グローバルな文脈での日本

REEXAMINING JAPAN IN GLOBAL CONTEXT

Suntory Foundation Research Project

FORUM REPORT 020

# Cybersecurity, Cyber Governance

Reexaming Japan in Global Context Forum, Tokyo, Japan, October 13, 2022

## The Cyber Great Game: International Politics Transformed by Digital Technologies

Motohiro Tsuchiya

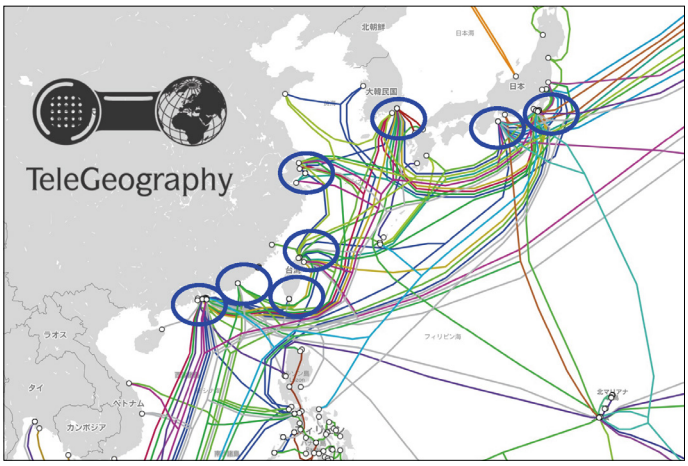
*Keio University Graduate School of Media and Governance, Tokyo, Japan*

On October 13, 2022, members of the *Reexamining Japan in Global Context* project met in Tokyo to discuss cybersecurity and cyber governance. The first presentation was by Professor Motohiro Tsuchiya of Keio University.

Professor Tsuchiya began by drawing an analogy between the "Great Game" played by 19th- and early 20th-century Great Powers (primarily Russia and Great Britain) for influence over Afghanistan and the current competition between Great Powers (primarily Russia, China, and the United States) for dominance in cyberspace. The first was essentially a geopolitical struggle for control of physical territory that took place in what Nicholas Spykman called the "rimland," or territories peripheral to what Halford Mackinder had earlier called the Eurasian "heartland." The second, in contrast, is famously said not to be spatial at all. People commonly say that cyberspace is "borderless"; data can travel all over the world. This would seem to suggest that geopolitics is an inapt lens through which to analyze the Cyber Great Game. But is this really the case?

Two considerations suggest that the Cyber Great Game is indeed profoundly geopolitical. The first consideration even hints at a spatial dimension: the United States regularly accuses four countries of cyberattacks—Russia, China, North Korea, and Iran. Russia is in the heartland; China, North Korea, and Iran are all in the rimland. The areas of both instability and competition in the 19th and early 20th centuries are also areas of instability and competition today.

Second, the cyber domain has clearly become another field of geopolitical struggle. We know that Russia under Vladimir Putin, for example, has sought to weaken key geopolitical rivals such as the United States by sowing division, discord, and confusion at home, undermining liberal democracies by interfering with their domestic politics. So also have threat actors such as Iran. By means of such things as fake social media accounts, manipulated videos, bots, and targeted email campaigns, these countries have attempted to promote conspiracy theories, aggravate partisan divisions, and influence the outcomes of elections. Russian hackers, for example, infiltrated both government and Democratic Party information systems to steal data, plant malware, and disrupt operations. Iranian hackers have promoted extremist groups such as The Proud Boys. In response, in 2017, the U.S. Department of Homeland Security designated as "critical infrastructure" information systems vital to free, fair, and reliable elections. Similarly, in 2018 the U.S. Department of Defense adopted a "Defend Forward" cyber strategy intended "to disrupt or halt malicious cyber activity at its source, including activity that falls below the level of armed conflict." A U.S. Cyber Command operation, for example, disrupted the Internet access of a Russian troll factory on the day of the 2018 U.S. midterm elections. On a daily basis, the United States proactively scours information systems on





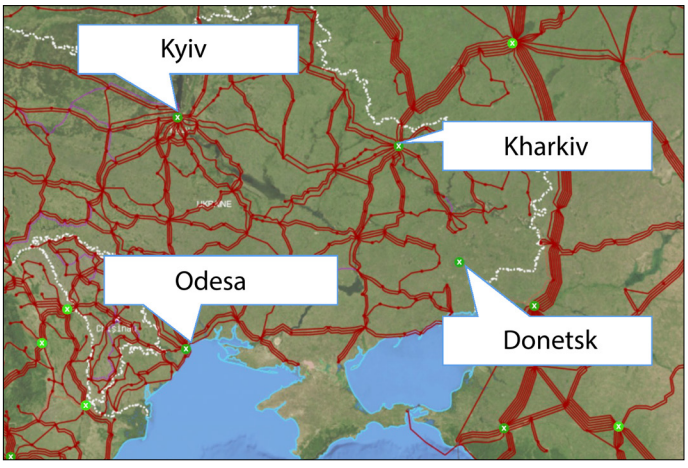
foreign soil for signs of impending cyberattack, demonstrating that cyberspace is far from truly borderless.

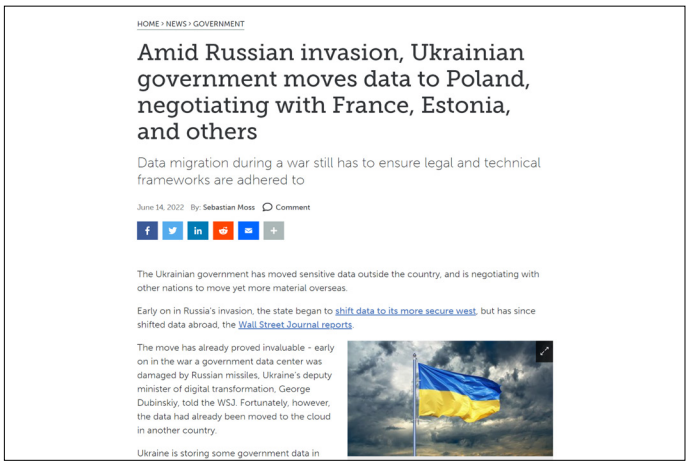
As a result of American efforts, the 2020 federal election was "America's most secure election in history," according to Christopher Krebs, the first director of the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA), Nevertheless, President Donald Trump insisted that the presidential election was stolen and on December 6, 2021, his supporters marched on the U.S. Capitol in an attempt to prevent the certification of the legitimate winner, Joe Biden, demonstrating that combatting foreign interference in democratic politics is more than a simple hardware and software issue: it requires preventing the organic spread of false information and false narratives.

Cyberspace has clearly now become a fifth operational military domain in addition to land, sea, air, and space. Cyberspace has a physical presence as well, however. Satellites in space, servers storing data in "the cloud," and cables, switches, and junction boxes connecting homes, businesses, and offices are all physical parts of cyberspace. Among the most important elements of the physical infrastructure of cyberspace are fibre-optic submarine cables. As much as 99 percent of Japan's international Internet traffic travels through submarine cables, for example. In principle, if the locations of these cables can be found, they can easily be cut. Many countries also have a small number of locations where submarine cables come ashore. In Japan, for example, most come ashore in Chiba and Ise Shima. It is even common for cable landing sites to be visibly marked. If the general public can find these points of vulnerability easily, so also can terrorists and other foreign threat actors.

The ability to combine cyber operations with physical operations targeting information systems is an important national power resource in the modern age, as the 2014 Russian occupation and annexation of Crimea clearly showed. In one swift operation, Russia was able to seize control of Crimea, cut it off from the rest of Ukraine, and score a fait accompli before any effective response or defence could be mounted. One of the great mysteries of Putin's recent invasion of the rest of Ukraine is how little effort Russia made to implement the same playbook. The operation was conducted almost entirely in a traditional military manner, with disastrous results. Importantly, Ukraine's Internet infrastructure remained largely intact and functioned normally. This was thanks primarily to proactive Internet infrastructure hardening and other security measures taken by Ukrainian Internet authorities in response to the lessons of Crimea. In this, Ukraine has benefited enormously also from Western assistance, not least from U.S. Cyber Command.

What does this all mean for Japan? In March 2018, Prime Minister Shinzo Abe made a speech at the National Defense Academy in which he said that nowadays having an advan-



HOME › NEWS › GOVERNMENT

Amid Russian invasion, Ukrainian government moves data to Poland, negotiating with France, Estonia, and others

Data migration during a war still has to ensure legal and technical frameworks are adhered to

June 14, 2022 By: Sebastian Moss Comment

The Ukrainian government has moved sensitive data outside the country, and is negotiating with other nations to move yet more material overseas.

Early on in Russia's invasion, the state began to shift data to its more secure west, but has since shifted data abroad, the Wall Street Journal reports.

The move has already proved invaluable - early on in the war a government data center was damaged by Russian missiles, Ukraine's deputy minister of digital transformation, George Dubinskiy, told the WSJ. Fortunately, however, the data had already been moved to the cloud in another country.

Ukraine is storing some government data in

tage in cyberspace and outer space is vital. At that time, we were talking about cross-domain warfare. Shortly thereafter, the Japanese government published a document titled the National Defense Program Guidelines (NDPG) intended to inform Japanese security policy for ten years or more; but, soon after taking office, Prime Minister Fumio Kishida announced that he would revise the NDPG, the National Security Strategy, and the Medium-Term Defense Force Development Plan. Clearly both the threat environment and the technological constraints and opportunities are evolving rapidly. It is difficult to keep up.

In cyberspace—and in particular in the Cyber Great Game—where, exactly, is the heartland? Professor Tsuchiya suggested that there are two. One is data centres. Increasingly, we depend in all aspects of our lives on data. One indication of this dependence is the decline of cash. More and more financial transactions are taking place purely in the digital domain. These transactions and other financial services depend upon reliable data centres. Recognizing the importance of these, Russia launched cruise missile attacks against Ukrainian data centres early in the course of its invasion, but, anticipating this, Ukraine had already moved much of its critical information to data centres in other countries.

The other crucial piece of the cyber heartland today is cognitive space: i.e., our brains. We are drunk with social media such as Twitter and Facebook. We consume too much fake information. If we are reading *Yomiuri Shimbun* or *Nikkei*, we are fine; but young people today get most of their information from unreliable social media. We are now used to talking about the IoT—the Internet of Things—but we should be talking about the IoB: the Internet of Brains, or Bodies, or Behaviours. In the future, our brains may be connected directly to the Internet, making those connections liable to hacking and disruption. What was fantasy in the 1982 Clint Eastwood movie *Firefox*, in which the Soviet Union had perfected a fighter aircraft controlled entirely by the thoughts of its pilot, is now reality. We are finding ways of connecting our minds to machines and controlling them solely by thought. In the future, it may be possible to hack those machines by hacking or hijacking the thoughts.

Thus, prevailing in the Cyber Great Game requires two capacities: protecting the physical infrastructure of cyberspace, and protecting the integrity of our data and cognitive space. The era of "hybrid warfare" is over; we must now think about the era of "super hybrid warfare" that fully embraces all aspects of the Cyber Great Game. Japan should take four firsts steps down this path as prepares the next version of the NDPG:

1. Organize units for psychological and cognitive warfare
2. Improve signal intelligence capabilities
3. Lay the constitutional and legal groundwork for the Japanese equivalent of a "Defend Forward" strategy
4. Develop "Persistent Engagement" capabilities to dissuade disinformation.

Following his presentation, Professor Tsuchiya took questions from the floor.

The first participant posed two questions. The first concerned attribution: How difficult is it to determine who is responsible for a cyberattack and whom to target in response? The second concerned the vulnerability of key parts of the physical infrastructure of cyberspace: as the Internet is a complex network, is it not the case that data can be rerouted relatively quickly through other nodes if certain data centres, cables, landing sites, etc., are disrupted or destroyed? With respect to the first question, Professor Tsuchiya responded that attribution can be very difficult for Japan, but that it is much easier for members of the Five Eyes because they have a legal framework for tapping communications during peacetime. Article 21 of the Japanese constitution protects secrecy of communication, and both the government and the private sector interpret this article very strictly. It is very difficult for the Japanese intelligence community to get permission to pry. With respect to the second question, a certain amount of disruption can be accommodated, but this varies by sector and by service. Everyone can tolerate a degree of latency in Facebook or Twitter, but the tolerance for latency in the financial sector (for example) is minimal.

The second participant also posed two questions: First, does Article 9 place any limits on cyber warfare capabilities? Second, is there a dominant capability in cyberspace today analogous to cavalry during the Mongol Empire or seapower in the 19th and and early 20th centuries? In response to the first question, Professor Tsuchiya said that much depends upon what counts as "warfare." Article 9 clearly prohibits offensive war, but bits are not bullets, and in his view Article 9 should not constrain proactive cyber defence operations. However, this is not the government's view. As for the second question, it is clear that an advantage goes to the country

that has the most sophisticated tools and techniques, and in this respect the United States (and in particular the National Security Agency) has no peer; but one of the things that makes the United States so effective in the cyber domain is cooperation between the U.S. government and important private sector players such as Microsoft and Google, whose products and services play such a big role in the operation of the Internet. Other countries do not benefit from this "teamwork" approach to cybersecurity.

A third participant, noting that in many countries such as Russia, China, and Iran the government is, in effect, engaged in cyber warfare with its own citizens to suppress dissent and maintain political control, asked whether it is possible for others (such as the United States) to interfere with these efforts on behalf of the people in those countries? Professor Tsuchiya answered that, yes, both third party governments and private third parties can interfere with this dynamic. One example is the provision of virtual private network (VPN) software to enable people to get around their own governments' censorship efforts. The result is a game of cat-and-mouse between state actors and both citizens and foreign actors over communications and access to information.

The next participant asked about the impact of cyber technology development on the future warfare. As the cyber domain becomes more advanced, vulnerabilities can increase. Can we expect state militaries to turn back to analog technologies that cannot be hacked or otherwise disrupted remotely in response? Relatedly, as it is difficult to measure cyber capability, how can we assess a modern balance of power? Professor Tsuchiya agreed that one workaround to opponents' cyber capabilities is to use older technologies or to avoid relying on modern ones. The U.S. military, for example, increasingly trains pilots and sea captains to navigate without the aid of GPS. As for measuring a balance of power in the cyber domain, Professor Tsuchiya acknowledged that this is very difficult without clear metrics and confessed that he knew of no reliable methods.

The final participant posed three questions: First, is it possible to distinguish offensive cyber capabilities from defensive ones, and, if not, what justifies the Japanese government's reluctance to engage in cyber operations on the ground that Article 9 prohibits them? Second, is it possible to deter cyberattack? Third, even when it is possible to identify the point of origin of a cyberattack (for example, to trace it back to Russia), is it technologically possible to determine whether it was conducted at the behest of a national leader? Professor Tsuchiya agreed that it is difficult to distinguish offence from defence in the cyber domain; they are generally two sides of the same coin. On his view, this means that "offence" and "defence" are not particularly helpful terms. But one good thing about the 2018 NDPG was that it did call simply and straightforwardly for authorizing counterstrike operations in pursuit of national security. The government—and in particular the Ministry of Defense—are reluctant, however. As for deterrence, this is simply not possible, in part because political leaders cover their tracks by engaging proxies. Much of the time it makes sense to assume that there is a connection between leaders and hackers, however, and Professor Tsuchiya said that he believes that it would be a mistake to avoid public attribution where there is reasonable suspicion.

# Policy, Governance, and Geopolitical Implications of Global Internet Metastasization

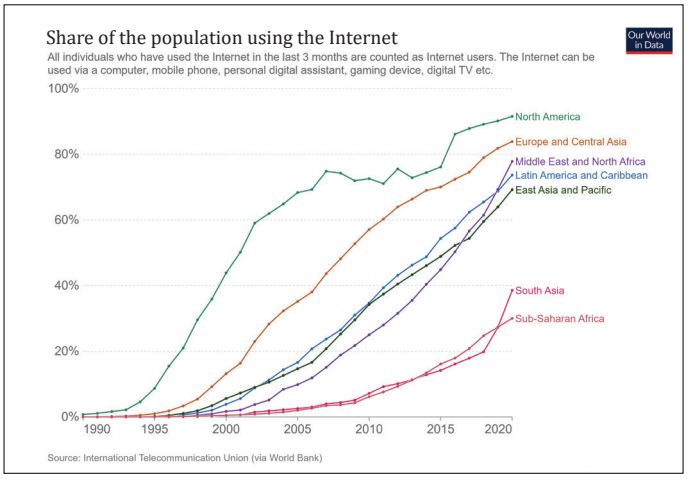
Mark Raymond

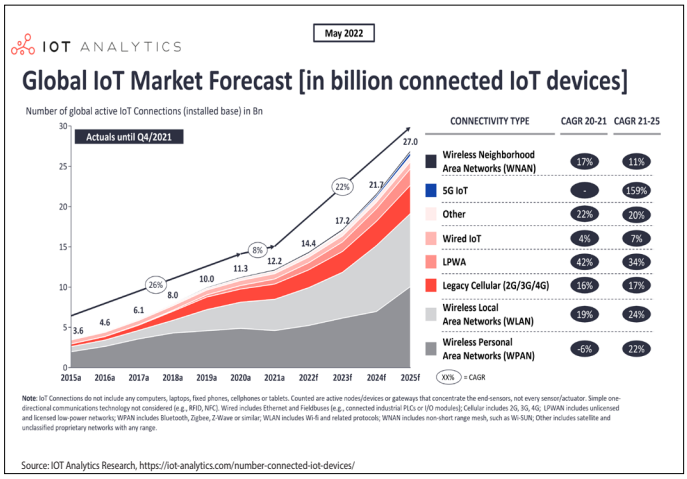
*Cyber Governance and Policy Center, University of Oklahoma, Norman, OK, USA*

The second presentation was by Professor Mark Raymond of the University of Oklahoma on the subject of cyber governance.

Professor Raymond began by drawing an analogy between the growth of the Internet and the metastasization of cancer. By this he did not mean to suggest that the Internet is cancerous, but that both exemplify a process of rapid systemic spread that can change the overall function of the system. With respect to the growth of the Internet, there are two phases to this metastasis: the first is technological; the second is of the governance arrangements that accompany the technology.

Approximately 62 percent of all people in the world are Internet users, although the timing and rates of adoption have varied considerably from region to region. There is also considerable within-region variation in many cases. We have to bear in mind as well that the experience of connecting to the Internet is very different in wealthy countries and poorer countries. In the latter, the cost of connectivity as a proportion of total income is considerably higher and both connection speeds and availability tend to be much lower. Illiteracy and a native language not well represented on the Internet are also significant barriers to access. There are many different kinds of digital divides. Nevertheless, this is a very striking story overall. For example, since 2007, Kazakhstan has gone from approximately 5 percent Internet penetration to




86 percent—a remarkable rate of progress.

We see evidence of rapid systemic spread in every technology associated with the Internet. The submarine cables about which Professor Tsuchiya spoke provide just one example. Individual service providers' network infrastructures provide another. Internet exchange points, where individual networks hand off traffic to one another, are yet another. Again, however, despite the rapid systemic spread of all these technologies, both the timing and extent of their spread has been uneven across the globe.

A particularly good example of technological metastasis is the Internet of Things (IoT). IoT devices are Internet-connected devices that are not intended primarily for direct human interaction. Most IoT connectivity is machine-to-machine. Increasingly, these connections are monitored by artificial intelligence (AI) systems that flag issues requiring human intervention. These are highly-automated, very large scale systems.

When we speak of IoT devices, we are generally talking about two categories of things: (1) sensors of various kinds; and (2) actuators, or switches. The main applications for these include consumer devices (such as wearables, medical devices, and appliances), industrial monitoring and control systems (e.g., logistics systems, energy systems, and manufacturing processes), and infrastructure (smart cities, smart grids, and surveillance). Note that surveillance is not an application unique to authoritarian states; some liberal democratic countries, such as Britain, invest heavily in surveillance infrastructure as well.

According to one consultancy firm, the number of IoT devices in the world will increase from 3.6 billion in 2015 to 27 billion in 2025—a mere ten-year span. Sensors and actuators will vastly outnumber computers, laptops, and smartphones. In other words, most Internet traffic will be machine-to-machine and will not require—or in most cases even permit—human interaction. In addition, most IoT connections will be wireless (e.g., Bluetooth, WiFi, cellular, and 5G), many of which have poor security protocols and are easy to exploit.

As technology spreads, the reach of the governance arrangements that correspond to those technologies also spreads. A necessary consequence of Internet metastasization, then, is the metastasization of the global Internet policy regime complex—the set of institutions and processes that somehow deals with Internet governance. This is an extremely decentralized regime complex. No single entity, institution, or process governs the Internet, and there are various loci of governance that involve a wide range of types of actors (for example, international organizations, multistakeholder organizations, private firms, sovereign states, and substate actors (national security agencies, regulatory agencies, legislatures, subnational governments, and courts).

Despite the cacophony of actors and the complexity of their interactions, it is vital that key Internet resources such as domain names and IP addresses be globally unique and that networked hardware and software use common standards and protocols (such as TCP/IP, BGP, Wi-Fi, 5G, and so on) to ensure interconnectivity. In addition, most sectors of the digital economy are heavily globalized with enormous market concentration in Western and East Asian firms. This means that states confront large tech incumbents with substantial influence over news consumption, email, search, mapping, and other key services, in addition to crucial hardware and software. The capacity of states to shape Internet governance to their liking is therefore severely limited. Nevertheless, contrary to a popular metaphor, the Internet is not "the Wild West." It is inherently rule-governed and requires a high level of cooperation and compliance. Cyber issues present novel governance challenges, but these are as much about too many potential governing actors and arrangements as too few.

Thus, like the Internet itself, governance arrangements for cyber policy are also metastasizing rapidly on two dimensions: (1) the number and kinds of actors seeking to participate in global cyber governance and policy; and (2) problems of deconfliction, i.e., reconciling disputes among different actors and governance processes over such things as transnational data flows, handling private and personal information, regulatory oversight conflicts, supply chain cybersecurity, human rights protections, moderating political speech, and regulating newsfeed algorithms. Because of metastasization

on these two dimensions, both the Internet and its governance arrangements are becoming enmeshed with institutions and governance arrangements in every issue area and in every state. This enmeshing is genuinely systemic—no part of the international system will remain untouched; it is both rapid and unplanned; and it is enormously consequential. It has the potential to fundamentally transform the operation and even the viability of the international system.

Cooperation and coordination in Internet governance are not automatic; they must be organized and managed. This requires figuring out how to monitor compliance in situations with defection incentives, figuring out how to interpret and apply multiple sets of loosely-related, partially-overlapping rules to novel empirical cases, satisfying the demand for democratic control and accountability, ensuring fairness (larger actors are in a good position to impose their preferences), and empowering smaller actors to shape domestic policy in the face of global pressures for conformity.

The phenomenon of Internet metastasization has three sets of implications. One set concerns policy and governance. The viability of most other global governance arrangements increasingly depends on the viability of the Internet governance regime because of Internet dependence and policy overlap. At the same time, Internet metastasization diminishes the scope for truly domestic policy. Everyone is now a small open polity.

The second set of implications is geopolitical. Increasingly, states are attempting to establish and enforce regulatory regimes that potentially have global implications and can affect state power. Recently, for example, we have seen the United States and the European Union attempt to assert their own visions of privacy protections and antitrust measures. These are "like" polities that agree on liberal democratic values, and yet their disagreements are severe. Russia and China are similarly engaged in Great Power competition by means of domestic regulatory processes intended to have global effects congenial to parochial national agendas.

The third and final set of implications is systemic. As Russia and China spearhead a move to bring Internet regulation increasingly under sovereign state control, we are witnessing a rise in what might be called "authoritarian multilateralism" whose ultimate purpose is to weaken the liberal DNA of global governance arrangements in general, disempowering the West.

All of this suggests that global cooperation and coordination on cyber governance is becoming more difficult even as it becomes more important.

The first participant in the Q&A session that followed Professor Raymond's presentation began by asking (1) What are some of the most important emergent properties of Internet metastasization? and (2) What are some of the most important unintended consequences of attempts to keep the governance of a metastasizing Internet up to speed? Professor Raymond replied to the second question first by means of an anecdote. Kazakhstan experienced severe political unrest in January 2022 that was in large part an unintended consequence of China's 2021 ban on cryptocurrency mining. Because Kazakhstan has an open cyber policy, crypto miners fled China for Kazakhstan where their server farms led to a spike in energy demand and electricity prices that prompted riots that toppled the government. As far as emergent properties are concerned, Professor Raymond opined that the most important ones are a dramatic decline in stability, a decline in respect for human rights, and an increase in violence. The 2021 January 6 insurrection in Washington, D.C., was in some sense a consequence of an out-of-control social-media-driven (dis)information environment leading to political polarization, an erosion of trust in public institutions, and disinhibition with respect to norm violations.

The second participant asked (1) whether Professor Raymond was pessimistic, and, if so, moderately pessimistic or deeply pessimistic, and (2) whether the main challenge to cyber governance today is China. Professor Raymond replied that he is pessimistic but takes heart in the thought that human history has been punctuated by crises and disasters and, so far, we have managed to survive. China is indeed a major challenge, but it is not the sole source of difficulty; the liberal democratic world has made its share of missteps and has had its share of bad ideas.

A third participant asked Professor Raymond what he envisioned as a nightmare scenario for unchecked Internet metastasization. Professor Raymond said that he believes that a failure to discipline social media could plausibly lead to catastrophic political instability. Allowing social media companies to self-regulate and/or leaving everything "up to the market" will only empower people to indulge their basest instincts and lead to a wholesale erosion of civilized norms.

The next participant asked whether domestic political and legal systems could keep up with both developments in global governance and developments in technology. Professor Raymond acknowledged that this is a challenge but felt that the wisest response would be to invest massively in social science research on how to embrace technological change gracefully. An illustration of the problem is the COVID-19 pandemic. Developing cutting-edge vaccines proved *not* to be a major challenge, but in many places persuading people to take them *was*. Cyber policy is a similar story. Getting people to embrace social media was no challenge at all; getting them to embrace it responsibly is proving to be enormously difficult. The good news is that social science is inexpensive; there is plenty of room for improvement at relatively little cost. Similarly, major investments should be made in enhancing states' and international organizations' governance capacity, so that policy can be implemented as effectively as possible.

The next participant asked if there was any prospect of a technological breakthrough that would enable us to reter-

ritorialize the Internet so that individual polities can have a cyberspace to their liking? Professor Raymond replied that the technology already exists to allow people to filter and silo to their liking, but this only works if there is a global network of networks. On the broader question of whether technology can solve social problems, people are enormously determined to break things that get in their way and can be ingenious in so doing. To the extent that social problems have solutions, those solutions are generally social. It would be unwise to invest much faith in technological solutions alone.

The next participant asked whether there is a more realistic and more useful taxonomy of regime types than a simple democratic/authoritarian binary and how this might inform our approach to cyber governance. Many states seem to fall into a gray zone between these archetypes. Professor Raymond agreed that there are "swing states" that do not fit neatly into the binary, but even representatives of the archetypes can behave in unexpected ways, undermining the utility of any rigid classification system. For example, when Russia and China sought to make cyber governance in the United Nations system less liberal in character, they did so by criticizing the U.N. General Assembly's Group of Governmental Experts process on the ground that it was "undemocratic." They sought to replace it with what ultimately became the Open-Ended Working Group, which any state could join. In effect, what they were doing was harnessing a liberal-democratic norm of inclusivity to take advantage of the fact that the U.N. has an authoritarian majority.

The next participant asked whether there is any interesting way in which the United States enjoys "hegemony" in cyberspace and whether there is any clear trend toward increasing fragility or increasing resilience in the cyber domain. Professor Raymond said he sees a clear trend toward increasing fragility. For him, realizing what weaponized social media could do was a wakeup call. Also, our rapidly increasing dependence upon vulnerable IoT devices is an underappreciated problem. As for whether the United States is hegemonic in cyberspace, it is difficult to know because hegemony is a fuzzy concept and to the extent that it exists it depends upon social recognition. Certainly, American firms and organizations have an outsized role in maintaining the technical infrastructure of the Internet, but the country as a whole currently lacks the vision and the unity of purpose to take a leadership role in cyber governance even if other countries were to welcome it.

The next participant asked for Professor Raymond's views on the lessons of the "Global War on Terror" for collaboration between government agencies and social media companies as a way of combating threat actors. Professor Raymond felt that this kind of collaboration can be valuable in principle, but a major problem is that a relatively small number of problematic people (such as Mark Zuckerberg and Elon Musk) can easily play spoiler roles. Until social media companies are regulated properly, there will be limits to the benefits of this kind of public-private partnership.

The final question was whether there were any heroes in Professor Raymond's story—for example, the European Union. Professor Raymond said no. For all of the EU's efforts to protect data privacy and rein in rogue social media companies, it has accomplished little other than forcing us to decide which cookies to accept when we visit EU websites. Our data are still for sale in Europe, just as they are almost anywhere else. More to the point: Professor Raymond said that he does not believe in heroes in general. Heroes get us off the hook of having to do the hard work of solving our own problems. No one is going to ride to our rescue in the face of Internet metastasization; we need to step up to the challenges ourselves.

# Reexamining Japan in Global Context

## Cybersecurity, Cyber Governance

October 13, 2022, Tokyo, Japan

**Presenters**

- Professor Motohiro TSUCHIYA, *Keio University*
- Professor Mark RAYMOND, *University of Oklahoma*

**Project Directors**

- Professor Masayuki TADOKORO, *International University of Japan*
- Professor David WELCH, *Balsillie School of International Affairs, University of Waterloo*

**Participants**

- Professor Naoyuki AGAWA, *Keio University*
- Mr. Hiroyuki AKITA, *Nihon Keizai Shimbun*
- Professor Tsuyoshi GOROKU, *Nishogakusha University*
- Professor Takako HIKOTANI, *Gakushuin University*
- Ms. Keiko IIZUKA, *Yomiuri Shimbu*n
- Professor Ryuzo KAWANAMI, *Osaka International University*
- Mr. Ryuichi KUROKI, *NTT Communications*
- Professor Seung Hyok LEE, *Tohoku Gakuin University*
- Mr. Yoshiyuki SAGARA, *Asia Pacific Initiative*
- Professor Noboru YAMAGUCHI, *International University of Japan*

**Suntory Foundation**

- Mr. Katsuyoshi OZAKI, *Executive Director*
- Ms. Noriko YAMAUCHI, *Chief Program Officer*
- Mr. Akira OU, *Associate Program Officer*

**Dr. Motohiro Tsuchiya** is Vice-President for Global Engagement and Information Technology at Keio University and Professor at the Keio University Graduate School of Media and Governance. He has been serving as guest editorialist at Nikkei since April 2019. He is the author of *Intelligence and National Security* (Tokyo: Keio University Press, 2007, in Japanese), *Cyber Terror* (Tokyo: Bungeishunju, 2012, in Japanese), *Cyber Security and International Relations* (Tokyo: Chikura Shobo, 2015, in Japanese), *The Cyber Great Game* (Tokyo: Chikura Shobo, 2020, in Japanese), and the co-author of *Cybersecurity: Public Sector Threats and Responses* (Boca Raton, FL: CRC Press, 2012) and 40 other books. He earned his BA in political science, MA in international relations, and Ph.D. in media and governance from Keio University. He received the 15th Nakasone Yasuhiro Award in 2019.

**Dr. Mark Raymond** (@ProfMarkRaymond) is the Wick Cary Associate Professor of International Relations and the Director of the Cyber Governance and Policy Center at the University of Oklahoma. He has contributed policy commentary to outlets including *Lawfare* and *The Monkey Cage*. He was a Senior Advisor with the United States Cyberspace Solarium Commission and has testified before the United Nations Commission on Science and Technology for Development, where he also participated in the Internet Governance Forum. He is an External Affiliate of the Ostrom Workshop at Indiana University and was previously a Fellow with the Center for Democracy and Technology as well as a Carnegie Fellow at the School of International and Public Affairs at Columbia University. He is the author, among other things, of *Social Practices of Rule-Making in World Politics* (New York: Oxford University Press, 2019).

REEXAMINING JAPAN IN GLOBAL CONTEXT 国際研究プロジェクト グローバルな文脈での日本 SUNTORY FOUNDATION

'Reexamining Japan in Global Context' is a proud partner of the Japan Futures Initiative, a network of scholars and practitioners dedicated to the promotion of the policy-relevant social scientific study of Japan. For more information, visit https://uwaterloo.ca/japan-futures-initiative/

JAPAN FUTURES INITIATIVE 日本の未来プロジェクト Hosted by the University of Waterloo・ウォータールー大学主催