Global Cyber Policy Dialogues: Southeast Asia

July 3-4, 2023
Singapore

MEETING SUMMARY

ORF AMERICA
RSIS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES Nanyang Technological University, Singapore
Ministry of Foreign Affairs of the Netherlands
CSA SINGAPORE

On July 3-4, 2023, 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 hosted an in-person Global Cyber Policy Dialogue in Singapore, held at the ASEAN-Singapore Cybersecurity Centre of Excellence. This multistakeholder meeting brought together over sixty participants from government, civil society, academia, and the private sector from across Southeast Asia. A principal goal of the meeting was to foster genuine, open dialogue among stakeholders from different sectors and backgrounds, and included representatives from nine Association of Southeast Asian Nations (ASEAN) member states.

A virtual preparatory meeting in August 2020 laid the groundwork for this event (see summary). The virtual meeting addressed the roles 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.

The July 2023 in-person conference built on the themes of the virtual meeting and covered new topics in four moderated roundtable conversations. These conversations covered the emerging threat landscape in cyberspace, promoting cooperation through cyber confidence building measures (CBMs), developing public private partnerships, and continuing to strengthen Southeast Asian contributions to United Nations and international cyber discussions. The two-day meeting began with a reception hosted by the Dutch Ambassador to Singapore where the delegates connected and shared perspectives and viewpoints on an informal basis. The following day consisted of four working sessions, conducted in roundtable format to maximize participation and diversity of viewpoints.

This dialogue was convened as part of the Global Cyber Policy Dialogue Series, a project undertaken by ORF America and the Ministry of Foreign Affairs of the Netherlands, which seeks to address key cyber challenges, strengthen multistakeholder networks, and increase coordination of regional capacity building initiatives. These meetings are intended to complement and inform ongoing international-level cyber norms processes, such as the United Nations Open-ended Working Group on Security of and in the use of ICTs (OEWG) and the Ad Hoc Committee to Elaborate a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes (Ad Hoc Committee).

The discussions took place under the Chatham House Rule. Sithuraj Ponraj, Director, International Cyber Policy Office, Cyber Security Agency of Singapore, Yaacob Bin Ibrahim, Professor in Practice, Lee Kuan Yew School of Public Policy, National University of Singapore, and Boon Hui Khoo, Director, Global Cyber Alliance were invited to deliver opening remarks.

The opening speakers provided comments that emphasized the importance of participants embracing different perspectives and learning through the various “languages” of the diverse sectoral expertise in attendance. They pointed to the growth in Southeast Asian states’ collaboration in cyberspace through ASEAN and bilateral engagements, significant progress in a short time made on involvement with the UN and international processes, and the research findings of new cybersecurity institutions set up at the national level within the region. In a rising threat environment with increasing complexity in cyberspace, utilizing an approach based on multistakeholder principles and collaboration will increase the capacity of the region to meet those challenges.

The following four discussion sessions were moderated by Bruce W. McConnell, Distinguished Fellow at ORF America, and Benjamin Ang, Senior Fellow and Deputy Head, Centre of Excellence for National Security (CENS) at RSIS.

Assessing the Emerging Threat Landscape in Cyberspace

Southeast Asia faces a rapidly evolving threat landscape with over 125,000 new Internet users added in the region each day. With these new users, the dependence of critical infrastructure on the Internet, and increased use of digital electoral services, online healthcare services, online payments and crypto currencies, cybercrime and cybersecurity have become major concerns.

This session began with brief remarks by Seow Hiong Goh (Cisco Systems), Haji Mas Zuraime Haji Abdul Hamid (BruCERT), Craig Jones (INTERPOL), and Elina Noor (Carnegie Endowment for International Peace).

It was pointed out that because cybercrime is borderless, existing national laws and regulations make it challenging to redress incidents. Concerns were shared about "ransomware as a service" whereby increasingly sophisticated, wealthy criminal enterprises have specialized in selling specific cybercrime tools. Criminals have increased victims' incentives to pay ransoms, including threatening to discredit an organization's leadership. Some participants shared that Bank Identification Number (BIN) attacks that are then leveraged to compromise ChatGPT accounts present another demonstrated, emerging problem tied to AI.

Law enforcement and private sector stakeholders shared examples of linking training to specific operations, public policy outcomes, or business achievements to overcome sustainment issues. There was also a tension identified in national cyber strategy development whereby frameworks tend to be inward looking despite international threat vectors.

Some participants explained that access to tools that detect attacks is crucial. The Singaporean government is creating a subsidized public service to support small and medium size enterprises with tools and software. It was emphasized that ASEAN faces uneven development across countries, and that many countries still lack basic capabilities. An emphasis on in-country training could address or offset some of these limitations and build trust.

In the context of the Russia-Ukraine war, attacks from state or state-sponsored actors targeting critical information infrastructure, including potential cyber surprise attacks in combination with physical/kinetic strikes, represent a newly demonstrated threat frontier. Coupled with the increasing use of AI-driven cyber attacks, it was agreed that all parties must make considerable efforts to ensure cybersecurity.

One participant outlined how Southeast Asia's geographic position in the context of great power competition makes it increasingly vulnerable to state-driven cyber activity, particularly intelligence collection and espionage in cyberspace. The region's proximity to and the rising recognition of the global economic importance of the South China Sea have corresponded with a significant buildup of "advanced persistent threats" against Southeast Asian targets.

Many attendees identified information sharing – at the regional, national, and cross-sectoral levels, as a key challenge for governments, law enforcement, civil society, and the private sector. Some participants reported on successful efforts to patch vulnerabilities and make arrests based on shared information within the region. Bridging gaps in national policy, regional cooperation, and multistakeholder engagement is becoming a new normal in day-to-day efforts, and threat and vulnerability reporting, tracking, and aggregation continues to improve within the region. Many participants agreed that making information sharing policies more robust should be a regional priority.

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 discussed 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.

Opening remarks for the session were provided by Ian Lim (Palo Alto Networks), Amir Hamzah Mohd Nasir (Ministry of Foreign Affairs of Malaysia), Szilvia Tóth, Organization for Security and Co-operation in Europe (OSCE), and Lea Kaspar (Global Partners Digital).

Participants mentioned that the UN Open-ended Working Group on Security of and in the use of ICTs (OEWG)'s current negotiations and discussions on establishing a point of contact directory represent a positive outcome in the global system. However, they emphasized that ASEAN has had its own POC directory in place and operational for several years. Some participants pinpointed the benefits of analyzing both OSCE and ASEAN confidence building measures, including the structure of informal working groups and the public resources that were available, including the OSCE's e-learning, training, and incident classification.

ASEAN has much to offer in international settings for sharing lessons learned for implementation. Attendees laid out the benefits that internal conferencing, training, drills, and cooperation have had on confidence and trust among governments in Southeast Asia. Some participants accentuated that internal conversations within ASEAN need to focus on identifying the key elements of the region's experience. These can be extrapolated to form lessons learned from their regional efforts to the OEWG or the Ad Hoc Committee to aid the global experience.

Multiple attendees made the case for the importance of speaking in multiple "languages" to improve comprehension across diverse political, diplomatic, technical, business, academic, and civil society approaches to cybersecurity to build confidence. Similarly, participants affirmed the benefits of fostering cross-regional dialogue, particularly South-South dialogue.

From a diplomatic and technical perspective, some participants emphasized the genuine achievement of the ASEAN regional Computer Emergency Response Team, or CERT, but also acknowledged that ASEAN members were only as strong as the lowest common denominator on cybersecurity. The importance of cooperation between public and private organizations to build trust toward positive outcomes is critical. From a citizen's level, the importance of developing cyber literacy and safety was highlighted.

One participant argued that the diversity of private sector cybersecurity solutions can create unmanageable complexity. Organizations buy a specific tool for a specific security problem, but this leads to fragmented systems implementations, which can lead to fragmented state policies. Another participant mentioned that some private sector firms recommend a "mesh architecture" approach to security defined by Gartner, "as a composable and scalable approach to extending security controls, even to widely distributed assets," and that how to shape security architectures remains challenging.

With respect to multistakeholder engagement and trust building, the situation has improved over the last decade. Increasing awareness of the need for CBMs, the critical role for civil society, CERTs, think tanks, and other institutions is more widely acknowledged. Civil society and governments have made progress in their approaches to cyber challenges, by developing stronger connections and communications. Today, many training or operational practices are in fact CBMs, but not explicitly labeled as such as they become institutionalized and accepted.

However, multiple participants made the case that more is needed, including: institutionalizing embedded dialogue; improving follow up; ensuring diversity and inclusiveness; building tangible links to formal UN processes; and, ensuring that multistakeholder participation does not stop with experts, but includes local communities in order to address a democratic deficit of institutions. Participants emphasized the importance of creating centers of excellence in every ASEAN member state for community engagement to build out the human capital required to sustain trust building. The ASEAN Regional Forum's format as a "mini-UN" led to action-oriented discussion on trust building. Some participants felt the OEWG currently lacks that impetus, due to combative remarks among the permanent five members of the UN Security Council. Some attendees advocated that Southeast Asian societies should maintain lines of communication and have open and candid discussions to preserve digital security. Establishing a workflow of incident sharing mechanisms and early warning mechanisms at the practical level are fundamental objectives still underway.

Trust building and capacity building are "two-way streets" and leading actors need to be mindful that multiple approaches are required for cybersecurity efforts. In addition, several attendees described how humanitarian institutions have been targeted globally, emphasizing the importance of combating "hackers for hire," whilst increasing incentives for vulnerability disclosure and sharing.

One problem discussed at length was the pathway to ensure that larger, diverse groups have access to high quality resources. For example, municipalities should pool funds and leverage shared resources on a prorated basis. Meanwhile, states need to provide support to chief security officers from the public sector and recognize that no civil society organizations have the budget to defend against nation-state level resources or attacks. The importance of the concept of "free" cyberspace was noted – pointing out that it is not free in terms of cost or infrastructure, and that costs must be borne to ensure trust.

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 (PPPs) 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 began with remarks by Kathleen Bei (Global Forum on Cyber Expertise), Michael Karimian (Microsoft), Charles Ng (Ensign InfoSecurity), Phannarith Ou (Ministry of Post and Telecommunications of Cambodia), and Nynke Stegink (National Cyber Security Centre of the Netherlands). The introductory speakers focused on specific examples of successful public private partnerships from within and outside the cybersecurity field and urged participants to think of whole ecosystems when considering structure of partnerships.

An example ecosystem worth highlighting was that of Talking Traffic, an initiative created by the Dutch government, an infrastructure service that facilitates data exchange between roadusers and intelligence infrastructure. By using actual data, the negative effects of traffic mobility were reduced. This public private data-chain approach started with government subsidiaries but also included mutual investments by private enterprises. This system of adding info via data sharing and then allowing withdrawal of it, i.e., "You get out what you put in," allowed for better access and implementation of public services. One participant advocated that such a circular approach ensures equity trust, and, critically, such reciprocity will be helpful for governments to ensure effective PPPs in cyberspace.

Other effective public private partnerships on the global cyber diplomacy side that were detailed included the Paris Call for Trust and Security in Cyberspace, Let's Talk Cyber, the Cyber Threat Alliance, Cybercrime ATLAS at the World Economic Forum and the Cybersecurity Tech Accord.

Overall, in ASEAN, while there are some successful public private partnerships, the engagement process needs more time and collective effort. From the private sector perspective, firms face challenges in terms of funding horizontal sharing of intelligence data – including cross border data. One participant argued that there is a challenge in financing public goods that are required for the community to maintain cybersecurity, but actors like non-profits or homeowner associations struggle to identify what specific product or service they should procure to protect themselves. Several participants pointed out that firms have a role to play in providing a "safe space" for chief security officers to share best practices and telemetry on threats.

The discussion also included considerations for less developed countries (LDCs), which included raising awareness about cybersecurity, building up CERT capacity (through public private task forces and information sharing) and establishing national strategies. On the other hand, it was also emphasized that states with minimal resources face challenging choices between investing in public infrastructure and facilities such as hospitals, schools, and roads. These all weighed against building additional cybersecurity capacity. Moreover, resource commitments, national willingness, and the relatively small scale of commercial market opportunities contribute to an environment where companies are less likely to engage. In this situation, knowledge transfer becomes essential to ensuring that developing states have an opportunity to shape their own cybersecurity futures.

Several participants detailed the important role of the Global Forum on Cyber Expertise (GFCE) in providing information, capacity building, and matchmaking between different parties to enhance cybersecurity. One of the key ideas put forward was that actors in the Global South offer different perspectives and approaches, that have proven valuable because they do not represent long established players within the ICT system. These perspectives stimulate policy brokering within and among public private partnerships and international negotiations, with particular emphasis on the importance of multistakeholder efforts.

Multiple attendees outlined that ASEAN as a region does have a number of Track 1, 1.5, and Track 2 initiatives, including ministerial engagement through the ASEAN Digital Ministers Meeting, coordination through the ASEAN Cybersecurity Coordinating Committee (Cyber-CC), the Council for Security Cooperation in the Asia Pacific, the ASEAN Regional Forum (ARF)'s Inter-Sessional Meeting on ICTs Security , the establishment of three Cyber Centers for Excellence (including a new center announced through the ASEAN Defence Ministers' Meeting (ADMM) in July 2023, titled the ADMM Cybersecurity and Information Centre of Excellence). However, many participants emphasized that more needs to be done in this area, particularly to ensure equitable, inclusive, and multistakeholder engagement. The International Telecommunication Union's Cyber for Good program was put forward as another model. The UN-Singapore Cyber Fellowship Programme and the Women in International Security and Cyber Fellowship were put forward as examples for encouraging diverse perspectives. At the national level, additional efforts to build diversity and inclusion are underway. For instance, a focus on women's engagement in cybersecurity in Indonesia, where notable progress has been made in training, mentoring and leadership programs, and public private partnerships can drive funding.

Several states have recently adopted new national cybersecurity plans, which took in multistakeholder input, but still face challenges in implementation across sectors. For example, in energy security, and for efforts to address human trafficking, online sexual abuse, and exploitation of children. These all require cooperation from Internet service providers and telecom providers to ensure successful outcomes.

Finally, participants commented on challenges in workforce and brain drain, including in areas of corporate cybersecurity, critical information infrastructure protection, and instruction. Ensuring academic curricula better position students to enter the cyber workforce. Partnerships to address imbalances in expertise and job security between the public and private sector in cyber will be essential for the region moving forward.

Continuing to Strengthen Southeast Asian Contributions at UN and International Cyber Discussions

This session opened with remarks by Platima Atthakor (Ministry of Foreign Affairs of Thailand), Bart Hogeveen (Australian Strategic Policy Institute), Huu Phu Nguyen (Ministry of Foreign Affairs of Vietnam), and Farlina Said (Institute of Strategic and International Studies Malaysia).

ASEAN generally has made steady improvement in making contributions at the UN OEWG for ICTs and the Ad Hoc Committee on Cybercrime to the point that the practice of UN interventions has been normalized. Participants felt that Southeast Asian governments and stakeholders are well-positioned to contribute to the UN because ASEAN member states are interested in developing capacity and addressing threats. ASEAN also has tangible experience in enacting effective multilateral CBMs and cooperation, which could further add to the conversation at the UN. In addition, numerous participants emphasized that international law applies in cyberspace.

Many ASEAN members are active in the Ad Hoc Committee on Cybercrime established in May 2021. The importance of the process and the transparency of its execution was highlighted. Some participants voiced skepticism that the current timeline for reaching a final text could be achieved, but remained hopeful that differences on key issues such as scope and terminology and the use of ICTs for criminal purposes could be overcome in time. Detailed discussion covered cyber-enabled versus cyber-dependent crimes, the Budapest Convention on Cybercrime, human trafficking, sexual abuse, and the danger of politicization within the Ad Hoc Committee on Cybercrime. There was also discussion of the risk that youth exposed to the possibilities of cybercrime could be recruited by malicious organizations, a scenario that the Thai government is working proactively to prevent. The Netherlands referred to a best practice in this regard, the Cyber Offender Prevention Programme that is run by the Dutch National Police. In this program the police work together with private companies, public sector and teachers to make youngsters more aware and inform them about what is illegal and what are consequences.

With respect to the OEWG, participants pointed out that Southeast Asian governments' engagement with the First Committee processes was initially low, but has risen over the years, including increased participation by ASEAN member states at recent meetings of the UN OEWG. For example, the 2017 First Committee process failed to reach consensus on key issues – but ASEAN did. ASEAN diplomats have begun to consistently feed inputs into the system. Moreover, the process of making interventions has forced states to begin conversations among relevant agencies, so that diplomats can frame a common position without referring to their capital retroactively. That said, one participant expressed that the burden now rests with the capitals in many areas. With no shortage of multilateral dialogues (ARF, CSCAP, ADMM+, ASEAN), participants pointed out that this requires governments to be more forward leaning and trusting across different communities. While a public point of contact directory is coming to the UN and an attribution framework may also emerge – it remains an open question (including for ASEAN governments) whether this framework and responsibility should rest solely with government. Challenges remain in integrating and sustaining multistakeholder engagement in the OEWG and Ad Hoc Committee and ensuring that states follow through on the practical implementation of agreed norms and principles.

Multiple participants underscored that multistakeholder engagement, where governments listen and absorb inputs from private sector, civil society, and academia, will be essential to formulating a durable and legitimate approach to norms implementation and action. One participant shared that the speed of adoption of emerging technology has forced regional governments to understand what it does to the ecosystem strategically. The primary method of gaining that information is through multistakeholder dialogue. One participant suggested that cooperation on standards represents a key area for engagement through UN and regional processes, and that future dialogues should address this issue in greater detail.

That said, several attendees stressed that prioritization is essential, given that even mature economies struggle to grapple with all of these challenges, and ASEAN has diverging levels of economic development. Nevertheless, key challenges like perspective and approach (urban centric vs rural centric, government services, civil society amplification, data protection and digital rights) require consultation because of their importance and the diversity of perspectives across the region.

Finally, the geopolitical dynamics of international cyber dialogue were noted. One participant reiterated the desire for developing countries to avoid outright disagreement with powerful states like Russia and the United States, so that retaining flexibility and finding common ground were important.

Concluding Remarks

Maartje Peters (Head of the Taskforce International Cyber Policies at the Ministry of Foreign Affairs of the Netherlands) provided concluding remarks and summarized key themes across the dialogue, including advancing multistakeholderism, sustaining commitments, and maintaining genuine dialogue and knowledge sharing. She articulated that middle powers have insights and can play an important role in constructive dialogue and digital rebalancing. With the challenges governments face in handling malicious actors in an environment animated by the war in the Ukraine, ASEAN states must work to ensure that donor governments remain focused on developing international networks of experts, protecting critical infrastructure, and building capacity, in order to ensure preserving an open, free, inclusive and secure Internet and cyberspace.

Subsequent concluding discussion among small groups of participants identified the following key takeaways and areas for potential future projects and research.

Assessing the Emerging Threat Landscape in Cyberspace

- Southeast Asian governments and societies need to monitor and address new threat trends including AI-assisted attacks, sophisticated ransomware, hackers-for-hire, and the heavy specialization among cyber criminal enterprises within ASEAN's regional threat landscape in cyberspace.
- Regional governments and private sector organizations should ensure that portals for vulnerability disclosure and threat intelligence sharing are available, responsive, incentivized, and acted on.
- Regional corporate and government planning should match the reality that chief security officers (CSOs) and chief information security officers (CISOs) of corporations and organizations lack the resources and infrastructure to combat state driven cyber attacks. Given the increasing number of these state driven attacks, next steps should include providing access both to tools that detect attacks and to information sharing portals to raise situational awareness.

Promoting Cooperation Through Cyber Confidence Building Measures

- Effective regional cyber capacity building requires a funder, a local partner, and an implementer in tight coordination. In addition, on ground integration of cybersecurity expertise within government agencies or partner organizations, leads to the most durable training, capacity enhancement, and trust building. Informal communication channels developed during such training can also be highly effective during a crisis.
- When engaging with international partners and organizations in capacity and confidence building for the region, ensure that training is tied to specific operations, public policy outcomes, or business achievements. This can aid in overcoming sustainment issues and aid results-driven evaluation.
- Ensuring cybersecurity for critical infrastructure and critical information infrastructure requires sustained investment and support over the life cycle of the infrastructure. Distilling the best models and lessons to achieve this will be essential from partners like the OSCE as well as ASEAN's own experience. Ensuring that national frameworks and strategies are not overly insular in their outlook and scope allows for better channels of collaboration and information sharing.

- Southeast Asian governments should continue to build mechanisms for knowledge transfer to members with fewer resources to ensure societies can shape their cybersecurity futures and enhance collective confidence.

Creating and Engaging with Public Private Partnerships

- Public private partnerships should be structured with reciprocal arrangements - "You put in as much as you take out" - to ensure buy-in and equity among different partners. Partnerships should reflect the elements of the given cyber ecosystem, and governments need to commit funds to ensure viability.
- With a wider variety of crucial ecosystems, Southeast Asian governments should enhance interagency cooperation and communication internally, as well build formal and informal channels to other actors plugged into relevant crucial ecosystems.
- Organizations with multistakeholder conscious approaches to cybersecurity, e.g. the Forum of Incident Response and Security Teams (FIRST) framework, should be studied and emulated to identify key fundamentals to incorporating a variety of stakeholders (government, private sector, civil society, local communities, and academia) into practical, action-oriented agendas to form effective partnerships.
- Vulnerable groups of smaller, diverse entities, such as municipalities or associations, should pursue creative ways to pool funding for cybersecurity protection by unifying their efforts and then leveraging prorated services.

Continuing to Strengthen Southeast Asian Contributions at UN and International Cyber Discussions

- The experience of ASEAN's institution building, capacity enhancement, and regional cooperation provides a framework of lessons learned that can aid other regions in the Global South in their efforts to ensure cybersecurity, cyber stability, and public safety.
- Ensuring that regional governments continue to have the confidence and diplomatic flexibility to engage with external actors is essential - whether in vulnerability disclosure, negotiations, or problem solving.
- ASEAN members should hold preparation meetings ahead of substantive OEWG or Ad Hoc Committee meetings for policy coordination and consensus building. These meetings should also embrace multistakeholderism to capture input from a variety of key Southeast Asian perspectives, and target specific areas of input, for example ASEAN's experience with confidence building measures and a regional point of contact directory.
- Striving for responsible state behavior in cyberspace requires not just agreement but implementation and continual practice. Maximizing thoughtful contributions by regional governments and multistakeholder organizations (local and global) to these international negotiations and discussions will support broader norms adoption and implementation.

These results of the small group discussions indicate that the Dialogue succeeded in providing deep insights and generating meaningful discourse among the participants on all of the topics. They also illustrate that much further work needs to be done in building cyber policy in Southeast Asia, on the part of all stakeholders (government, private sector, civil society, local communities, and academia).