PACIFIC FORUM

WOMEN, PEACE & SECURITY

KEY FINDINGS & RECOMMENDATIONS FROM THE WORKSHOP ON

FORGING US-SOUTHEAST ASIA COOPERATION ON WOMEN, PEACE, AND CYBERSECURITY

Mark Manantan, Pacific Forum
Crystal Pryor (Ed.), Pacific Forum

FORGING US-SOUTHEAST ASIA COOPERATION ON WOMEN, PEACE, AND CYBERSECURITY

INTRODUCTION

Pacific Forum, in collaboration with the U.S. Indo-Pacific Command (USINDOPACOM) Office of Women, Peace & Security successfully concluded the regional workshop, "Forging US-Southeast Asia Cooperation on Women, Peace, and Cybersecurity," on November 15-16, 2023, at the Peninsula Manila, Makati City, Philippines. The two-day workshop supported those objectives outlined in the Association of Southeast Asian Nations (ASEAN) Regional Plan of Action on Women, Peace, and Security (RPA WPS) related to cybersecurity.

WORKSHOP OBJECTIVES

Leveraging Pacific Forum's Cyber ASEAN capacity-building initiative, the workshop adopted a multi-stakeholder approach that convened a total of 34 participants, including representatives from the Philippine Army, Philippine Navy, Armed Forces of the Philippines, the US Government, civil society organizations, and cybersecurity experts from think tanks and academia. The workshop aimed to achieve the following objectives:

- Unpack the concept of using a gender perspective in the formulation and implementation of cyber policy and strategy.
- Share best practices and lessons learned between the US and Southeast Asia to improve cyber capacity considering variances in digital maturity, and culture.
- Explore practical and actionable cyber policy recommendations oriented around gender inclusion.

PARTICIPANTS

Government/Defense

United States

U.S. Cybersecurity and Infrastructure Security Agency (CISA)
U.S. Indo-Pacific Command Office of Women, Peace & Security (WPS)

Philippines

Philippine Cybersecurity Bureau
Philippine Department of National Defense

Participating Defense Force Branches

Philippine Army
Philippine Navy
Armed Forces of the Philippines

Civil Society Organizations

Bullyid App-NMA Foundation
Center for Creative Initiatives in Health, and Population
Due Diligence Project
Foundation for Media Alternatives
Global Forum on Cyber Expertise
Institute of Strategic International Studies (ISIS) Malaysia
Stimson Center
UN Women - Regional Office for Asia and the Pacific
Vietnam Center for Creative Initiatives in Health and Population

KEY FINDINGS

Cyber threats pose significant challenges to international security, as evidenced by incidents such as state-sponsored cyber espionage campaigns targeting critical infrastructure, ransomware attacks disrupting global supply chains, and coordinated cyberattacks destabilizing diplomatic relations between nations. The field of cybersecurity faces significant human resource challenges exacerbated by the underrepresentation of women, hindering diversity, innovation, and the comprehensive response to evolving cyber threats.

Beyond the ways in which gender intersects with cybersecurity risks to international peace, cyber threats profoundly impact human security by jeopardizing personal privacy, financial stability, and even physical safety, exemplified through instances of identity theft, cyberbullying leading to mental health issues, and malicious hacking compromising medical records, thus highlighting the intricate link between digital vulnerabilities and individual well-being.

The intersection of cybersecurity and gender illuminates the complex dynamics shaping digital security, with profound implications for individuals and societies alike. Incorporating a gender perspective in cybersecurity is crucial for recognizing and addressing the unique vulnerabilities faced by diverse populations, fostering more inclusive and effective strategies in cybercrime prevention, cyber diplomacy negotiations, and cyber defense measures. By understanding how gender intersects with cybersecurity, we can develop more holistic approaches to safeguarding digital spaces and promote equity in the digital realm.

Context: Cybersecurity in the ASEAN RPA WPS

The RPA WPS was developed under the auspices of the U.S.-ASEAN Comprehensive Strategic Partnership with the U.S. Agency for International Development (USAID) in 2022. The RPA WPS recognizes the need to re-evaluate security beyond the traditional lens of armed conflict, taking into consideration emerging security challenges such as cybersecurity. The RPA WPS aims to mobilize pathways to increase women's meaningful participation in ensuring peace and stability and address the exclusion of all discriminatory factors such as age, gender, race, displacement, disability, and other drivers of insecurity to cultivate women's and men's meaningful participation.

To explore the four pillars of the RPA WPS, the Pacific Forum, in collaboration with the US Indo-Pacific Command (USINDOPACOM) Office of Women, Peace & Security held the regional workshop, "Forging US-Southeast Asia Cooperation on Women, Peace, and Cybersecurity," at the Peninsula Manila, Makati City, Philippines from November 15 to 16, 2023. Adopting a multi-stakeholder dialogue approach, the two-day workshop explored four important and interrelated facets of cybersecurity: cyber defense, cyber diplomacy, cybercrime, and cyber capacity to catalyze pragmatic cooperation in the context of U.S.-Southeast Asia cooperation.

Key findings from this event are described below.

USINDOPACOM's Women, Peace and Security Program Integrator, Amalia Hilliard, emphasized the urgency of integrating gender analysis into cyber policy and strategy during her opening remarks. "Understanding the role of gender in cyber can provide insights into how men, women, and gender-diverse individuals may experience and respond to cyber threats differently," she said. She provided several examples, including technology-assisted gender-based violence and gendered disinformation, harassment, and abuse in online spaces. Reflecting upon USINDOPACOM's engagements among partner nations, Hilliard noted the importance of collecting and analyzing sex-disaggregated data to inform gender-inclusive training, education, and decision-making in cybersecurity.

Pacific Forum's Director of Cybersecurity and Critical Technologies, Mark Manantan, discussed the imperative to analyze Southeast Asia as a diverse region comprising a multitude of languages, cultures, and levels of

digital maturity. Building on Pacific Forum's ASEAN cyber capacity-building project, Manantan noted the role of inclusion in reinforcing gender analysis to include perspectives from minority groups and persons with disabilities.

In the plenary sessions on Cyber Defense, Cyber Diplomacy, Cybercrime, and Cyber Capacity, experts and practitioners from government, industry, academia, and civil society from the US and Southeast Asia exchanged views on implementing gender perspectives in concrete terms. Overall, experts endorsed the need for localized and context-specific approaches or strategies, comprehensive and gender-responsive protection and support mechanisms, multi-sectoral dialogues, and financial support to fully advance the women, peace, and cybersecurity agenda.

As most countries in Southeast Asia are establishing their respective cyber defenses, experts urged defense planners and policymakers to leverage the perspectives of women and gender-diverse populations in addressing gender-specific cybersecurity concerns. Gender diverse perspectives in cyber-diplomacy ensure that cyber defense and cyber diplomacy efforts consider the experiences, needs, and concerns of all individuals affected by cyber policies and practices, promoting more inclusive and effective international cooperation in addressing cyber challenges.

Experts also argued that simply increasing the number of women in cybersecurity-related fields does not guarantee their meaningful participation, nor does it automatically result in effective integration of gender perspectives. To remedy this misconception, the experts echoed the need to operationalize and institutionalize gender perspectives in cyber defense to mitigate gender bias and disparities in women's recruitment and training.

Similarly, increasing women's proactive participation at the UN Group of Governmental Experts or UN Open-Ended Working Group on cybersecurity should require strengthening women's technical and negotiation skills as well as implementation of a gender perspective. Foreign Affairs ministries and departments must adopt gender-responsive policies to mitigate the prevailing stereotypes in diplomatic processes and negotiations between women and men.

Promoting inclusive growth in the cybersecurity workforce is a significant first step in addressing the myriad cybersecurity challenges in Southeast Asia. Although education and training opportunities are growing, structural barriers continue to prevent women from sustaining a viable career in the cybersecurity field over the long-term. To enhance cyber capacity, the formation of women, peace, and cybersecurity advocates is key. Allyship will help women thrive in the workplace and ensure career longevity. Creating a community of women, peace and cybersecurity champions will help elevate awareness of women's credibility and distinct capabilities in the male-dominated field of cybersecurity.

Utilization of a gender perspective in cybersecurity requires that practitioners look beyond human resource challenges to examine the human security risks posed by cybercrime, and how gendered insecurities contribute to wider national and regional instabilities. In Southeast Asia, women and young girls continue to suffer disproportionately as compared to men and young boys from online fraud and phishing scams. The proliferation of deep fakes due to generative AI have made women and girls even more vulnerable to cyber harassment and bullying. Due to the rapid evolution of cyber-related threats, experts stressed the need to reframe such concerns to be more encompassing.

Ignoring gendered cyber-insecurities not only perpetuates and reinforces systemic vulnerabilities for women and girls, but also undermines national security. Diverse perspectives are crucial for understanding and mitigating multifaceted cyber threats; ignoring them ultimately compromises the resilience of digital infrastructures and strategic defense capabilities. Integrating women's perspectives and expertise is essential for fostering inclusive strategies that address the full spectrum of cyber risks, safeguarding national interests and promoting sustainable security in an increasingly interconnected world. The workshop's key outcomes contribute to ongoing initiatives promoting the integration of gender-responsive cybersecurity measures in the Indo-Pacific region. This is consistent with Pacific Forum and USINDPACOM's commitment to advancing actionable policy recommendations and sharing best

practices for integrating WPS principles and a gender perspective into every aspect of defense and security.