Global Cyber Policy Dialogues: Southeast Asia

July 3-4, 2023
Singapore

MEETING MATERIALS

The Observer Research Foundation America and the S. Rajaratnam School of International Studies (RSIS), in partnership with the Cyber Security Agency of Singapore and the Ministry of Foreign Affairs of the Netherlands will be hosting an in-person Global Cyber Policy Dialogue in July 2023 in Singapore. This multistakeholder meeting will bring together participants from government, civil society, academia, and the private sector from across the region. A principal goal of the meeting is to foster genuine and open dialogue among stakeholders from different sectors and backgrounds. As such, the event will convene 50 participants from countries in the Southeast Asian region that are active in international discussions on cybersecurity and cybercrime taking place at the United Nations (UN), the Association of Southeast Asian Nations (ASEAN), and elsewhere. These include Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Philippines, Singapore, Thailand, Timor-Leste, and Vietnam.

A virtual preparatory meeting laid the groundwork for this event, and a summary is available to provide further background. The virtual meeting addressed the role of emerging technologies, international norms processes, and capacity building in the context of the region and the COVID-19 pandemic. In particular, the discussion produced insights about the foundational role of capacity building for international cooperation on information and communications technology (ICT) matters, the importance of cyber hygiene, the need for practical and trusted cooperation to address cybercrime, and the opportunities for engagement with multiple stakeholders at the regional level as well as in the context of the UN norms processes. This in-person conference will build on the themes of the virtual meeting and new topics in four moderated roundtable conversations that will cover the emerging threat landscape in cyberspace, promoting cooperation through cyber confidence building measures, developing public private partnerships, and continuing to strengthen Southeast Asian contributions to UN and international cyber discussions.

Monday, July 3, 2023

18:30-20:30	**RECEPTION HOSTED BY THE AMBASSADOR OF THE NETHERLANDS TO SINGAPORE, H.E. ANNEKE ADEMA**
Venue:	The Netherlands Residence 23 Ridout Road, Singapore 248416
18:00	*Bus departs for the Netherlands Residence (23 Ridout Road, Singapore 248416) from the official hotels: InterContinental Singapore Hotel (80 Middle Road, Singapore 188966) and Concorde Hotel Singapore (100 Orchard Road, Singapore 238840)*
20:30	*Bus departs the Netherlands Residence (23 Ridout Road, Singapore 248416) for the official hotels: InterContinental Singapore Hotel (80 Middle Road, Singapore 188966) and Concorde Hotel Singapore (100 Orchard Road, Singapore 238840)*

Tuesday, July 4, 2023

Venue: ASEAN-Singapore Cybersecurity Centre of Excellence
        251 North Bridge Road, Level 3
        Singapore 179102

        Please bring your passport (for all foreign participants) or NRIC (for local participants) for identification purposes

08:30 - 09:00   REGISTRATION

09:00 - 09:05   **WELCOME REMARKS**

        Sithuraj Ponraj, Director, International Cyber Policy Office, Cyber Security Agency of Singapore

09:05 - 09:20   **OPENING REMARKS**

        Yaacob Bin Ibrahim, Professor in Practice, Lee Kuan Yew School of Public Policy, National University of Singapore
        Boon Hui Khoo, Director, Global Cyber Alliance

09:20 – 10:45   **SESSION I: ASSESSING THE EMERGING THREAT LANDSCAPE IN CYBERSPACE**

        As a region with strong potential for digital transformation, Southeast Asia is striving to unpack the implications of both emerging threats and emerging technologies. As technology and geopolitical conditions evolve, Southeast Asian countries are working to understand the national security implications that cyber activities can pose. Ransomware, both criminal and state-connected, poses serious challenges to governments and businesses at all levels, as do online scams and business e-mail compromise. Emerging technologies, including AI-assisted attacks and power that quantum computing will bring, raise longer-term concerns. The proliferation of cryptocurrency and the rise of hacktivism add additional threats. This session will aim to establish and animate the landscape of contemporary threats and issues affecting Southeast Asian societies in cyberspace.

Moderator: **Bruce W. McConnell**, Distinguished Fellow, Observer Research Foundation America

Speakers: **Seow Hiong Goh**, Executive Director, Global Policy and Government Affairs, Asia Pacific, Cisco Systems
        Haji Mas Zuraime Haji Abdul Hamid, Head, Brunei Computer Emergency Response Team (BruCERT), Cyber Security Brunei
        Craig Jones, Director, Cybercrime Directorate, INTERPOL
        Elina Noor, Senior Fellow, Asia Program, Carnegie Endowment for International Peace *(via pre-recorded message)*

10:45 – 11:15   NETWORKING BREAK

11:15 – 12:30   **SESSION II: PROMOTING COOPERATION THROUGH CYBER CONFIDENCE BUILDING MEASURES**

Confidence building measures (CBMs) provide a vehicle for states to communicate concerns, alleviate mistrust and misperception, ensure predictability, and enhance cyber stability in the light of an evolving threat environment. This session will build on the experience of the Organization for Security and Co-operation in Europe's (OSCE) Confidence Building Measures on critical infrastructure, and ASEAN's own efforts through the ASEAN Regional Forum, particularly the open-ended Study Group on Confidence Building Measures. Initiatives such as the ASEAN Points of Contact Directory and ASEAN Regional CERT will be examined as well as other avenues for confidence building such as CERT-to-CERT cooperation. This session will discuss how existing trust building mechanisms fit with new issues and challenges for Southeast Asia, and what modifications or new tools could be brought to bear to facilitate information sharing, trust building, and norms implementation to reduce the chance of conflict. It will also touch upon the relationship between regional CBMs and the current discussions on CBMs in cyberspace taking place at the level of the United Nations.

Moderator: **Benjamin Ang**, Senior Fellow and Deputy Head, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

Speakers: **Ian Lim**, Field Chief Security Officer, Asia Pacific, Palo Alto Networks
Amir Hamzah Mohd Nasir, Assistant Secretary, Multilateral Security Division, Ministry of Foreign Affairs of Malaysia
Szilvia Tóth, Cyber Security Officer, Transnational Threats Department, Organization for Security and Co-operation in Europe (OSCE) *(via pre-recorded message)*
Lea Kaspar, Executive Director, Global Partners Digital

12:30 – 13:30   LUNCH

13:30 – 14:45   **SESSION III: CREATING AND ENGAGING WITH PUBLIC PRIVATE PARTNERSHIPS**

Industry and civil society are critical partners in responding to existing and emerging challenges including cybercrime, cybersecurity, trust building, enhancing capacity, and establishing and implementing norms. Public private partnerships within Southeast Asia are an important mechanism to ensure that, for everyday users and digital infrastructure ecosystems in the region, the availability and integrity of systems and data is maintained, and potential harmful impact is mitigated. This session will address how Southeast Asian governments can foster greater engagement and collaboration with the private sector and civil society, and vice versa, through partnerships to address cyber threats, undergird capacity, and achieve practical, mutually beneficial outcomes.

Moderator: **Bruce W. McConnell**, Distinguished Fellow, Observer Research Foundation America

Speakers: **Kathleen Bei**, Senior Advisor, Global Forum on Cyber Expertise (GFCE)
Michael Karimian, Director, Digital Diplomacy, Asia and the Pacific, Microsoft
Charles Ng, Executive Vice President, International Business and Consulting, Ensign InfoSecurity

Phannarith Ou, Director, Department of Information and Communications Technology (ICT) Security, Ministry of Post and Telecommunications (MPTC) of Cambodia

Nynke Stegink, Manager, Cyber Capacity Building, National Cyber Security Center of the Netherlands (NCSC-NL)

14:45 – 15:15	NETWORKING BREAK

15:15 – 16:30   **SESSION IV: CONTINUING TO STRENGTHEN SOUTHEAST ASIAN CONTRIBUTIONS AT UN AND INTERNATIONAL CYBER DISCUSSIONS**

ASEAN Member States have been playing an active and constructive role in supporting, and contributing to, international and regional cybersecurity discussions – including at the present UN Open-Ended Working Group (OEWG). This session will build on the previous sessions and take stock of the progress made at the OEWG and in other fora and consider ways in which Southeast Asian states can continue to contribute to these discussions, engage stakeholders and advance international cybersecurity cooperation through practical, concrete initiatives.

Moderator: **Benjamin Ang**, Senior Fellow and Deputy Head, Centre of Excellence for National Security (CENS), S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore

Speakers: **Platima Atthakor**, Head, Human Security Section, Department of International Organizations, Ministry of Foreign Affairs of Thailand

Bart Hogeveen, Head, Cyber Capacity Building, International Cyber Policy Centre, Australian Strategic Policy Institute

Huu Phu Nguyen, Deputy Director-General, Political and Security Matters, Department of International Law and Treaties, Ministry of Foreign Affairs of Vietnam

Farlina Said, Senior Analyst, Institute of Strategic and International Studies (ISIS) Malaysia

16:30 – 16:50   **REFLECTIONS FROM THE FLOOR**

16:50 – 17:00   **CONCLUDING REMARKS**

Maartje Peters, Head, Taskforce International Cyber Policies, Ministry of Foreign Affairs of the Netherlands

17:00 – 18:00	RECEPTION