US-Japan Cybersecurity Mapping Project: Advisory Workshop

Abstract

On July 20, 2022, the NEXT Alliance Initiative convened an Advisory Workshop with Japanese and American specialists from think tanks and government to share the ideas and plans of the NEXT Alliance cyber security mapping project. The small gathering of subject matter experts was designed to solicit feedback and help improve the overall approach of the project. This not-for-attribution workshop summary was prepared to raise awareness of our alliance mapping project and highlight important bilateral issues in the realm of cyber security management.

Alliance Mapping

This cyber security project by the Sasakawa Peace Foundation USA's NEXT Alliance Initiative aims to create a web-based tool that will "map" cyber security management in the United States, Japan, and bilaterally. Such an interactive organization and flow chart will help policy makers, scholars, and the private sector more easily understand how each country organizes itself to maintain cyber security and how the management process functions in and across both countries.

When the project is completed and the tool is created, all sectors can better understand the various responsibilities, capabilities, and characteristics of each agency in ways that should facilitate smoother and more effective cooperation. The lunch roundtable was just the first in a planned series of similar discussions designed to help steer the mapping project in a productive direction. The NEXT Alliance team is conducting its research with two overarching questions in mind: what type of information will be of interest to alliance managers, policy makers, and the private sector on both sides; and how can it help improve mutual understanding and policy coordination?

Advisory Workshop Outline

Sasakawa USA Senior Director Jim Schoff began by describing the cyber security alliance mapping project objectives, approach, and research to date. Designing the interactive web-based tool begins with recognizing the cyber security landscape in each country and the allies' bilateral agenda. Schoff explained the project's understanding of pertinent cyber security agencies, leaders, and policies in the United States and Japan. He then suggested that one possible way to organize this information would be to make it searchable around three broad themes in which the key players might be involved: 1) strategy and policy; 2) protection and enforcement; and 3) regulations and compliance. After the initial presentation, Schoff facilitated group discussion to confirm various facts about the alliance mapping research and consider collectively the best way to convey this information to an end user.

Discussion Summary

The fruitful discussion yielded several good ideas, insights and perspectives from the attendees that helped improve the direction of the project. The attendees complimented the initial steps taken in research, structure, and presentation, but they also pointed out areas that could be improved. The discussion began with consideration of how cyber security is managed "in practice" by each government, compared to how it simply looks "on paper."

A Japanese participant noted that his country has been working hard to improve the quality and comprehensiveness of its cyber security management, although it still has work left to do. A key issue he noted was insufficient interagency communication, and that while it is required within

ministries to report cyber incidents, there is neither a national coordination requirement nor standardized inter-ministry notification. He suggested that the National Security Secretariat could be a bridge for cyber security both domestically and internationally. Despite this, the participant highlighted Japan's successful cyber defense during the 2020 Tokyo Olympic games, as they handled as many as four million cyber-attacks without a single crippling incident. He stated that the goal of Japan's cyber security community should be to strengthen channels of information sharing at the confidential level and improve threat detection and attribution capabilities. He added that greater cooperation internationally is needed in order to bridge the gaps that exist in cyber security management.

An American participant highlighted a range of issues within industry, work force staffing, and incident reporting. He pointed out that within the US-Japan alliance there is a shortage of cyber security staff and suggested the allies shift focus to how alliance managers could support the growth of that work force. He also noted that a major challenge for cyber security in the United States is effective information sharing between the public and private sectors. Private sector security clearances are supposed to aid this information sharing, but the necessary procedures can be burdensome and discourage follow through. Finally, on incident reporting, he added that the primary concern should be identifying who suffered an attack, where it occurred, and which agencies need to be informed and involved.

Turning to the issue of how to design a web-based organization and flow chart for maximum utility, another American suggested that the "three themes" approach (noted above) would likely be too difficult to distinguish clearly, given that at some level nearly all relevant agencies and offices are involved in all three areas. Moreover, the delineation points between where one organization's jurisdiction or responsibility ends and another's begins is usually vague. In fact, government officials involved are generally reluctant to clarify these points because it can limit their discretion depending on the situation. Officials are often caught between not wanting to take on too much responsibility for which their budgets and capabilities might not be sufficient, while also not wanting to clearly cede a role or stake in certain kinds of operations.

Rather, several participants suggested a narrower functional approach to theme development, and then identify the agencies relevant to the cyber security activities referenced in a flow chart for these activities. For example, national strategy might still be one theme, but without covering all of "policy." Other functions could include protection of critical infrastructure, incidence response, workforce development, and the like. They recommended approaching former government employees currently in think tanks who can shed additional light on how different cyber security offices factor into these different functional areas.

Last to comment and building off the participants observations and recommendations, Schoff noted that the online tool will need to be relatively basic in content to make it easy to use and navigate, as well as to limit the need for frequent updating. But the tool will require sufficient detail to add value for the end user. The functional areas chosen should correspond to activities that are important to the alliance and their bilateral cooperation agenda. This is the balance that must be struck.

NEXT Steps for Alliance Mapping

Cyber security has become an increasingly important part of US and Japanese strategic interests and alliance management. Both countries are taking steps—domestically, bilaterally, and multilaterally—to enhance resiliency and strengthen countermeasures in these areas. This has resulted in domestic reforms to cyber security policy making, capacity building, enforcement, and mitigation that in some cases is changing the way each country organizes itself to carry out these (and related) tasks (e.g., Japan's establishment of a Digital Agency or the US creation of the Office of the National Cyber Director).

Based on feedback from this roundtable discussion, the NEXT Alliance cyber security mapping project is shifting toward a more detailed functional approach. A flow chart design would allow the user to navigate through different processes, the organizations and offices involved, and how these functions might relate to the US-Japan bilateral cooperation agenda. The next leg of our research will explore the feasibility of mapping nine or ten different cyber security functions such as: incident response, critical infrastructure protection, work force development, law enforcement,

multilateral engagement, national strategy, national defense, public-private partnerships, and the telecom and Internet of Things sector. Updates will be published on this website when available.

The US-Japan NEXT Alliance Initiative is a forum for bilateral dialogue, networking, and the development of joint recommendations involving a wide range of policy and technical specialists (in and out of government) to stimulate new alliance connections across foreign, security, and technology policy areas. Established by Sasakawa Peace Foundation USA with support from the Nippon Foundation, the goal is to help improve the alliance and how it serves shared interests, preparing it for emerging challenges within an increasingly complex and dynamic geostrategic environment. Launched in 2021, the Initiative includes two overlapping lines of effort: 1) Foreign & Security Policy, and 2) Technology & Innovation Connections. The Initiative is led by Sr. Director Jim Schoff.