Global Cyber Policy Dialogues: Southeast Asia

August 6, 2020
07:00 CEST/13:00 SGT

MEETING SUMMARY

EastWest INSTITUTE

RSiS S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

Ministry of Foreign Affairs of the Netherlands

CSR SINGAPORE

On August 6, the EastWest Institute (EWI) and the S. Rajaratnam School of International Studies, in partnership with the Ministry of Foreign Affairs of the Netherlands and the Cyber Security Agency of Singapore, hosted the virtual Global Cyber Policy Dialogues: Southeast Asia meeting. Meeting participants addressed challenges to building a secure, safe and resilient cyberspace in Southeast Asia during the COVID-19 pandemic, emphasizing emerging technologies, the current international cyber norms processes and priorities for the Association of Southeast Asian Nations (ASEAN) states.

This event is the first in a series of planned Global Dialogues being undertaken by EWI, aiming to convene regional meetings to address capacity building around key cyber challenges. The initiative is intended to complement the two ongoing UN cyber norms processes: the Open-Ended Working Group (OEWG) and the Group of Governmental Experts (GGE), and seeks to convene discussions that go beyond exchanges among like-minded stakeholders to ensure the representation of a broad range of views and solutions at international fora and processes. This virtual meeting, along with future meetings focusing on other regions, are laying the groundwork for in-person events currently planned for 2021.

The August 6 Southeast Asia meeting featured four speaker presentations on emerging technologies, UN norms processes and capacity building, followed by a roundtable discussion with participants representing governments, businesses, civil society organizations and universities from Southeast Asia and beyond. The following sections briefly summarize each of the speaker's presentations and characterizes the main points from the discussion, which took place under the Chatham House Rule. The meeting was moderated by Bruce W. McConnell, Interim President, EastWest Institute.

LEVERAGING EMERGING TECHNOLOGIES FOR A MORE SAFE AND SECURE CYBERSPACE
David Koh, Chief Executive, Cyber Security Agency of Singapore

The COVID-19 pandemic has shown how important digital technologies are in ensuring that essential services and governance can continue in a highly disrupted environment. Lockdowns have fundamentally changed the way people live, and digital technologies have allowed workforces to cope. But with this reliance come new vulnerabilities, driven by a massively enlarged attack surface for malicious actors and a rush to ensure connectivity without adequate consideration for security.

Emerging technologies are disruptive, but they can also provide solutions to better secure cyberspace. They can also be a double-edged sword. Technologies such as the Internet of Things (IoT) and artificial intelligence (AI) algorithms can enable early detection and swift action to deal with threats, but malicious actors can also take advantage of the new vulnerabilities produced by these technologies or even use them to speed up attacks. Singapore intends to implement a cybersecurity labelling scheme to help users make informed choices about the security features of IoT devices which should, over time, incentivize companies to improve them.

However, technology is only one part of the solution. There is a need to sustain a rules-based international order to advance security, cooperation and trust. Both the United Nations GGE and OEWG are actively discussing these issues and it is important that such discussions continue to be hosted at the UN, where all countries, big or small, have a voice. ASEAN has also been taking positive steps on this front: the Fourth ASEAN

Ministerial Conference on Cybersecurity set up a working group to outline a path for implementing the UN GGE norms. Given the disparity in capability within ASEAN, there is an urgent need for cyber capacity building efforts at both the policy and technical levels so that countries can implement the rules and norms that advance peace and security in a hyperconnected cyberspace. Cybersecurity threats do not respect borders and we are only as strong as the weakest link.

CURRENT DEVELOPMENTS TOWARDS NORMS-BASED CYBERSECURITY
Carmen Gonsalves, Head, International Cyber Policy, Ministry of Foreign Affairs of the Netherlands

There is a growing sense of urgency to work for a rules-based order in cyberspace to help counter the growing challenge of cyber insecurity. The Netherlands is strongly committed to the UN norms processes and puts a strong emphasis on capacity building to help tackle these issues.

To start, the Netherlands has launched a network of cyber diplomats to deepen engagement globally. Actions in cyberspace force us to think about our core values as both nations and humans. Questions about priorities in these values have arisen in public debates, such as the balance between privacy rights and collective rights like public safety when creating COVID-19 tracing apps.

Mitigating cyberspace threats is not just a technical problem; it is a policy and normative challenge. The UN GGE has taken the important step of noting that international law is applicable to cyberspace, as well as acknowledging that there is a need for more capacity around the globe. The current GGE and the OEWG are taking these discussions even further. The GGE will continue to push beyond its 2015 consensus report to drive the conversation forward, while the OEWG will deepen the implementation of existing UN agreements and bring in new perspectives.

In the OEWG, the Netherlands has raised a proposal to protect the public core of the Internet to ensure its general availability and integrity, which is currently threatened by cyber operations. The Netherlands has also sought the same protection for the technical infrastructure supporting and enabling elections. The Netherlands is not alone in introducing and supporting measures to build a norms-based cyberspace however, and multistakeholder engagement is necessary to build the stability and security required for cyberspace to function.

ASEAN CYBER CAPACITY BUILDING PRIORITIES AND THE RELEVANCE OF UN NORMS PROCESSES
Elina Noor, Visiting Fellow, Institute of Strategic and International Studies Malaysia

The UN norms processes, particularly the OEWG, have been valuable in raising awareness and bringing diversity to conversations about cyber norms. While different opinions often seem to muddle the threat landscape, the discussion at the OEWG brought useful insights because of the inclusion of multistakeholder perspectives. The OEWG gives all states a chance to register interest on important and still nascent discussions which will also likely affect the agenda of the GGE.

For ASEAN to take full advantage of these discussions, members must know what they want. If capacity building is intended to be demand driven, as it should be, then goals must be driven by the priorities of the countries receiving help. So what is ASEAN's agenda in cyberspace? It strives to be a connected, innovative, inclusive, integrated and resilient community. Its priorities can be boiled down to four C's: cyber crime, content, critical information infrastructure and connectivity. These last two are increasingly becoming a

concern due to Fourth Industrial Revolution development projects. These involve not just the private sector, but also ASEAN partners that may not always see eye to eye, especially on technology, security or norms issues.

ASEAN is a prime area for geo-technological contestation, which makes it a frontline for geopolitical competition. Thus, it is imperative that Southeast Asian countries are able to independently decide their own positions on how international law should apply in cyberspace. Many of the legal traditions in ASEAN countries are colonial hold-overs and as younger nations, they have tended to accept many international concepts as a given. However, these concepts need to be unpacked in light of disparate historical and legal contexts to bring more diversity to international conversations. International law is an interplay of rules, policies, politics and power. The UN processes allow a glimpse into how these will play out, but rules are already being made by state practice, especially that of more powerful states. Capacity building is a great start, but there must be a diversity of opinions and practices reflected in the process.

PUBLIC-PRIVATE PARTNERSHIPS AND THE FUTURE OF CYBER CAPACITY BUILDING EFFORTS
Chris Painter, President, Global Forum on Cyber Expertise Foundation

Countries have been racing to create digital economies and infrastructure for some time, with little regard to security. This has been changing lately with new initiatives such as the previously mentioned Fourth ASEAN Ministerial Conference on Cybersecurity. However, cybersecurity has not been mainstreamed as one of the key issues of national security, foreign policy and economic security in high-level political discussions, possibly because it is harder to grasp than other economic concepts. COVID-19 has altered the landscape however, as countries around the world have learned the full extent of their dependence on these technologies and where exactly their vulnerabilities lie.

Another observation is that although all countries, including ASEAN states, naturally have different levels of cybersecurity, every country needs to be up to a minimum standard. These processes will be richer if all countries have the cyber capacity to elaborate their own perspective and create their own goals. Many countries list capacity building, a commonly addressed theme in these discussions, as one of their key issues; though often characterized as low-hanging fruit, capacity building is made up of many components and is quite complicated. On the policy side, there are national cyber strategies: the key foundational element that outlines priorities for cybersecurity capacity building. Ideally, these should be built from a multistakeholder process, involving voices from outside the government. On the institutional side, there are computer emergency response teams (CERTs) and cyber-diplomatic corps that can be built up to participate in these processes.

The Global Forum on Cyber Expertise ("GFCE"), originally a Dutch initiative which is now an independent foundation with over 130 members and partners around the world, is designed to deal precisely with these many different components of capacity building. Its core mission is to coordinate cybersecurity capacity building around the world, a critical process as there are very limited resources devoted to ensuring harmonization in capacity building efforts. This coordination is done primarily through a clearinghouse process (matching countries who need capacity building with resources that can provide it), a portal containing global best practices, a global research agenda, meetings and working groups.

DISCUSSION

Following the presentations, the floor was opened to the participants for questions and general discussion. Participants quickly turned to the role COVID-19 has played in the cybersecurity landscape, noting that it has raised awareness about security issues and highlighted existing trends. In particular, the pandemic has

impressed upon leaders, including in the private sector, the need for basic cyber hygiene. Concerns were expressed that this intense interest would fade as the crisis subsides, as it usually does following major cyber incidents.

Participants were also eager to discuss practical methods of achieving consensus on the issues of creating a norms-based cyberspace. In particular, they noted the desirability and practicality of focusing on specific questions in the international discussion first before moving onto larger questions. They also advocated a regional approach to solving practical cybersecurity problems. For example, Southeast Asia could focus on the issue of cyber crime, given that capacity exists within the region, and apply lessons-learned globally. Finally, the importance of a multistakeholder approach and the value of civil society perspectives were discussed, both for efforts at the regional level, as well as in the context of the UN norms processes.

CONCLUDING REMARKS

Shashi Jayakumar, Senior Fellow and Head of Centre of Excellence for National Security, S. Rajaratnam School of International Studies

Reflecting on the discussion as the meeting drew to a close, questions were raised about the viability and relevance of UN discussions on cyber norms in the current context. As many speakers pointed out, the current landscape is one of cyber insecurity. Cyber crime and malicious activities are on the rise, major cyber powers are implementing doctrines such as “Defend Forward,” which can undermine trust, and furthermore the priorities of many countries, including those in ASEAN, are not necessarily reflected in the international discussions.

The international community is faced with the prospect that progress on international cyber norms will take years; as a result, the most pressing issues at the end of the processes may not be the same as those identified in current discussions. There is a disconnect between the issues given priority in international cyber norms conversations and the issues of most concern for ASEAN (and other) countries. This highlights the importance of having discussions that include more diverse stakeholders and go beyond exchanges among like-minded states. The resulting diversity of opinions would ensure fair deliberation on what constitutes a cyber issue, increasing the likelihood of lasting global agreements in cyberspace.