelligence cooperation with Australia, New Zealand, and Canada. As of December 2018, Japan had committed to engaging more actively with the Five Eyes and to increasing its capability to assess multisource threat intelligence, although threat intelligence and counter-intelligence sharing is limited by Japan's constitution. The United States and the United Kingdom have a more direct capability to share classified

Table 2. Recent Progress in International Collaboration on Cyber

July 2013	Legal framework for UK-Japan "2+2"—includes Information Security Agreement
January 2015	UK-Japan Strategic Dialogue (Sasakawa Peace Foundation/ Royal United Services Institute)
August 2017	Cyber formally included in Japan-UK Joint Declaration on Security Cooperation
September 2018	US-Japan Cybersecurity Joint Training with Association of Southeast Asian Nations (ASEAN) member states—36 participants from 15 countries and regions
July 2018	Council to Secure the Digital Economy, International Botnet Guide
November 2018	700 cyber defenders from among NATO allies, partners, industry, and academia trained by 11th annual NATO Cyber Coalition
January 2019	US-Japan Security Seminar: Challenges and Opportunities for the Alliance
June 2019	US-Japan Roadmap Working Group (US Cyber Command/ Japanese Ministry of Defense); exercises to follow including ministries and critical national infrastructure suppliers
June 2019	Bilateral dialogue with CISA, DHS, and NISC on workforce development
2008–current	Joint exercises (e.g., DHS-sponsored Cyber Storm, with US/ UK involvement since 2008 and Japan involvement in 2013 and 2018)

information than Japan does, as Japan's platform sharing currently does not allow direct exchange of classified information with allies, and there are issues with comparable data classification schemes.

International Collaboration

Table 2 indicates the scope of the extensive dialogue among Japan, the United States, and the United Kingdom. The formal Japan-US defense cooperation guidelines have included cyberspace since the 2015 revision. They specify that the two governments will cooperate to protect critical infrastructure, and that, in the event of a cyberattack against any part of Japan's critical infrastructure used by both the US Armed Forces and Japan Self-Defense Forces, Japan will have the primary responsibility to respond; the United States will provide support that could escalate to its conducting offensive operations on behalf of Japan. The Cyber Defense Policy Working Group set up in 2013 includes information sharing and critical infrastructure protection within its scope.

Most of the UK-Japan formal relationship is structured under the "2+2," led by ministers from Japan's Ministry of Foreign Affairs and the UK's Foreign Office and Ministry of Defence, which set a three-year plan for UK-Japan defense cooperation. The 2013 legal framework for UK-Japan defense and security cooperation includes an Information Security Agreement, which allows for the exchange of classified information. Allies still lack direct access, however, to a platform that can deliver forensic data for rapid attribution of attacks.

Conclusions

The emerging conclusions of my research suggest the capacity of a nation state to build cyber resilience and hold adversaries accountable is based on the quality and depth of national technical oversight, threat intelligence, standards, and interoperability. Securing critical infrastructure is a top concern for Japan, the United States, and the United Kingdom (and many other nations). A gap exists, however, between the expressed concern and enforceable laws. Too much government oversight is a bad thing for free market economies; too little is a terrible thing for national security.

The effectiveness of the different cybersecurity strategies of nation states is shaped, first, by the capacity of a nation state to enforce laws, engage in the international sphere, and prosecute cybercriminals across jurisdictions; second, by national technical oversight of information assets, information sharing, standards, and interoperability; and, third, by the culture surrounding cybersecurity among

government and business leadership. Existing collaboration frameworks can lay a foundation for stronger, shared accountability and resilience in cyberspace.

The findings of this research suggest the need to formalize a trilateral agreement for building cyber capabilities and accountability. Such an agreement would address four areas:

1. Accountability across entire supply chains, with monitoring of foreign direct investments for critical infrastructure and DIB and blacklisting of firms that fail to meet minimum cyber performance standards
2. Authority for attribution capability oversight
3. Improved threat intelligence, including exchange across critical national functions and among allies, using a common framework
4. Workforce development via public-private training models, such as those already emplaced by DHS, DoD, and United States Cyber Command (USCYBERCOM)

Strategic culture and priority accorded to cybersecurity among government and business leadership form the context within which we can carry out attribution and hold adversaries accountable. Harmonizing how we use and share threat intelligence and improve attribution analysis capability could transcend the variation in our strategic cultures, help close the gap in cyber capabilities, and improve collective action against the many known adversaries. How we strategize, as individual nations and collectively, can reduce the risk of a catastrophic event.

NOTES

1. J.A. Lewis, "How Much Have the Chinese Actually Taken?" CSIS, March 22, 2018, https://www.csis.org/analysis/how-much-have-chinese-actually-taken.

2. CSIS, "Economic Impact of Cybercrime," February 21, 2018, https://www.csis.org/analysis/economic-impact-cybercrime.

3. Lewis, "How Much Have the Chinese Actually Taken?"

4. Ibid.

5. NATO, "NotPetya and WannaCry Call for a Joint Response from International Community," 2017, https://ccdcoe.org/notpetya-and-wannacry-call-joint-response-international-community.html.

6. Economist Intelligence Unit, "World Risk: Alert—Global Risk Scenarios," January 17, 2018, http://viewswire.eiu.com/index.asp?layout=RKArticleVW3&article_id=1876319171.

7. Economist Intelligence Unit, "Economic and geopolitical insight guiding the world's organisations," 2019, https://pages.eiu.com/rs/753-RIQ 438/images/Global_risks_2019.pdf.

8. Department of Homeland Security Cybersecurity and Infrastructure Security Agency, "Critical Infrastructure Sectors," March 24, 2020, https://www.dhs.gov/critical-infrastructure-sectors.

9. Centre for the Protection of National Infrastructure, "Critical National Infrastructure," September 2019, https://www.cpni.gov.uk/critical-national-infrastructure-0.

10. National Center of Incident Readiness and Strategy of Cybersecurity (NISC), Cybersecurity Policy for Critical Infrastructure Protection 4th ed, (2017), p.54, https://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4_r1.pdf

11. Department of Homeland Security, "National Critical Functions," January 13, 2020, https://www.dhs.gov/cisa/national-critical-functions.

12. Government of Japan, Cybersecurity Strategic Headquarters, "The Cybersecurity Policy for Critical Infrastructure Protection," 4th ed., April 18, 2017, http://www.nisc.go.jp/eng/pdf/cs_policy_cip_eng_v4.pdf.

13. Her Majesty's Government, "Cyber Security Regulation and Incentives Review," December 21, 2016, https://www.gov.uk/government/publications/cyber-security-regulation-and-incentives-review.

14. For details, see R. Hannigan, "Organising a Government for Cyber: The Creation of the UK's National Cyber Security Centre," RUSI Occasional Paper, February 27, 2019.

15. Nigel Inkster, "Measuring Military Cyber Power," *Survival* 59, no. 4 (2017): 27–34, DOI: 10.1080/00396338.2017.1349770.

16. M. Matsubara, "How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World," Council on Foreign Relations, June 4, 2018, https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world.

17. Kallender and Hughes, "Japan's Emerging Trajectory as a 'Cyber Power.'"

18. In person interview with Dr. Kenzo Fujisue Senate, House of Council, Japan Government Administration, on Dec 10, 2019.

19. National Center of Incident Readiness and Strategy for Cybersecurity, "Cybersecurity Strategy," section 3.1, July 27, 2018, http://www.nisc.go.jp/eng/pdf/cs-senryaku2018-en.pdf, 10.

20. Her Majesty's Government, "National Cyber Security Strategy 2016 to 2021," November 1, 2016, https://www.gov.uk/government/publications/national-cyber-security-strategy-2016-to-2021.

21. Cornell University, "18 US Code §1030. Fraud and related activity in connection with computers," https://www.law.cornell.edu/uscode/text/18/1030.

22. Office of Legal Education, "Prosecuting Computer Crimes," https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf.

23. US Department of Justice Cybersecurity Unit, "Cybersecurity Unit," March 12, 2020, https://www.justice.gov/criminal-ccips/cybersecurity-unit.

24. US Federal Acquisition Regulation, "Federal Acquisition Regulations System," May 07, 2020, https://www.acquisition.gov/browsefar.

25. US Federal Acquisition Regulation, "Supplemental Regulations," Last updated May 07, 2020, https://www.acquisition.gov/Supplemental_Regulations

26. New York State Department of Financial Services, FAQs: 23 NYCRR Part 500 – Cybersecurity, https://www.dfs.ny.gov/industry_guidance/cyber_faqs

27. US Senate Bill 1386 Chapter 915, 2002, http://www.leginfo.ca.gov/pub/01-02/bill/sen/sb_1351-1400/sb_1386_bill_20020926_chaptered.pdf

28. State of California Department of Justice, "Data Security Breach Reporting," 2020, https://oag.ca.gov/ecrime/databreach/reporting

29. The Commission on the Theft of American Intellectual Property, "Written Comments on Behalf of The Commission on the Theft of American Intellectual Property to The United States Trade Representative," May 11, 2018, http://www.ipcommission.org/report/ustr_written_comments_301_tariffs-may2018.pdf

30. International Telecommunication Union (ITU), "Global Cybersecurity Index 2018," draft, 2018, https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

31. U.S Department of Homeland Security, "National Cybersecurity and Communications Integration Center," June 5, 2019, https://www.dhs.gov/cisa/national-cybersecurity-communications-integration-center

32. U.S Department of Homeland Security, "ICS-CERT" https://ics-cert.us-cert.gov/advisories

The Global Competition for Information Superiority

Patrick Cronin

Hudson Institute

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*. Thus, 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.

Let me briefly 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.

"Cybersecurity" needs to be considered in historical context.

Information has always been vital to intelligence and security. Consider even the relatively recent history of signals intelligence (SIGINT). After World War I, the

Patrick M. Cronin is the Asia-Pacific security chair at Hudson Institute. Dr. Cronin's research program analyzes the challenges and opportunities confronting the United States in the Indo-Pacific region, including China's total competition campaign, the future of the Korean peninsula, and strengthening US alliances and partnerships. Dr. Cronin was previously senior advisor and senior director of the Asia-Pacific Security Program at the Center for a New American Security (CNAS), and before that, senior director of the Institute for National Strategic Studies (INSS) at the National Defense University, where he simultaneously oversaw the Center for the Study of Chinese Military Affairs. In 2001, Dr. Cronin was confirmed by the United States Senate to the third-ranking position at the US Agency for International Development (USAID). While serving as assistant administrator for policy and program coordination, Dr. Cronin also led the interagency task force that helped design the Millennium Challenge Corporation (MCC). From 1998 until 2001, Dr. Cronin served as director of research at the US Institute of Peace. Prior to that, he spent seven years at the National Defense University, first arriving at INSS in 1990 as a senior research professor covering Asian and long-range security issues. He was the founding executive editor of *Joint Force Quarterly* and subsequently became both deputy director and director of research at the Institute.

British established a global peacetime codebreaking organization designed to intercept and decode diplomatic cryptosystems. This interwar SIGINT agency, the Government Code and Cypher School (better known as GC&CS), was the precursor to the post-World War II Government Communications Headquarters (GCHQ).[1]

From wiretapping stations in Hong Kong and Shanghai, the British GC&CS intercepted communications detailing secret, Soviet-backed organizations in China. In the 1920s, these intercepts enabled Chiang Kai-shek to deliver an early blow to the Communist insurgency in China, as well as to humiliate 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. Predating Wikileaks by eighty years, Dai Li went on to evolve his Clandestine Investigations Section into the innocuous-sounding "Investigations and Statistics Bureau."

Accumulating dossiers and statistics is another way of amassing information, 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 twenty-first century's global economy.

We have embarked 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."[2]

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 (AI), the Internet of Things, 3D printing, and quantum computing. These technologies are vital to economic clout and preeminence. That is why in 2015 China issued a ten-year state industrial strategy—Made in China 2025—as a roadmap for ensuring Beijing would be the world beater in next-generation information technology and telecommunications, AI, and other high-tech industries.[3]

The tussle over 5G telecommunications encapsulates the competition for economic preeminence embedded in information technologies. Chinese tech company 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 pass through it.[4] Huawei relies on products, pricing, and various state inducements (from China's 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 thirty-two years ago—four years after leaving the People's Liberation Army (PLA). Having set up shop in the Shenzhen Special Economic Zone adjacent to Hong Kong, Huawei came to epitomize Beijing's approach to "profiting from and buying the rest of the world."[5] China's 5G ambitions are inseparable from Beijing's desire to dominate the global "infosphere."[6]

China is accumulating, through all means, the biggest collection of data in the world and using it 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 enable China 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 investment opportunities, driving not just economic growth but also tomorrow's military systems.

Information power could determine which country enjoys military primacy in the Indo-Pacific region, if not worldwide.

China's desire to rule the world in AI by 2030 is both a bold ambition and a threat that cannot be ignored by businesses or governments.

Chinese writers clearly think China's chances of becoming the world leader in AI over the next decade are excellent. Edward Tse argues, for instance, that,

> 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. My bet is that China will indeed reach its goal over the next decade, in part because of how far it has already come. *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 vibrant grassroots-level innovation.*[7]

Or as Eric Schmidt, then chairman of Google's parent company, Alphabet, told an audience of Americans, "The future will belong to countries that can surf the technological tidal wave of artificial intelligence, and while China's efforts appear up to the challenge, the United States is swimming in the wrong direction."[8]

China technology specialist Elsa Kania has captured as well as anyone Xi Jinping's gambit for becoming a world-class military power by leveraging emerging technologies. As she wrote recently,

> The PLA aspires not only to equal but also to surpass the US 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. The PLA may even offset US 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 the US-China relationship.[9]

Information-driven economic development is dual use and thus 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.

Security in the public square in the digital age is a "wicked problem" for democracies.

In his 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 their American Counterparts."[10] This is seen in myriad ways, as the Chinese Communist Party (CCP) 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 Freedom of Information and Protection of Privacy (FOIP). 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. China is turning the American reaction to its exploitation of rules and the digital age 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 concerning—even alarming—multifaceted campaigns led by organizations such as the United Front Work Department.[11] Taiwan's election in 2020 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 authoritarian systems 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 postwar liberal international order championed by the United States and Japan. As one Japanese commentator wrote recently about China's export of everything from its social credit scoring system to surveillance-state technology, "China's Orwellian vision of the future has huge implications for how its battle with the US for global hegemony will play out. If . . . many Asian nations opt for authoritarianism, the foundations of the US-led liberal order will gradually erode."[12]

To sum up, the Internet, global competition, and national security are intertwined in the twenty-first century. Not only must countries like the United States and Japan 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.

NOTES

1. Christopher Andrew, *The Secret World: A History of Intelligence* (New Haven and London: Yale University Press, 2018), 576.

2. Klaus Schwab, "The Fourth Industrial Revolution: What It Means, How to Respond," World Economic Forum, January 14, 2016, https://www.weforum.org/agenda/2016/01/the-fourth-industrial-revolution-what-it-means-and-how-to-respond/.

3. James McBride and Andrew Chatzky, "Is 'Made in China 2025' a Threat to Global Trade?" Council on Foreign Relations, *Backgrounder*, May 13, 2019, https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade.

4. Shaun Turton and Tomoya Onishi, "Cambodia 5G Set to Leapfrog ASEAN Rivals with Huawei and ZTE," *Nikkei Asian Review*, September 5, 2019, https://asia.nikkei.com/Spotlight/5G-networks/Cambodia-5G-set-to-leapfrog-ASEAN-rivals-with-Huawei-and-ZTE; Pauline Reich, June Park, Aman Thakker, Motohiro Tsuchiya, and Danielle Cave, "Asia's Great Huawei Debate," *The Diplomat*, no. 57, August 2019, https://magazine.thediplomat.com/#/issues/-LkcL5rbLCPRkBz-CXfY/read.

5. These words were written by French journalist Roger Faligot in his comprehensive analysis of Chinese intelligence operations, *Chinese Spies: From Chairman Mao to Xi Jinping* (London: Hurst & Co., 2019), 285.

6. William Schneider, Jr., "China, 5G, and Dominance of the Global 'Infosphere,'" Hudson Institute Briefing Memo, September 2019, https://s3.amazonaws.com/media.hudson.org/Hudson_Institute_China_5G_Digital_Silkroad%20FINAL.pdf.

7. Edward Tse, "Inside China's Quest to Be the Global Leader in AI," *Washington Post*, October 19, 2017, https://www.washingtonpost.com/news/theworldpost/wp/2017/10/19/inside-chinas-quest-to-become-the-global-leader-in-ai/. Emphasis added.

8. Gregory C. Allen, "China's Artificial Intelligence Strategy Poses a Credible Threat to US Leadership," Council on Foreign Relations, *Net Politics Blog*, December 4, 2017, https://www.cfr.org/blog/chinas-artificial-intelligence-strategy-poses-credible-threat-us-tech-leadership.

9. Elsa B. Kania, "Chinese Military Innovation in Artificial Intelligence," CNAS, June 7, 2019, https://www.cnas.org/publications/congressional-testimony/chinese-military-innovation-in-artificial-intelligence.

10. Niall Ferguson, *The Square and the Tower: Networks and Power, from the Freemasons to Facebook* (New York: Penguin Press, 2018), 417.

11. Anne-Marie Brady, *Magic Weapons: China's Political Influence Activities* (Washington, DC: Woodrow Wilson Center, 2017), https://www.wilsoncenter.org/sites/default/files/magic_weapons.pdf; Clive Hamilton, *Silent Invasion: China's Influence in Australia* (Richmond, Australia: Hardie Grant, 2018); and Peter Mattis and Alex Joske, "The Third Magic Weapon: Reforming China's United Front," *War on the Rocks*, June 24, 2019, https://warontherocks.com/2019/06/the-third-magic-weapon-reforming-chinas-united-front/.

12. Hiroyuki Akita, "China is Exporting AI-driven Authoritarianism," *Nikkei Asian Review*, June 14, 2019, https://asia.nikkei.com/Spotlight/Comment/China-is-exporting-AI-driven-authoritarianism.

Technonationalism with Chinese and American Characteristics: Implications for Third Countries; a Canadian Take

Paul Evans

University of British Columbia

This paper represents a reconstituted and updated amalgam of presentations given at the EastWest Institute's Global Cooperation in Cyberspace Progress Roundtable in Palo Alto on September 3, 2019, and at the Abe Global 2019 forum on Cyber Challenges: The Internet, Global Competition and National Security at the Hudson Institute in Washington, DC, September 5, 2019.

I greatly appreciate the opportunity to offer these remarks as part of a bicoastal American trip organized by the Abe Fellowship Program and the Social Science Research Council, intended to highlight some of the work by Abe Fellows on the general subject of cybersecurity.

My own fellowship twenty years ago, based at Harvard University and the National Institute for Research Advancement, provided a platform for fascinating research in Japan, the United States, and China on Northeast Asian security matters. It opened layers of issues and established contacts and friendships that I still value today and that have continuing relevance, including in the Canadian context.

Paul Evans (Abe Fellow 1997) has been a professor at the University of British Columbia since 1999 teaching Asian and trans-Pacific affairs. Paul is the director emeritus of the Institute of Asian Research. His academic appointments have been as assistant, associate and professor, Department of Political Science, York University, 1981-97; director, University of Toronto - York University Joint Centre for Asia Pacific Studies, 1991-96; visiting professor, Asia Center, Harvard University, 1997-99; acting director, Liu Institute for Global Issues, 2004-5; director, Institute of Asian Research, 2008-11. He has held visiting fellowships at the Australian National University (1988); National Chengchi University (1989); Chulalongkorn University (1989); the East-West Center (1995); and the National Institute for Research Advancement in Tokyo (1999). He has been a visiting professor at the University of Hong Kong in 2011 and 2013 and Singapore Management University in 2015 and 2016 as head of the International Academic Advisory Panel for its School of Social Sciences. He has directed exchange and partnership projects with numerous institutes in Asia and the Chinese Ministry of Foreign Affairs and funded by governments and foundations in Canada, Japan, the United States, China, Taiwan, South Korea, Thailand and Indonesia. He is a Canadian representative on the Expert and Eminent Persons Group of the ASEAN Regional Forum.

The cyber domain is enormous and of pressing importance in an era of warp-speed commercial and scientific progress and as a matter of individual, institutional, and national security. My aim here is to cast the net a little wider still by focusing on the matter of competitive innovation and technonationalist confrontation between two chief protagonists, the United States and China. This competition is intense and public and lies behind and beyond the trade policy conflict between the two countries that receives so much attention.

The stakes are high for the US-China relationship and worldwide. Canada is not alone in facing a series of difficult decisions about how and how far to link with Chinese partners and investors. Chinese tech giant Huawei's potential involvement in our 5G network is on the front burner, and right beside it sit a dozen other decisions on Chinese technology investment and partnerships with Chinese universities that are the subjects of intense American scrutiny and pressure.

In Canada, an additional layer of complications has been added by the arrest on an American extradition warrant of Meng Wanzhou, Huawei's chief financial officer and the daughter of its founding chairman. Ottawa has been unwittingly and unwillingly pulled into the vortex of a US-China conflict that has generated a major diplomatic crisis with Beijing. It has featured Chinese arrests of Michael Kovrig [former Canadian diplomat with International Crisis Group] and Michael Spavor [Paektu Cultural Exchange], who are widely understood to be two hostages; Chinese restrictions on particular Canadian exports; a war of words; replacement of ambassadors; and a hardening of public attitudes about China.

It is widely argued that the United States has thrown Canada under the bus of America's own confrontation with China, that Washington is now trying to tie Canada to the back of that American-driven bus in matters related to Huawei and 5G and connections with other Chinese tech companies, and that an increasing number of Canadians want to get on that bus, headed for a Cold War–like strategic confrontation with China and a decoupling from its economy.

At this fevered moment of a world untethered, I'll first define technonationalism, describe its Chinese and American variants that are now in collision, and then look through one set of third-party eyes at its implications.

The Meaning and Significance of Technonationalism

The safeguarding of technologies and information deemed essential for state security and the development of technology and information for state advantage are as old as the state system itself.

In the post-World War II era, the United States and its allies shared special concerns about protecting particular technologies and sectors, sometime successfully, sometimes not, through elaborate export controls, surveillance, and enforcement mechanisms, sometimes acting unilaterally, sometimes through multinational cooperation with likeminded states to limit the transfer of technologies and products of military and dual-use application.

The technonationalism of the current moment is a new species born on the eve of what is being described as the Fourth Industrial Revolution. Its focus is not just on sectors related to defense and dual use technologies; it is being expanded to include sectors seen as foundational to dominating activity that will shape commercial and economic competitiveness. National power in these areas thus becomes an integral part of national security.

Technonationalism is the securitization of technological development. It can now be seen as part of the battle for leadership in what are variously described as emerging, frontier, or sensitive technologies in areas that include artificial intelligence (AI), data science, advanced battery storage, robotics, advanced semiconductors, genomics and synthetic biology, 5G cellular network technology, and quantum information systems.

Neither the United States nor China is unique in making technological preeminence a national goal. They vary, however, in their historical starting points, the specific tools at their disposal, and the ideologies and institutions in which their efforts are embedded.

. . . with Chinese Characteristics

Even in the era of reform and opening, the state has remained a major player in Chinese economic policy. It has cordoned off significant areas of the economy, including telecommunications, as out of bounds for foreign involvement. Chinese leaders have understood that their country has long lagged behind the West in science and technology and that the gap was a principal reason for a century of humiliation and, more recently, China's second-tier role in the international division of labor in the global economy: as the assembler or factory for the world, but not the leader in technological innovation or the scientific research behind it or the country best able to capture the high-value-added sectors that are essential to military capacity and economic benefit.

In the last five years, the effort to identify and be a prime mover in several of these sectors has intensified. No stranger to industrial policies and major state involvement, Beijing has made major investments in research and development, advances in its higher education capabilities, especially in the STEM (science, technology, engineering, and mathematics) fields, and in efforts to attract top talent to China's universities and labs through mechanisms like the Thousand Talents program. The total investment in research and development for 2018 was about $280 billion, roughly half of the American total but a far higher percentage of national gross domestic product (GDP). National priorities and action plans were laid out in the 2014 Integrated Circuits Promotion Guidelines, the Next Generation Artificial Intelligence Plan, and, above all, the 2015 Made in China 2025 plan, intended to help China climb up global value chains, address economic weaknesses, and secure new sources of growth in the twenty-first century economy. These programs were also linked to the civil-military fusion that is a hallmark of the Chinese ecosystem for innovation. Under President Xi Jinping, science has increasingly been seen as serving the interests of the state and restricting room for more autonomous realms of a professional community or a private economy.

Five years ago, informed Americans were concerned about some elements of China's rise, including its military capacities, economic competitiveness, and foreign policy assertiveness. But there was little real concern about its capacities for technological preeminence. China could imitate, steal, and assemble, but it could not innovate. And it could not innovate because of the nature of its authoritarian political system, its comparatively weak universities and ecosystem for innovation, and its state-led economic system.

Now the analysis has been turned on its head. China is at the forefront in several sectors, including e-commerce, but, more significantly, science-based sectors,

including quantum computing; 5G research, design, and installation; and aspects of space exploration. More important, it is advancing so rapidly because of, not despite, its hybrid, state-led market economy and political system, which allow the concentration of resources and national mobilization for quicker development and application. And it is at the forefront in other ways as well, including strategic planning, government-led investments, a permissive regulatory environment, large amounts of data, and a pool of increasingly well-trained (in China and abroad) human capital.

Whether or not this hybrid mix would have worked in the private sector–driven third generation of digital technologies is debatable. But what makes technonationalism with Chinese characteristics so significant is that it appears to be especially well suited to at least the initial phases of a Fourth Industrial Revolution, where scale of investment and integrated capacities provide advantages in terms of the Internet of Things, robotics, virtual reality, and big data.

. . . with American Characteristics

It is in this context of fear of a China that can innovate that the Trump administration has embarked on a series of moves to counter what it defines as a new China threat.

It has been surprising to outsiders how fast and how deeply the consensus has developed about the need to counter China as a strategic competitor or adversary. The most visible concerns are intellectual property (IP) theft and acquisition, forced technology transfers, market-distorting subsidies, and incentives that have informed the trade war, with its arsenal of tariffs. Beyond the trade balance is a bigger agenda related to the structure of the Chinese development model and China's ecosystem for innovation and technological development.

Here the full-court press against Huawei is front and center. It has included the ban on Huawei's involvement in the rollout of America's 5G network, the ban on its products and services including research, and substantial pressure on other countries to do the same, especially in 5G.

While the United States is not unfamiliar with blending scientific and technological development with its military, and it has an intermittent history of major government involvement in mega-innovation projects driven by national security concerns—think the Manhattan Project and the space programs—it is in unfamiliar territory when facing a major peer competitor that, in scale and structure, has several core advantages, and with which it is so economically intertwined.

The distinctive element of technonationalism with Trumpian characteristics is that it responds to the China challenge via tariffs and a growing array of restrictions on successful Chinese enterprises and shows at least initial signs of attempting to decouple from China in trade and technology matters. The number of Chinese companies on the proscribed Entity List has gone well beyond Huawei to include twenty-eight additional companies in the information technology (IT) sector and AI startups. The rationale is these companies have taken actions contrary to the national security or foreign policy interests of the United States, ostensibly related to their involvement in Beijing's activities in Xinjiang. This comes at a time when the pace of innovation and technological disruption is accelerating rapidly, and the production of ideas and core equipment is deeply embedded in complex supply chains linked to global markets.

In dealing with China, and with other countries—including Canada—trade and technology moves may have protectionist objectives, but they are defended on the basis of protecting national security. It is difficult to know if US actions are part of a concerted strategic plan to isolate China and decouple the two economies or if the moves are largely tactical in putting additional pressure on China in the trade negotiations. But it is clear that technonationalism, American-style, is largely defensive at the moment rather than based on a national strategy for making the United States more competitive in these areas. In the words of a recent Council on Foreign Relations (CFR) report, the United States is "lagging behind." Without a national security innovation strategy, it "risks losing the economic and national security benefits it has enjoyed over its decades of technological leadership and investment."[1]

Third Country Implications: Canada

The immediate and longer-term impacts of the clash are enormous for China and the United States. But they have huge implications for other countries, too—Canada included—caught in a firefight not of their making.

Canada has already been the target of Section 302 tariffs on steel and aluminum exports on the grounds that it is a threat to US national security. There has been major pressure to follow suit with Washington's ban on Huawei in the 5G and other domains. Washington has also weighed in heavily in opposition to Chinese investments in construction companies deemed to constitute critical infrastructure.

Less visible but very real are extraterritorial spillovers. It is easy to make the case that the extradition warrant for Meng Wanzhou was precipitated by the American battle against Huawei, related in part to its violation of American sanctions against

Iran that Canada itself does not support. Canadian universities face a difficult choice between expanded research cooperation with Huawei that they value (for the money, for Huawei's flexibility and responsiveness, and based on the calculation that the basic and applied science behind Huawei's technology is world class) and continuing to work with American institutions that, by federal regulation, are unable to work with partners that collaborate with Huawei. Export control restrictions on goods and services to China are also becoming wider and deeper, with special relevance to dual-use possibilities, which in areas like AI are almost infinite.

Despite hardening public views against China in light of the current crisis around Meng and the two Michaels, most policymakers in Canada are still reluctant to sign onto the framing of China as a strategic adversary or enemy and favor a mixed view of China as competitor, occasional threat, and necessary partner in advancing Canadian national interests and making progress on key global issues, including climate change. And while Canadians are increasingly aware of the risks of intellectual property loss and both legal and illegal IP transfer, and while they harbor deep concerns about internal developments in China and in its foreign relations, they have little enthusiasm for decoupling or undermining bilateral links built over decades in trade, investment, education, and many other areas.

Let me end with three sets of questions that are of most concern to policymakers and analysts in Canada about how to interpret and react to this new phase of American policy toward China.

First, how much wider and deeper is the Trump administration likely to go in decoupling from China? How far are the measures employed against Huawei and other IT leaders in China likely to be applied in other fields defined as advanced, frontier, or sensitive sectors? In the framing of China as a whole-of-society threat, what further restrictions on visa issuance, student recruitment and exchanges, joint research, IP protection, and faculty vetting will be rolled out?

Second, how deep and durable is the current consensus in Washington about framing China as a strategic adversary? On a related note, even if this is a long-term disposition, are the tactics and tools of the Trump administration and the move toward technological decoupling likely to be replicated by a future administration? Academic institutions in the United States are already chafing at restrictions, especially in the STEM areas and medicine. Think tanks are raising questions about the administration's tactics and strategic rationale.

Third, what are the prospects for a revised American strategy that will take a more nuanced position on where and how to compete with China rather than against it? Is there anything we can do to collaborate with likeminded Americans in encouraging more active federal roles in expanding domestic capacities, in working with the

likeminded on deeper collaboration on research, in protecting existing multinational efforts at defining standards and integrated supply chains, and in collaborating on international standards and joint projects that also include China, especially as they relate to pressing global problems like climate change?

Our discussions here in the United States reinforce the conviction that technonationalism need not and should not be a zero-sum game. The CFR's recent report gives a sound rationale and some very positive suggestions for a positive approach.

Techno-internationalism is also a possibility.

NOTES

1. James Manyika, William McRaven, and Adam Segal, "Innovation and National Security: Keeping Our Edge," Council on Foreign Relations, Independent Task Force Report No. 77, September 2019, https://www.cfr.org/report/keeping-our-edge/pdf/TFR_Innovation_Strategy.pdf.

Protect the Internet Core: A Case of Undersea Cables

Motohiro Tsuchiya

Keio University

Presented as a "lightning talk" at the EastWest Institute's Global Cooperation in Cyberspace Progress Roundtable in Palo Alto, CA, on September 3, 2019

In the late 1940s, Nobert Wiener coined the term "cybernetics" to describe the connection of the space for exchange of information with the structures in physical space that facilitate those exchanges. Today we often imagine the Internet as something like a cloud, and in recent years digital cloud services have become increasingly popular. Cyberspace is not something that actually floats in the sky, however, but is, rather, firmly planted in physical spaces. Google's cloud services, for example, are provided by a large collection of servers in its data centers.

The importance of this physical space came home to me several years ago when I took a sabbatical leave from my university and spent a year in Hawaii. As I walked on a street in Oahu, I noticed a manhole cover on the ground (figure 1). When the cover was removed, I could see the network cables for controlling traffic signals (figure 2). While I do not know whether these cables were connected to the Internet, they were undoubtedly using cyber technologies.

Figure 1. Manhole for Traffic Signal Cables (photo by author)

Motohiro Tsuchiya (2000 Abe Fellow) is a professor at the Graduate School of Media and Governance at Keio University, and deputy director of the Keio Global Research Institute (KGRI). Prior to joining the Keio faculty, he was an associate professor at the Center for Global Communications (GLOCOM), International University of Japan. In 2001 and 2002 he conducted research in Washington, DC, as a visiting scholar at the Center for International Development and Conflict Management (CIDCM), University of Maryland, and at the Cyberspace Policy Institute (CPI), George Washington University. From March 2008 to March 2009 he was a visiting scholar at the MIT Center for International Studies. He served as an expert member of the Information Security Policy Council (ISPC) of the Japanese government from 2009 to 2013. From March 2014 to February 2015 he was visiting scholar at East-West Center. He earned his BA in political science, MA in international relations, and PhD in media and governance from Keio University.

Figure 2. Manhole with Cover Removed (photo by author)

Figure 3. A Box on a Street (photo by author)

found a gray metal box on a roadside, as well (figure 3), with a cyber system inside it that also controlled traffic lights. Both of these everyday experiences were a reminder of how dependent we are on cyber systems in our daily lives. In addition to going online every day, we use many other cyber systems we do not think of as part of the Internet but are based on similar technologies. As cyberspace has expanded, it has become intimately connected to a vast array of activities on which our social systems depend. In thinking about cyberspace and its vulnerabilities, we should remember it is not just a "cloud"; it is firmly planted in a very physical infrastructure.

Let me turn now to Japan. There are tunnels under Tokyo streets, many of which were built by a public telephone company several decades ago. An infinite number of cables run through the tunnels and function as the nerve system of Tokyo. Someone who wanted to disrupt the communication networks of Tokyo would find it easier to cut those cables than to send malware to thousands of computers.

The cyber links, of course, not only serve the public infrastructure. When I want to use a fiber optic service at home, a communications provider installs a cable that will link my computers to the Internet. If someone wanted to disrupt my communications for a few days, cutting that cable would be the easiest way. What is true for my home computers is also true for the whole Japanese nation. Japan is an island country, and its links to the global Internet depend on undersea cables. Ninety-nine percent of Japan's international communications traffic goes through undersea cables. The remaining 1 percent goes through artificial satellites. While satellites seem to represent cutting edge technology, communications through them are actually slower and more expensive than by undersea cable. Geostationary orbit satellites float 36,000 kilometers above the earth, and it takes some time for messages to go up and down. Moreover, the bandwidth of satellites is narrower than that of undersea cables.

Let us consider for a moment the vulnerability of the vast world of undersea cables. Would it be possible to cut cables deliberately? History tells us it is. Right after the outbreak of World War I, the British cut German cables to manipulate German communications routes. We have, of course, many more undersea cables today, and the threat of physical attacks on them is very real. Recently, Admiral James Stavridis wrote a piece entitled, "China's Next Naval Target Is the Internet's Underwater Cables," in which he warned of a possible attack on undersea cables in the near future.

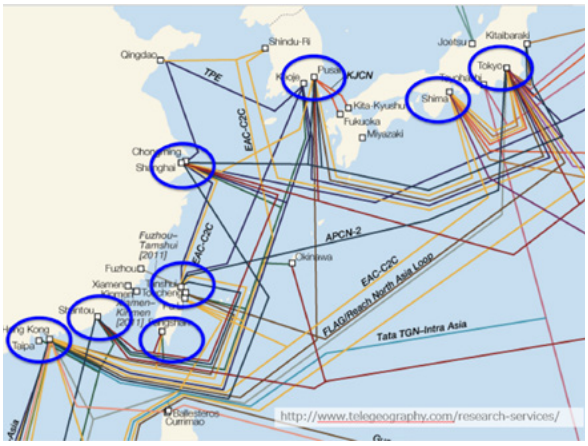


Figure 4. Map of Undersea Cables and Landing Stations

As we can see from a map of undersea cables (figure 4), the area around East Asia is one of the most crowded spots in the world. Attacks on these cables would affect all of the economies in the region. Cutting them by hand would be very dangerous, however, since high voltage electricity runs through today's fiber optic cables. Machines such as unmanned underwater vehicles (UUVs) would be needed to cut those at the bottom of the sea.

The cables could be attacked in another way, though, that would make them an easier target. At the beginning of this brief talk, I showed you pictures of manholes and the cables inside. Many undersea cables can also be reached through manholes for maintenance, often located on beaches near where the cables enter landing stations. An attacker would not need to go to the bottom of the sea to cut these cables.

Figure 5. Landing Station (photos by author)

The location of undersea cables is known from open sources, and each country has cable landing stations (figure 5) in a few concentrated locations. Facilities for cable landing stations are usually owned by private companies. They can be part of critical infrastructure, but it is difficult for military forces to guard them in peacetime.

The Global Commission on the Stability of Cyberspace (GCSC) has published a norm to protect the Internet core, and undersea cables are an important part of that core.

So, to summarize my argument: Cyberspace is not something floating in the sky. It is an aggregation of physical communication devices, communication channels, and data storage facilities. When we think of cybersecurity, we should consider not just conventional cyberattacks through hacking and other such activities, but also the protection of the physical facilities that make up the "cloud" and the fibers linking the systems. In this short talk, I will take up three major issues: first, how the

---

Cyber Challenges: Perspectives from Japan

Presented at Abe Global 2019 |Washington, DC, on September 5, 2019

Japanese people perceive cybersecurity; second, our worries about cybersecurity during the [now-postponed] 2020 Olympics, which will be held in Tokyo; and, third, what we have been doing to try to strengthen cybersecurity.

The data for the first two issues—how the Japanese people perceive cybersecurity and our worries about cybersecurity during the Olympics—come from the *Nihon Keizai Shimbun (Nikkei)*, one of Japan's leading national newspapers. Figure 1 shows the results of a search of *Nikkei* on the term "cyberattacks."

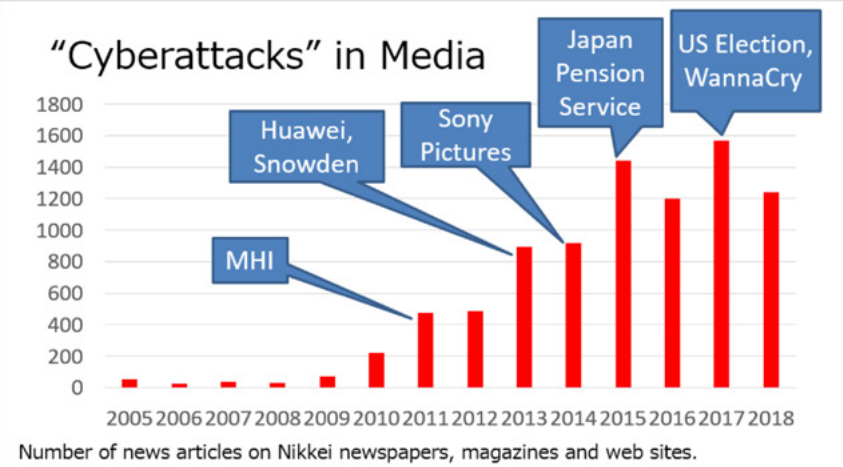


Figure 1. Articles Containing "Cyberattack" in Nihon Keizai Shimbun

As the figure shows, the first incident that gained significant attention in Japan was a hack of Mitsubishi Heavy Industries (MHI), the biggest military contractor in Japan, in 2011. The next major discussion of cybersecurity had to do with questions about security risks associated with the Chinese firm, Huawei, which gained attention in 2013 amid rising tensions between the United States and China. Edward Snowden's revelations based on top-secret documents from the US National Security Agency (NSA) was also a popular topic that year.

In November 2014, Sony Pictures Entertainment (SPE) was hacked, and its business was disrupted. Although SPE is an American company, the Sony brand began in Japan, and the Japanese nation closely followed the news. In 2015, the Japan Pension Service (JPS), an independent administrative corporation, lost about 12.5 million pension records as a result of hacking. As Japan is an aging society, this incident created great worries about the safety of the pension system and became a major political scandal. Finally, Russian interference in the US presidential election in November 2016 was widely reported in Japan. At about the same time, there were reports about WannaCry, one of the worst ransomware attacks; although there was little damage to Japanese firms or organizations, the attack was widely discussed.

Figure 2 shows which countries were considered responsible for each cyberattack. In the early years, China was usually mentioned as the most likely suspect, but Russia caught up after the 2016 US presidential election.

Figure 2. Articles Related to "Cyberattack" and Specific Countries in Nihon Keizai Shimbun

Figure 3 shows the number of "cyberattack" articles mentioning the Olympic games and elections, respectively. In 2013, when Tokyo was selected to host the 2020 Olympics, few articles discussed potential cyberattacks, but the number began to increase the following year. I should note that the lineup for future Olympic games after Tokyo includes Summer Olympics to be held in Paris in 2024 and Los Angeles in 2028. Soon these cities will also share our concerns about cyberattacks on Olympic games. As for the other chief target, that is, cybersecurity concerns around elections, figure 3 shows that articles increased in number after the 2016 US presidential election. In Japan, discussions are currently ongoing about changing the constitution; if the Diet votes to do so, the final stage of the approval process calls for a national referendum. In this event, concerns will arise about the security of the elections, along with fears of outside interference.

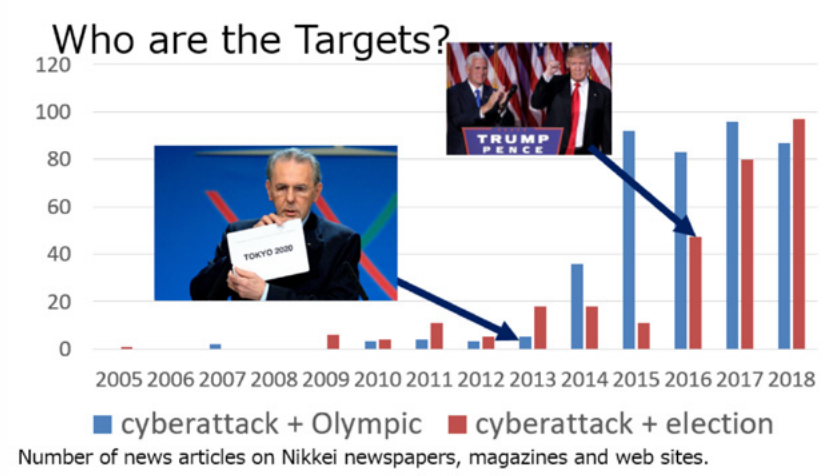


Figure 3. Articles Related to "Cyberattack," Olympic Games, and Elections in the Nihon Keizai Shimbun

Finally, Japan has lately been trying to strengthen cybersecurity. With less than a year [at the time of this writing] until the opening of the 2020 Summer Olympics in Tokyo, the government has secured a budget of US$260 million to protect the games from cyberattacks, both offline and online. Many cyber-related risks will be present during the games:

- Fake tickets
- Too many/too few hotel reservations
- Traffic disorder
- Blackouts
- Malfunction of timing, measuring, and display equipment

- Malfunction of websites and message systems
- Disruption of TV/net streaming
- Disruption of communications networks
- Stealing of personal data
- Confusion of financial markets
- Accidents at nuclear power plants
- Loss of police, defense, and government functions

In August 2018, the prime minister's office held the first meeting of the Council on Security and Defense Capabilities, leading in December 2018 to new National Defense Program Guidelines (NDPG). The key concept in the new guidelines is the creation of a Multidomain Defense Force covering land, sea, air, space, cyberspace, and electromagnetic space. With regard to cybersecurity, the guidelines state that Japan will "fundamentally strengthen cyber defense capabilities, including the capability to disrupt, during attacks against Japan, the opponent's use of cyberspace for the attack." Under the peace constitution, Japan Self-Defense Forces' Cyber Defense Unit (SDF) had focused only on defense, but the new guidelines include a change in policy to allow a "counterstrike." This is a step forward for better cybersecurity.

To carry out a counterstrike, however, we must be able to attribute the attack accurately—to identify who is attacking Japan. Therefore, the NDPG says, "SDF will leverage its capabilities in all domains to conduct wide-area, persistent intelligence, surveillance, and reconnaissance activities around Japan."

James R. Clapper, the Director of National Intelligence (DNI) for the Barack Obama administration, wrote in his memoir, *Facts and Fears*, "At the Pentagon I'd often heard the military truism that every nation is preparing to refight its last war." Japan's last war was World War II. There were no cyberattacks at that time. In thinking about the future, Japan must prepare for a very new security situation.

In conclusion, first, Japan and the United States share cyber concerns with regard to possible attacks during the Olympic Games, as well as worries about election interference. The Japan-US alliance should be strengthened in the area of cybersecurity, in addition to addressing conventional security concerns. Second, Japan has decided to create a Multidomain Defense Force based on the NDPG. This means joint operations are expected among Japan's Ground Self-Defense Force, Maritime Self-Defense Force, Air Self-Defense Force, and new joint forces. This will bring big organizational and operational changes to the forces. Finally, Japan is strengthening cyber capabilities in many ways. Cyber counterstrike capabilities should be based on strengthened capabilities to attribute attacks accurately. Persistent intelligence, surveillance, and reconnaissance activities in cyberspace should be pursued in a timely manner.

Discussion and Q&A

Moderated by:
Thomas Duesterberg

Hudson Institute

Thomas Duesterberg: I'm going to start off with a very general question, and then we will turn to the audience, so please get your questions ready. One of the themes that came up in each of the presentations was the need for international cooperation in setting the rules for this new world of information security 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 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 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, likeminded nations?

Motohiro Tsuchiya: I'm trying to organize a CJK—China, Japan, and South Korea—track two dialogue; we will have the first round this year. I'm trying to persuade everyone to have this kind of agreement in the final stages of the dialogue, but we cannot agree. And this is a track two discussion in just three countries. It's quite difficult. I think you are familiar with the UN GGE [United Nations Group of Governmental Experts] framework. I think twenty, twenty-five countries are arguing about how to organize global governance of cyberspace. It's quite difficult, so we

---

Thomas J. Duesterberg is a senior fellow at Hudson Institute. An expert of trade, manufacturing, economics, and foreign policy, Dr. Duesterberg leads project work on trade with Europe and China, reform of the World Trade Organization (WTO), global competition in advanced technologies such as 5G, and the strength of the US manufacturing sector. Previously, Dr. Duesterberg was executive director of the Manufacturing and Society in the 21st Century Program at the Aspen Institute. From 1999 to 2011 he served as president and CEO of the Manufacturers Alliance/MAPI, an economic research and executive education organization based in Virginia. He co-wrote *US Manufacturing: The Engine of Growth in a Global Economy* and three other books, and is the author of over 200 articles in journals and major newspapers. He is a graduate of Princeton University (BA) and Indiana University (MA, PhD).

are divided. And China and Russia are trying to divide the Internet itself. They are warning about US intervention into their systems, so they are trying to set up a Chinese Internet or Russian Internet. We may face a divided Internet in the future.

Well, one positive thing is that cyberspace is organized by geeks. It's a kind of republic of geeks, and they are talking to each other. They are trying to maintain the real, physical space of the Internet. For example, one of my students is working for JPCERT (Japan CERT). CERT is a computer emergency response team, and they find it easy to talk to their counterparts all over the world—CNCERT (China CERT) or KN-CERT (Korea CERT). If we find something wrong in a server in Japan—for example, it's receiving DDoS [distributed denial of service] attacks—and we determine that the command and control site might be in China, JPCERT makes a phone call to CNCERT. Hey, we are getting DDoS attacks from China. Could you stop that site? This works. Geeks can talk to each very easily. But political leaders—very difficult, even academics.

Duesterberg: OK, would anybody else like to dive in on that?

Dorothea LaChon Abraham: I just want to say, to focus on all of those areas, I don't think anything's going to get accomplished anytime 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 [International Organization for Standardization] or the ones that have been established that are developing standards for cyber asset creation and for mitigation techniques, those that are risk management oriented? 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, to get that community of geeks online, as well as with our international standards organizations, to come up with cataloguing 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?

Paul Evans: 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 studying—to consider 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 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 the problem—these are "wicked problems," in terms of their technological complexity, but also the politics. But I would say, Tom, I think one of the issues, when we discuss this matter with our American friends, is we are going to need different kinds of venues for this discussion. Sometimes it's among the likeminded,

the friendly states, Five Eyes groups. Sometimes it's going to be among those who are not likeminded. And bringing in the non-likeminded in is becoming increasingly complicated.

That's partly the China story, if I can be direct. But it's a US story as well, and about how far the United States would like to work toward collaborative solutions on these problems that run across the likeminded and the non-likeminded, 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.

Patrick 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 [Chinese Communist Party]. In the United States, on the other hand, the national security strategy—the defense strategy—that was issued 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 on well after this panel, we have diminished power. We recognize that. And, so, clearly, there are going to be compromises. This is a bounded competition with China. And this is a huge area of

governance, a gap that we have. For the same reason, I argue that information is so key to the twenty-first century, the governance challenge is huge. It's going to take a long time. It will take multiple different attempts. Accountability and transparency are going to be very important to this likeminded group trying to hold up a high standard for where we want to go with this.

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

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

Evans: The meeting we just attended with the EastWest 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 was being advocated by . . . a cross-partisan group, both Republican and Democratic, involving some people in your administration now, [considering] 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 the United States is a country that has not been averse to government leadership in key areas—the Manhattan Project, space projects. It's not the way the Chinese do it. But how the United States can play a lead in using private sector forces—that's something many of our countries would like to work with.

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 twenty-first century, it will be largely private sector driven. And so we have to figure out how to unleash that, catalyze that. 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: Okay. Well, let's turn to the audience. I'm sure there are many questions.

Hiro Matsura: Thank you. I am Hiro Matsura from Japan, and I'm just visiting for the summertime. I have a question for Professor Abraham. I think your theme has been interesting. You tried to assess the capabilities and the problems of three countries—Japan, the United States, and Britain—and tried to focus on the need for

trilateral cooperation But I wanted to re-understand your rationale, why you may focus on this particular possibility of trilateral cooperation. Why did you put priority on this particular trilateral cooperation? Considering Japan's cyber capability and the work toward government centralization in this field, Japan may be lagging behind more than ten years.

Well, the Japanese government is very good at documentation for national cybersecurity. But, as you have already mentioned, the United States and United Kingdom have a long history [together] and the legacy of the Second World War. And they have a very close collaborative relationship in intelligence, as core members of the Five Eyes. But Japan is not a core member of this Five Eyes. So, given that, why do you put priority on a possible trilateral cooperation?

Abraham: The primary reason is because, even though we don't have a direct defense relationship like the United States and Japan do for the Asia-Pacific region, Japanese companies actually provide the industrial base for the Defense Information Infrastructure for the UK. So that's one component. And when that attack happened last June, by a Russian actor who was going after US IP [intellectual property], it did so through Japanese networks because of the particular vendor--a primary vendor for the UK and the United States. They share networks. They share information. And so there's a trilateral relationship with these vendors that could expose vulnerabilities of all three countries if they don't have the same capabilities and security measures in place.

That was a case that really kind of made apparent these extenuating circumstances and linkages that we may not see readily among the countries but are exacerbated when you have a cyberattack. So that was my rationale for going with those three. And then, also, the United States and UK—as you noted and we've talked about—have an extensive intelligence capacity or assessment capacity, something that can be leveraged by Japan, which does not have the capabilities currently to absorb the amount of information to do the assessment. And the United States and UK 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: Okay, who else?

Tsuchiya: Very quickly—so, if you put the United States at the center, who is a partner on the Atlantic side? It's the UK. No explanation. But who is a partner on the Pacific side? You may be looking at Singapore, South Korea, or other countries. But Japan could be one of the best partners. And, so, the UK is approaching Japan these days. Some two years ago, Prime Minister [Theresa] May came to Japan. And she said the United Kingdom would help Japanese cybersecurity because they had Olympic Games in London in 2012, and they are helping us so much. The UK and

Japan are getting closer these days. So, what we can do? We can contain erasure in a geopolitical sense. China is there. Russia is there. North Korea is there. Iran is there. We can contain those countries with the partnerships.

Abraham: This relationship actually has extended, with the maritime connections among the UK, the United States, and Japan and the Asia-Pacific region being that channel. From the need to secure maritime operations, we have connected networks that are sharing information among the three countries that need to have cybersecurity, as well. It's very critical for these three countries to have comparable capabilities.

Liz Kim: My name's Liz Kim. 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 its heist of cryptocurrency these days. And I was also wondering if you believe North Korea's denial of the heist.

Cronin: Well, maybe North Korea didn't make $2 billion off the cryptocurrency heist, but it made a lot of money. And I think the point is we need to keep following just how quickly North Korea adapts to new technologies, especially in cyberspace, as well as the work around sanctions. The more pressure we can agree to exert with sanctions, [the better]; you can be sure North Korea is not stopping. They're just finding a different path to raise money through a largely illicit economy. So this is a serious problem. They've got 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.

Richard Coleman: Hi. I'm Richard Coleman. 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 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 the four experts [today] have told us about cyberattacks. With the coming election in the United States, is there anything that can be done to protect our elections at the state level? Now, their stuff, presumably, is four years old—their software and whatever protection [they have]. With the state of the art of ransomware, which has already scored big hits in the United States, is there anything after the fact 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 not just with Russia, but also China now, and their electronic interference and broader interference in our election next year. They're doing very good bipartisan work. Their recommendations are thoughtful and deserve to be looked at. And they're online.

Dave Rabinowitz: All right. Thank you. I'm Dave Rabinowitz. 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 take that one on?

Abraham: They're out preparing technical solutions and don't have—no, but you're right. You're right. I was at a conference for Sans. Are you familiar with Sans? It's a credentialing organization, probably the 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 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, 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 who don't allow certain technologies to be implemented. We have also just an 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 China produces and uses domestically, it's gone through audit for cyber. It builds to the cyber specifications that are 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—to change this culture, then maybe we can also, you know, improve not only cybersecurity but to boost or raise their capacity to inform our policy, as well. But if you have an administration who, you know, fires its own CISO [chief information security officer] and subjugates the cybersecurity personnel that have the relevant acumen, then how can we raise that to the level of importance 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 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 who matter are tied into real organizations and used one way or another. Second, Chinese geeks I have met are not identical to my California geek friends, in that they feel their responsibilities are to the state and as actors to serve the state. And, on occasion, when I've had the unfortunate opportunity 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: Jun Murai, he's my boss at the graduate school. He's called the father of the Japanese Internet. He imported Internet technology into Japan. And he and I shared membership on a government council maybe seven years ago. And we were always arguing in the council. I said, "This is a council for thinking about national security, for cybersecurity." But he always said, "The Internet is global; it's not national. We have to connect the Internet beyond borders." The mindsets are

very, very different. And my first experience in the geek community was in 2002, while I was an Abe Fellow. I went to Utah. I went for an IETF [Internet Engineering Task Force] meeting in February. It was very cold outside, with a lot of snow. But they were wearing short pants and ponytails and T-shirts with logos and something geeky. And they were sitting on the ground in a very fancy hotel, and they were typing. Their mindsets are very, very different. Washington people don't understand what they are thinking, actually.

We have to try to understand each other.

Closing Remarks

Ronald Kassimir

Social Science Research Council

It's never a good thing to stand between a great panel and a reception, so I will try to be brief and mostly give a few thank yous. Really, deep appreciation to the panelists, both our Abe Fellows and Patrick, for a really stimulating discussion that I hope we will continue in a more informal way during the reception. I'd also like to thank President Weinstein and his colleagues here at Hudson Institute, not only for being 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 spanning twenty-eight years with the Abe Fellowship Program—with four hundred fellows supported over that time and counting—and also for developing the Abe Fellows Global Forum, which has brought us this event. Abe Global has been a really great way to bring the knowledge that's being produced by the fellows to a wider audience, beyond the academy and beyond their own fields and institutions, and it is a really exciting innovation in the Abe program. Thank you all for being such great contributors to it.

Ronald Kassimir is vice president of programs at the Social Science Research Council, providing strategic planning for and fostering coherence across the Council's programs while also supporting the development of new program initiatives. He also provides leadership for the Religion and the Public Sphere program, works closely on the Council's Africa-focused activities, and is managing editor of the SSRC's digital forum *Items*. From 1996 to 2005, Kassimir was first a program officer and then a program director at the Council, where he managed the Africa Program and, from 2000 to 2005, the International Dissertation Field Research Fellowship Program. In 2005, Kassimir became associate dean at the New School for Social Research and associate professor in the Department of Politics, and in 2007 he moved to the New School's Office of the Provost, where he worked for six years as associate provost for research and special projects. From 2011 to 2013, he cochaired the university committee that produced an institutional self-study as part of the New School's reaccreditation process. He returned to the Council in 2013 as senior adviser, and then executive program director. Kassimir earned a PhD in political science from the University of Chicago in 1996. He has published on religion, civil society, higher education, and globalization in Africa, as well as on youth activism and civic engagement. He is coeditor of *Intervention and Transnationalism in Africa: Global-Local Networks of Power* (Cambridge University Press, 2001), *Youth Activism: An International Encyclopedia* (Greenwood Publishing, 2005), and *Youth, Globalization, and the Law* (Stanford University Press, 2007).

For those of you who don't know much about the SSRC, we're now a ninety-six-year-old private nonprofit foundation. Our centenary is coming up, so we're starting to think about that. Over all that time, we have, as our major mission, promoted social science research using a range of mechanisms—through 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. Perhaps most broadly, we build bridges within the research community and between it and policymakers, the media, and the philanthropic world. If anyone's interested to hear more about the SSRC, we can talk at the reception.

Just before I conclude, I do want to mention two things we're doing at the Council that have been touched on—some in very direct, some in indirect ways—in 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 have 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 and convenes scholars to look at how media—all forms of media—shape and affect 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. I think this will be a really great resource to give scholars, and also practitioners who are interested in these issues, access to the latest debates and the latest findings on the impact of disinformation.

I'd be happy to connect any of you to my colleagues who are working on those programs.

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 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.

ABE GLOBAL | 安倍 ABE FELLOWSHIP PROGRAM

September 5, 2019 | 3:00 PM - 6:00 PM
Stern Policy Center, Hudson Institute

Abe Global | WASHINGTON, DC

Welcome Remarks

Kenneth Weinstein
Hudson Institute

Junichi Chano
Japan Foundation Center for Global Partnership

Panel Discussion and Q&A

Moderator: Thomas Duesterberg
Hudson Institute

Dorothea LaChon Abraham
William and Mary | 2017 Fellow

Patrick Cronin
Hudson Institute

Paul Evans
University of British Columbia | 1997 Fellow

Motohiro Tsuchiya
Keio University | 2000 Fellow

Closing Remarks

Ronald Kassimir
Social Science Research Council

HUDSON INSTITUTE

Founded in 1961 by strategist Herman Kahn, Hudson Institute challenges conventional thinking and helps manage strategic transitions to the future through interdisciplinary studies in defense, international relations, economics, health care, technology, culture, and law.

Hudson guides public policy makers and global leaders in government and business through a vigorous program of publications, conferences, policy briefings, and recommendations.

THE JAPAN FOUNDATION CENTER FOR GLOBAL PARTNERSHIP

The Center for Global Partnership (CGP) was established within the Japan Foundation in April 1991 with offices in both Tokyo and New York. CGP is dedicated to strengthening the global US-Japan partnership and cultivating the next generation of public intellectuals necessary to sustain this partnership.

To carry out its mission, CGP supports an array of institutions and individuals, including nonprofit organizations, universities, policymakers, scholars and educators, through grant programs, fellowships as well as self-initiated projects. CGP's activities fall into the two following categories: policy-oriented Intellectual Exchange, and community-based Grassroots Exchange & Education.

THE SOCIAL SCIENCE RESEARCH COUNCIL

The Social Science Research Council (SSRC) is an independent, international, nonprofit organization founded in 1923. It fosters innovative research, nurtures new generations of social scientists, deepens how inquiry is practiced within and across disciplines, and mobilizes necessary knowledge on important public issues.

The SSRC is guided by the belief that justice, prosperity, and democracy all require better understanding of complex social, cultural, economic, and political processes. We work with practitioners, policymakers, and academic researchers in the social sciences, related professions, and the humanities and natural sciences. We build interdisciplinary and international networks, working with partners around the world to link research to practice and policy, strengthen individual and institutional capacities for learning, and enhance public access to information.