PACIFIC FORUM INTERNATIONAL

US-Japan Cyber Forum Virtual Series

Session 1: Advancing Cyber Defense and Resilience in the Age of Strategic Competition

February 16, 2023 (US) | February 17, 2023 (Japan)

Key Findings

On February 16, 2023 (US), with support from the US Embassy Tokyo, and in partnership with the Research Center for Advanced Science and Technology Open Laboratory for Emergence Strategies (ROLES) at the University of Tokyo, the Pacific Forum hosted the first session of the *US-Japan Cyber Forum*, "Advancing Cyber Defense and Resilience in the Age of Strategic Competition." Over 30 participants from government, private sector, academia, and non-governmental organizations joined the online discussion.

Dr. Emily Goldman, Strategist at the US Cyber Command, **Dr. Koichiro Komiyama**, Senior Researcher of the Keio Research Institute at SFC, and **Michael Karimian**, Director of Digital Diplomacy, Asia and the Pacific, at Microsoft assessed recent developments in US-Japan cybersecurity cooperation in the wake of a rapidly changing geostrategic landscape, increasing technical and operational challenges, and rising demands for improved public-private cooperation on information-sharing. **Mark Manantan**, Director of Cybersecurity & Critical Technologies at the Pacific Forum, served as the host and moderator of the virtual event.

Key findings from the webinar are below.

Defending against cyberattacks and cyber espionage is nothing novel for the US and Japan. However, heightened strategic competition and gray zone activities have prompted the allies to ramp up their cybersecurity capacity-building and bureaucratic restructuring to counter state-sponsored cyber threat actors. Russia's invasion of Ukraine, Iran's persistent attacks on US infrastructure, North Korea's cybercrime operations, and China's cyber-enabled intellectual property theft have continued to undermine stability within and beyond cyberspace.

According to its 2022 Digital Defense Report, Microsoft saw a sharp uptick in cyberattacks against critical national infrastructure, especially Information and Communications Technology entities, corporate firms, non-governmental organizations and research institutions in the US, UK, Israel, Switzerland, Japan, Australia, Germany, India, and Canada. In addition to longstanding advanced persistent threat campaigns, Russian cyber influence operations are also on the rise due to the ongoing war in Ukraine.

The increasing intensity, severity, and sophistication of cyber operations have led the US and Japan to coordinate more closely. They are expanding their recognition of adversarial capabilities beyond the binary of peacetime or wartime. As strong supporters of open, secure, and interoperable internet, the US and Japan have the primary responsibility to exemplify credible digital governance as they pioneer new methods of proactive cybersecurity and operational readiness in the increasingly contested cyber domain.

On the US side, election security concerns coupled with growing momentum for a more proactive approach to cybersecurity in the 2018 Department of Defense Cyber Strategy were pivotal for US Cyber Command's new operational approach called Persistent Engagement. The adoption of Persistent Engagement has enabled US military cyberspace forces to “defend forward” in cyberspace. Unlike a deterrence framework, Persistent Engagement fosters a more agile and anticipatory stance against adversaries operating below the threshold of armed conflict, while building more resilient domestic and foreign partnerships though a whole-of-nation "plus" approach.

Japan is also undergoing a dramatic shift to further strengthen its cybersecurity. The new National Security Strategy and accompanying National Defense Strategy and Defense Buildup Program released at the end of 2022 reflect Japan’s adaptive response, known as active cyber defense. Under active cyber defense, Japanese Self Defense Forces or relevant authorities can neutralize an adversary's systems if an imminent threat is detected.

Although the Kishida administration has made assurances that active cyber defense is still within the remit of defensive cyber operations, it certainly faces political, legal, and normative challenges before becoming fully operational. The Japanese constitution that grants broad protections to the secrecy and privacy of communications makes the implementation of active cyber defense difficult. Furthermore, active cyber defense requires approval from Japan’s legislative body. But given the urgency for Japan to bolster the reach and impact of its cybersecurity defenses, the Kishida administraiton will most likely propose changes to several laws to acquire the capacity to perform a preemptive cyber operation.

Despite their respective institutional and operational challenges, the US-Japan alliance holds the potential for even greater collaboration in cybersecurity based on a shared understanding of the need to proactively contest, rather than just react, to cyberspace threats. This is reflected in similarities between Japan's active cyber defense and the US approach of persistent engagement. An underlying objective of the cybersecurity partnership is proactive prevention of high-intensity conflict in the Indo-Pacific—an aim that ties cyber operations into other domains of ongoing defense cooperation.

This document was prepared by Brandt Mabuni and Mark Manantan. For more information, please contact Dr. Crystal Pryor (crystal@pacforum.org), Director of Research at the Pacific Forum. 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 or any government agency. The speakers have approved this summation of their presentation.*