



US-Japan Cyber Forum Series

Session 2: Strengthening International Cooperation Through Cyber Diplomacy

March 29, 2023 (US) | March 30, 2023 (Japan) | Virtual (Zoom)

Key Findings

On March 29, 2023 (US), with support from the US Embassy in Tokyo, and in partnership with the Research Center for Advanced Science and Technology Open Laboratory for Emergence Strategies (ROLES) at the University of Tokyo, Pacific Forum hosted the second virtual session of the *US-Japan Cyber Forum, “Strengthening International Cooperation Through Cyber Diplomacy.”* Over 30 participants from government, private sector, academia, and non-governmental organizations joined the online discussion.

Mihoko Matsubara, Chief Cybersecurity Strategist, NTT Corporation Tokyo, Japan, **Wilhelm Vosse, Ph.D.**, Professor of Political Science and International Relations, International Christian University, Tokyo, and **Benjamin Bartlett, Ph.D.**, Assistant Professor, Department of Political Science, Miami University evaluated the US and Japan’s respective cyber diplomacy efforts to improve and harmonize approaches to cyber capacity-building and ensure long-term impact. **Akira Igata**, Project lecturer at the Research Center for Advanced Science and Technology at the University of Tokyo moderated the discussion.

Evolving Cyber Threats

The ever-increasing volume and sophistication of cybersecurity threats have driven the US and Japan, to step up efforts in international cybersecurity cooperation. Major cyber incidents such as the 2021 Colonial Pipeline security breach and more recently, Russia’s deployment of malware targeting Ukrainian critical national infrastructure have further underscored the urgency to increase investment in cyber diplomacy as a vital component of national security.

Through its cyber diplomatic engagements, Japan has prioritized heightened cooperation with the US as well as other like-minded countries. Following Russia’s unprovoked invasion of Ukraine in February 2022, Japan’s Self-Defense Force hosted the first international cyber exercise involving armed forces personnel. Shortly after, the US, France, Australia, Indonesia, the Philippines, and Vietnam joined the Japan-led cyber exercise in March 2022. Similarly, Japan also mounted the biggest cyber defense drill that involved the US, UK, France, and the 10 ASEAN member countries at the height of the pandemic in 2020. Since 2011, the Japanese Ministry of Defense and the Japan Ground Self-Defense Force have been participating in the Locked Shields cyber exercise organized by the North Atlantic Treaty Organization Cooperative Cyber Defense Centre of Excellence. Additionally, Japanese civilian agencies and companies operating critical national infrastructure have also participated in the said exercise.

Apart from the proliferation of acute cyber threats, authoritarian states are also presenting broad challenges to international norms of “open and transparent internet governance” and relevant frameworks such as “Data Free Flow with trust” through mass surveillance, cyber espionage,

ensorship, disinformation campaigns, and promotion of data localization. Although, a major gap persists on how states should effectively confront such new types of Information and Communications Technology-related risks, Tokyo and Washington have remained committed to the precepts of international law and cyber norms as foundational pillars to maintain an open, secure, and interoperable internet.

Advancing Cyber Diplomacy

Russia's unprovoked invasion of Ukraine has had a profound impact on Japan's overall perception of threats and security concerns. While the Japanese government's spending on cybersecurity has risen over the last few years, the Ukraine crisis and its subsequent effects fueled the momentum further to meet the increased demands toward cyber threat deterrence and beefing up cyber capacity-building. In response, Japan has positioned cybersecurity as a top agenda that is closely tied to economic and national security based on the Economic Security Promotion Act and the National Security Strategy in 2022.

Although Japan's adoption of active cyber defense has dominated recent headlines, more attention should be devoted to Tokyo's sustained, if not elevated, cyber diplomacy engagements. Internationally, Japan continues to support a multi-stakeholder approach to internet governance through forums like the UN Group of Governmental Experts, and the UN Open-Ended Working Group and endorsed the 11 UN Norms of Responsible State Behavior in Cyberspace. Compared to the US which is still struggling to find the ideal balance between regulation innovation towards its Big Tech as well as China's top-down control of its digital economy, Japan has walked a similar path to the European Union in promoting a more human-centered approach to digital development.

While Japan's Ministry of Foreign Affairs and the Ministry of Economy and Industry have gained positive perception in leading cyber diplomacy engagements at the technical and policy level, more work needs to be done. Japanese ministries remain very operationally siloed. Greater interagency cooperation and clearer divisions of responsibility could produce more efficient coordination on capacity-building initiatives. If done right, this could lead to a more compelling public perception of Japanese cyber diplomacy at home and abroad.

Improved Prospects for US-Japan Cyber Diplomacy

Evidently, critical and emerging technologies have become the latest battleground for strategic competition between the US and China in the Indo-Pacific, especially in Southeast Asia. Concerns surrounding China's technology and infrastructure development range from covert mass surveillance and censorship to the rewriting of international technical standards and governance norms in the digital domain. Under the Biden administration, the US is determined to regain its influence by providing feasible alternatives to China's Digital Silk Road. However, its global portfolio of foreign policy and security often distract its focus. As the US struggles to fully concentrate in the Indo-Pacific amid the crisis in Europe, Japan is stepping up.

Japan's cyber diplomacy in Southeast Asia covers a wide swath of initiatives, spanning joint capacity-building, multilateral confidence-building initiatives, digital development partnerships, and cyber norm reinforcement. Considering Tokyo's trusted reputation in cyber diplomacy in the region, it will be strategic for Tokyo to lead with Washington D.C. providing complementary support. Together, the



US and Japan will continue to promote an open and transparent internet, especially in today's hyperconnected yet fragmented world.

This document was prepared by Brandt Mabuni and Mark Bryan Manantan. For more information, please contact Mark Bryan Manantan, Director of Cybersecurity and Critical Technologies at the Pacific Forum (mark@pacforum.org). These preliminary findings provide a general summary of the discussion. This is not a consensus document. The views expressed are those of the speakers and do not necessarily reflect the views of all participants. The speakers have approved this summation of their presentation.