GFCE

Global Forum on Cyber Expertise

GFCE Southeast Asia Regional Meeting

7 October 2021 | REPORT

The Global Forum on Cyber Expertise (GFCE), in collaboration with Cyber Security Agency (CSA) Singapore, held the inaugural GFCE Southeast Asia Regional Meeting on Thursday 7th October 2021 in the margins of Singapore International Cyber Week (SICW) 2021. This regional meeting brought together over 90 stakeholders from the GFCE community and ASEAN to identify opportunities and challenges for cyber capacity-building in the region and share good practices and knowledge. The session sought to provide an overview the cyber capacity-building landscape in Southeast Asia as well as discuss collaborative opportunities to enhance coordinated capacity-building efforts in the region.

1. Opening Session

David Koh, Commissioner of Cybersecurity and Chief Executive of the Cyber Security Agency (CSA) of Singapore, opened by highlighting that the OEWG and GGE discussions concluded earlier this year have spotlighted capacity building: raising awareness and stressing its importance. He announced that the GFCE Southeast Asia Regional Meeting will be hosted annually in the margins of the SICW, keeping capacity building on the agenda of this important cybersecurity event and ensuring continuity in our engagement with stakeholders in the region.

Chris Painter, President of the GFCE Foundation Board, highlighted the importance of cyber capacity building globally and within the region. He pointed out that as ASEAN member states have increasing placed an emphasis on cybersecurity, placing trust in information and communications technology (ICT) infrastructure, the GFCE reaffirms its commitment to strengthening engagement and better coordination of capacity building efforts in the region.

2. Opening Panel: Cyber Capacity Building Landscape in Southeast Asia

Chris first asked the panel if ASEAN is moving towards a more collaborative and coordinated effort in cyber capacity building, and what the future of cyber capacity building in the region may look like.

Shashi Jayakumar, Head of Centre of Excellence for National Security, S. Rajaratnam School of International Studies, remarked that there are several critical forums within ASEAN for cooperation on cyber capacity building. He highlighted the ASEAN Ministerial Conference on Cybersecurity (AMCC), ASEAN Regional Forum (ARF), ASEAN Defence Ministers' Meeting (ADMM), ADMM-Plus and ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE). Moreover, **Shashi** pointed to the fact that, despite some coordination of efforts, ASEAN member states have different priorities and needs regarding cyber capacity building, as is reflected by the fact that some states namely Singapore and Malaysia have dedicated cyber agencies, whereas other ASEAN members work on cyber issues within other departments such as justice and police. He notes that it will be interesting to see if states move closer to the cyber agencies model or continue to address cyber needs in various state departments.

Naveen Menon, President, Cisco Systems (ASEAN), pointed out that moving forward, policymakers need to work hand-in-hand with industry and continue the good work of groups such as the US-ASEAN Business Council which runs regular digital policy consultation forums, bringing together key industry experts and policy makers to discuss cybersecurity issues.

Le Quang Lan, Assistant Director of the ICT & Tourism Division and ASEAN Economic Community Department at the ASEAN Secretariat re-affirmed **Naveen**'s point that public-private partnerships and cooperation between government and industry should be promoted. Moreover, he points out that ASEAN is indeed moving towards a more cooperative effort on cyber capacity as the ASEAN Cybersecurity Cooperation Strategy is due to be implemented by 2025. **Lan** believes it is important to develop and support interoperable standards for businesses, people, and governments to work in tandem in the region. Additionally, Lan highlighted the importance of assessing country's individual capacity to coordinate progress, pointing to the CMM as a useful tool globally but particularly for this region. Alongside this, ASEAN members should continue to strengthen cooperation between CERTs such as what is being done through the ASEAN CERT drills.

Naveen added that in order to achieve these goals in cyber capacity building, training programs within the region need to be amplified to ensure a skilled cyber workforce. This should include tertiary education, engaging the tech industry to inform and support training, and bringing practitioners from other regions to share knowledge and expertise to tie in the regional with global expertise as cyber capacity building is a global effort. **Chris** adds that the merging of regional and global approaches can be assisted by the GFCE as it is a global forum with a regional focus as part of its strategic approach.

Chris then asked the panel how needs in ASEAN are being addressed, in light of the fact that needs-driven initiatives is a key pillar of cyber capacity building, and what the challenges are for the region.

Shashi explained that the needs of the region can only be honestly addressed when members come together to discuss these issues with a neutral convening party, which has become increasingly difficult in recent years. He speculates that perhaps Singapore as a leader in cyber capacity building in the region, or neutral think tanks, could remedy this challenge by acting as a neutral party to reconvene discussions.

Lan highlighted that taking a needs-driven approach is imperative for Southeast Asia as it enables the prioritization of limited resources. He points out that, in addition to the aim to conduct CMM assessments to identify needs on the national level, there are two mechanisms currently in use on the regional level to ensure a needs-driven approach. Firstly, Global Cybersecurity Index which identifies gaps in technical, institutional and legal capabilities among ASEAN member states, highlighting which states require more support. Secondly, the ASEAN Digital Integration Index: an evidence-based measure of progress towards the ASEAN Digital Integration Framework, which utilises data protection and cybersecurity as an indicator. This index reveals that a region-wide issue is the lack of technical capabilities.

Naveen re-affirmed **Lan**'s point that the ASEAN CMM is a tremendously important initiative that will give strategic direction all ASEAN member states to implement needs-driven policies on the national level. Moreover, the CMM should touch upon all factors of national cyber elements, such as governance, legislation, technical measures, accreditation, international cooperation, and capacity building, to paint a full picture of the region's needs.

Shashi noted that, in the past, implementing agencies in the region rarely focused on this needs-driven approach but that presently, this is changing as more needs assessments are being conducted prior to beginning capacity building projects. The lack of needs assessments or research into local contexts has posed a challenge for the region, and this should be avoided in the future by maintaining focus on local needs.

3. Presentation of GFCE's work & Overview of CCB efforts in Southeast Asia

Marjo Baayen, Director of the GFCE Secretariat, presented the GFCE's global strategy in coordinating the strengthening of cyber capacity building. She emphasized the GFCE's prioritization of its regional approach as it assists the identification of capacity needs which are translated into specific activities, in line with the GFCE's efforts to promote a demand-driven approach.

Robert Collett, Independent Researcher and Consultant for Cyber Capacity Building, presented the Cybil Knowledge Portal and an overview of cyber capacity building efforts in the region specifically. He highlighted that every country in ASEAN has benefitted from international knowledge and skill sharing projects, but Indonesia and Vietnam are the most represented beneficiaries in projects on the Cybil Portal, with 33 and 27 projects respectively. Moreover, regarding the themes addressed in the region's projects, most projects address Strategy, Policy and Cyberdiplomacy (34%), followed by Critical Information Management and Critical Information Infrastructure Protection (23%), Cybercrime (20%), Culture and Skills (18%) and Standards (8%). However, Robert emphasised that this analysis focused only on data available on the Cybil Portal and thus may be incomplete.

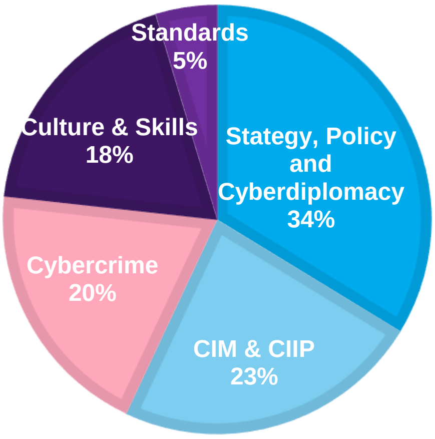

Figure 1. The distribution of projects in Southeast Asia by GFCE themes, based on data from the Cybil portal.

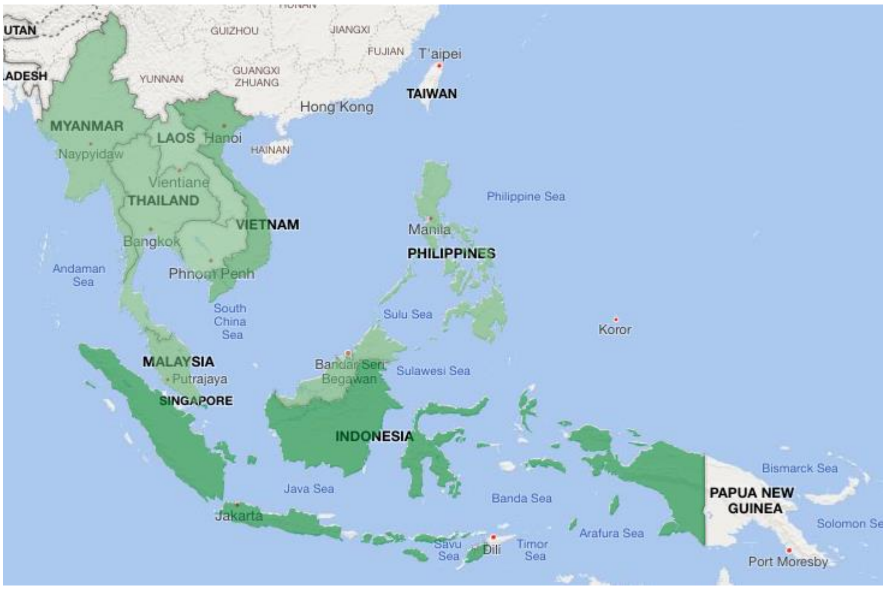

Figure 2. Indonesia and Vietnam have the most projects in Southeast Asia, based on data from the Cybil Portal.

4. Breakout Room Discussion: Capacity Building Needs & Coordination

The breakout rooms discussions were moderated by **Elina Noor**, Director of Political-Security Affairs and Deputy Director of the Washington, D.C. Office at the Asia Society Policy Institute, and **Bart Hogeveen**, Head of Cyber Capacity Building at the International Cyber Policy Centre of the Australian Strategic Policy Institute. The participants discussed whether or not the picture painted by **Robert** in the previous presentation offers a representative and comprehensive picture of CCB in SEA and what opportunities there are for multi-stakeholder collaboration.

Elina began by reviewing some key takeaways. She highlighted that it was discussed that ASEAN member states are focused on 'low hanging fruit,' namely focusing on the practical side of implementing cyber norms such as developing skills and operationalising the 11 GGE norms. This is due to differing priorities of member states and a region-wide lack of resources. Secondly, due to efforts being focused on these low hanging fruits, there is a lack of understanding of capacity gaps at the national and regional level. This highlights the potential need for a national and regional gaps assessment to reveal the more detailed needs that lay underneath a country's high-level needs. Thirdly, there is a severe gender gap in the technical side of cyber capacity building in ASEAN, as revealed by a survey conducted by ASEAN-Japan Cybersecurity Capacity Building Centre which found that only 18% of the region's cybersecurity workforce are female. This signals that there is space in the region to empower women to gain technical and policy skills required to join capacity building efforts.

Bart re-affirmed the point that the needs of the region are not fully understood even by ASEAN member states themselves, and this is reflected by the fact that those participating in discussions pertaining to capacity needs are often times implementing agencies rather than the states themselves who are on the receiving end of assistance. In addition to this, a key question is how forums such as the GFCE can arrange for frameworks for capacity building whereby needs are properly identified and the impacts and capacity assessments are monitored for progress. This is important as, particularly in Southeast Asia, this assessment of impact has yet to be done. Secondly, a portion of cybersecurity training and upscaling is being done on-the-job, which is not currently captured in existing statistics on training within industry. Thirdly, it was articulated that those working in cybersecurity or cyber capacity should be trained to understand both the technical and policy aspects and thus be 'bilingual' in this context.

5. Closing Panel: Key takeaways and way forward for the GFCE

Chris posed the question: how can the GFCE help facilitate cyber capacity building in the region? **Bart** explained that the GFCE as a neutral forum could bring together different stakeholders such as practitioners, cyber capacity experts and recipient countries, as it did for the Southeast Asia Regional Meeting 2021, to discuss the region's needs and coordinate efforts. Thus, the GFCE would facilitate the needs articulation by local stakeholders. **Elina** pointed out that the GFCE's role in coordinating research on knowledge gaps facilitates the region's understanding of their capacity gaps and subsequent best practices.