Elevating ASEAN Australia Cyber Security Cooperation to the Next Level

ASEAN-Australia Relations / By AASYP

AAYLF delegate from Indonesia Aditya Arnanda examines the role that governments and private actors play in addressing the increasing cybersecurity threats in the region.

ASEAN-Singapore Cyber Security Centre of Excellence (ASCCE): Australia's role in capacity building

The ASEAN centre for capacity building in cyber security (ASCCE) will be opened in the second quarter of 2020 in Singapore, the region's most advanced cyber nation according to Global Cyber Security Index by ITU [1]. Australia, as the first dialogue partner of ASEAN along with other countries such as the United States and the United Kingdom have shown their commitments to engage with the centre [2]. Although the list of participating countries seems reassuring, it is not adequate. The private sector should be invited to play a role in the centre.

Australia's Ambassador for Cyber Affairs, Tobias Feakin has recognized the importance of the private sector in internet governance [3]. Australia in this regard should push the involvement of the private sector in ASEAN settings as well. It is coherent with Australia's pledge in its International Cyber Engagement Strategy to ensure the stance of private actors is represented in international forums [4]. A platform already exists of global technology companies that are committed to strengthening cyber security, namely The Cyber Security Tech Accord [5]. Cyber behemoths like Facebook, Microsoft and Cisco are signatories of this accord. According to its mission statement, signatories are ready to collaborate with initiatives aiming to enhance security, stability and resilience of cyberspace. This is precisely

what ASCCE and Australia wish to accomplish. Therefore, the idea of collaboration between signatories of the Tech Accord with ASCCE should be taken into consideration.

ASCCE's mission includes CERT-related technical training and exchange of cyber threat information. The signatories will perfectly fit for this role in accordance with their vow to work with like-minded groups to further enhance cyber security best practices.

Non-State Actors: The looming Cyber Threat

The challenge in cyberspace is constantly evolving and constructive engagement between ASEAN and Australia should be maintained. Discussion between cyber authorities since the ASEAN-Australia Cyber Policy Dialogue in 2018 has been promising [6]. The implementation of the Regional Cyber Point of Contact and Cyber Bootcamp projects are some of the onward initiatives between ASEAN and Australia [7]. However, these must be expanded to incorporate other stakeholders as well. The internet is not only a domain for governments to set rules for each other, the potential of non-state actors should also be harnessed.

Despite robust commitment in the implementation of international law and confidence building measures in the cyber realm based on 11 UNGGE voluntary norms, non-state actors will be able to jeopardize mutual trust that has been built in a cordial fashion [8]. Certain groups of people who possess the necessary expertise and tools can easily wreak havoc towards norm-abiding states. These people are commonly known as hacktivist, patriotic hackers or cyber proxies [9]. There was a precedent in 2013 where Indonesian patriotic hackers launched a DDoS attack against an Australian government website [10]. More catastrophic cyber attacks by non-state actors has previously taken place in Estonia in 2007 where the country's internet was systematically brought down [11].

Unlike kinetic wars where only armed forces own cruise missiles sufficient to hit adversaries, non-state cyber actors can simply purchase a zero-day exploit on the dark web and unleash it against digital infrastructure abroad [12]. While there has not been an Estonia-style attack against ASEAN or Australia, the risk has been and always will be there. Therefore, extended cyber policy and dialogue upon which multi stakeholders are included should be contemplated to make cyberspace safer, more secure and more stable.

References

1. ITU 2018, Global Cyber Security Index, <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf>.
2. CSA 2019, Factsheet: ASEAN-SINGAPORE CYBERSECURITY CENTRE OF EXCELLENCE (ASCCE), <https://www.csa.gov.sg/~/media/csa/documents/sicw_2019/amcc/factsheet%20ascce%202019.pdf>.
3. DFAT 2017, International Cyber Engagement Strategy – chapter overviews and messages from Chapter Champions', <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/cyber-strategy-transcripts.aspx>.
4. Commonwealth of Australia 2017, International Cyber Engagement Strategy, <https://dfat.gov.au/international-relations/themes/cyber-affairs/aices/pdf/DFAT%20AICES_AccPDF.pdf>.
5. The Cyber Security Tech Accord 2018, Signatories Objective, <https://cybertechaccord.org/about/>.
6. CSA & DFAT 2018, Joint Chairs' Statement ASEAN-Australia Cyber Policy Dialogue, <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/joint-chairs-statement-asean-australia-cyber-policy-dialogue.aspx>.
7. DFAT, Cyber Affairs, <https://dfat.gov.au/international-relations/themes/cyber-affairs/Pages/default.aspx>.
8. NATO CCDCOE 2015, UN GGE Report: Major Players Recommending Norms of Behaviour, Highlighting Aspects of International Law, <https://ccdcoe.org/incyder-articles/2015-un-gge-report-major-players-recommending-norms-of-behaviour-highlighting-aspects-of-international-law/>.
9. Maurer 2015, Cyber Proxies and the Crisis in Ukraine, Chapter 9 in Kenneth Geers (Ed.), Cyber War in Perspective: Russian Aggression against Ukraine, NATO CCDCOE, Tallinn.
10. Cumming 2017, 'Hacktivism: will it pose a threat to Southeast Asia and, if so, what are the implications for Australia?', Indo-Pacific Strategic Digest, Australia Department of Defence.
11. Ottis 2018, 'Analysis of the 2007 Cyber Attacks Against Estonia from the Information Warfare Perspective', NATO Cooperative Cyber Defence Centre of Excellence, <https://ccdcoe.org/uploads/2018/10/Ottis2008_AnalysisOf2007FromTheInformationWarfarePerspective.pdf>.
12. Rosenbach, Eric. "Keynote Address." AFCEA Cyber Con 2013. <http://www.c-span.org/video/?c4390789/keynote-address-eric-rosenbach> at 3:24.

← Previous Post

Next Post →

Tweets by @AusASEANyouth

ASEAN-Australia Strategic Youth Partnership
@AusASEANyouth

Rachel is our current Perth Hub Manager! See what she has to say about her experiences below 👇

Don't forget applications for Canberra Hub Manager, Company Secretary and AASYP Sub-editors close this Sunday 22 March! Apply at aasyp.org/apply-2020/ 💻#aasyp #opportunity