<u>**16 NOVEMBER 2023**</u>

SINGAPORE'S INPUT TO ICT SECURTY CAPACITY-BUILDING MAPPING EXERCISE CONDUCTED BY THE UNITED NATIONS SECRETARIAT

Introduction

Singapore emphasizes that capacity-building is a key element in global efforts to strengthen our collective cybersecurity posture against current and emerging threats, and to enable all States to contribute to and participate meaningfully in international discussions. In this regard, increased commitment to capacity-building by the international community is an urgent necessity in our efforts towards achieving security and resilience for all States in cyberspace.

2 Singapore reiterates the recognition by the Open-ended working group on security of and in the use of ICTs 2021-2025 (OEWG) in its second Annual Progress Report that capacity-building is an important confidence-building measure, is a topic that cuts across all the pillars of our work on ICT security at the global level, and that a holistic approach to capacity-building in the context of ICT security is essential.

3 In this regard, it is important that international discussions, including those at the OEWG, consider how to best to build on and coordinate the global capacity-building agenda with the existing work being carried out by various actors in different regions. In this regard, there is a need to (a) improve awareness of the landscape of existing capacity-building programmes on offer and improve the accessibility of these programmes for all States, and (b) develop a universal, inter-governmental platform to share experiences and best practices by providers of capacity-building. Such measures will help us maximise resources, avoid overlaps and better address the capacity-building needs of States.

Singapore's Role in Cybersecurity Capacity-Building

4 Singapore believes that it is important to take a holistic approach to capacity-building to address the challenges of cybersecurity, covering the policy, strategy, operational and legal aspects of cybersecurity as well as through exchanging best practices on whole-of-government coordination and digital and cyber diplomacy, so as to ensure that capacity-building efforts are effective.

5 At the regional level, the ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) under Singapore’s Cyber Security Agency (CSA) works closely with all ASEAN Member States and ASEAN Dialogue Partners, various UN partners including the UN Office of Disarmament Affairs and ITU as well as the ASEAN-Japan Cybersecurity Capacity Building Centre, to run coordinated cybersecurity capacity-building programmes aimed at developing cybersecurity skills among ASEAN officials. The ASCCE also offered online cyber capacity-building programmes during the Covid-19 pandemic. These online programmes continue to be offered currently for selected courses based on participant needs and feedback. From 2024, ASCCE programmes will also be offered to countries outside the ASEAN region (further information about ASCCE programming follows).

ASEAN-Singapore Cybersecurity Centre of Excellence (ASCCE) Programmes

6 The ASEAN-Singapore Cybersecurity Centre of Excellence was launched in October 2019 as an extension of the ASEAN Cyber Capacity Program (ACCP) previously launched in 2016. ASCCE’s broad-based curriculum is guided by the ‘4M’ approach: modular, multi-disciplinary, multi-stakeholder and measurable. Over the last 5 years, the ASCCE has delivered more than 50 programmes attended by over 1600 senior officials from ASEAN Member States (AMS) and beyond. Through ASCCE, Singapore partners with and strengthens bilateral relations with every ASEAN dialogue partner. Singapore's 2019 funding commitment of SGD$30 million for the ASCCE was renewed and extended by another three years running from 2024 through 2026.

7 **Scope and Modality of ASCCE Programmes.** The ASCCE’s programmes are targeted at senior government officials, from the cybersecurity agencies or ministries overseeing national cybersecurity and the national CERTs. For selected courses, international legal officers, and officials from other ministries such as ministries of foreign affairs will be invited where relevant. Singapore’s focus is on conducting programmes for all ASEAN Member States together, to build up a network of trained ASEAN officials. This interaction and networking are important aspects in addition to the knowledge our participants take away from the programmes. To ensure the holistic development of national cybersecurity capabilities, it is important that programmes focus on building capacities across the different dimensions of **cyber policy, operations, technical skills, international law in cyberspace, and diplomacy**, and **at different levels of proficiency**. Taken together, building capacities in these dimensions can potentially help States to both advance national cybersecurity and resilience – and also allow them to participate in international cyber discussions more effectively,

such as those at regional dialogues or international fora including at the ongoing UN OEWG. Additionally, it will also help States more effectively implement norms and confidence-building measures that contribute to international peace and security.

UN Singapore Cyber Fellowship (UNSCF)

8 The UN Singapore Cyber Fellowship was launched in October 2021, as part of the United Nations-Singapore Cyber Programme (UNSCP), in partnership with UNODA. UNSCF engages senior officials and decision-makers over a 6-day programme on national cyber and digital security policy, strategy, and operations. UNSCF has received commendations from Under-Secretary-General and High Representative for Disarmament Affairs Izumi Nakamitsu, as well as from various delegates at the UN for the value of insights and networking opportunities that Singapore has provided through the UNSCF. The most recent iteration of the UNSCF was oversubscribed by 300%. There is now an alumni network of over 70 UNSCF Fellows from 62 UN Member States.

Capacity-Building Activities with External Partners

9 In order to provide a holistic breadth of programmes to address the policy, strategy, operational and legal aspects of cybersecurity capacity-building, Singapore has also organised the following programmes with ASEAN Member States, ASEAN Dialogue Partners, and others:

ASEAN Member States and Dialogue Partners

- Executive Course and Alumni Workshop on International Law of Cyber Operations with Australia, the Netherlands and Cyber Law International

- Webinar on National Cyber Strategy with Canada

- ASEAN Regional Forum (ARF) Intersessional Meeting on ICTs Workshop on Awareness-Raising and Information Sharing on Emergency Responses to Security Incidents in the Use of ICTs, co-organised with Cambodia and China

- ASEAN Regional Forum Workshop on Critical Information Infrastructure Protection with EU

- ASCCE-ESIWA Webinar Confidence Building Measures in Cyberspace with EU

- ASCCE Webinar on Cyber Threat Hunting with India

- Cybersecurity Executive Awareness Course with Japan International Cooperation Agency (JICA)

- ASEAN Regional Action Plan Matrix Workshop with Malaysia

- Webinar on Awareness Building with New Zealand

- Webinar with Russia’s Moscow State Institute of International Relations (MGIMO) University on Development of Effective Coordination at the National Level for The Participation in International Discussions on the Security of and in the Use of ICTs

- Cyber Conference and Workshop on Strategic Communications with UK Government Communication Service International

- Digital Diplomacy Course with UK Foreign, Commonwealth and Development Office (FCDO)

- Webinar on Ransomware Threats and Mitigation with United States (US) Cybersecurity and Infrastructure Security Agency (CISA)

- Industrial Control Systems/Operational Technology Cybersecurity Analysis and Evaluation (ICS401V) with US CISA and CSA Academy

- Singapore-US Third Country Training Programme Workshop on Cybersecurity

- Singapore is the voluntary lead shepherd for cybercrime at the ASEAN Senior Officials Meeting on Transnational Crime. We have developed initiatives with our Dialogue Partners to level up our collective capability as a region to counter cybercrime. Examples of these initiatives are the ASEAN-Italy Course on Cybercrime and the ASEAN-Australia Cyber Capacity Building Workshop.

- The Singapore Police Force (SPF) has also developed capacity-building initiatives at the regional and global levels such as the Cyber Safety Asia Programme, which is a joint initiative between the Australian Federal Police (AFP), Australian Department of Foreign Affairs and Trade (DFAT) and SPF to develop expertise and leadership skills in cybercrime investigations, capacity-building and cyber safety awareness to complement and enhance existing capabilities within ASEANAPOL agencies.

- The ASEAN Defence Ministers Meeting (ADMM) Cybersecurity and Information Centre of Excellence (ACICE) will be conducting an inaugural Cybersecurity Course on "Cyber Incident Response & Threat Analysis" in Singapore from 26 February to 2 March 2024. This is an introductory course offered to all ASEAN Member States. The course will cover cybersecurity fundamentals where participants will be taught key cybersecurity concepts and various approaches to address cyber incidents. At the end of the course, participants will be equipped with the basic skills to monitor, detect, analyse, and respond to cybercrime, cyberespionage, insider threats, advanced persistent threats, regulatory requirements, and other cybersecurity issues facing organisations.

UN Partners

- Norms Implementation Checklist Workshop for ASEAN Member States with UN Office for Disarmament Affairs (UNODA) and S. Rajaratnam School of International Studies, Centre of Excellence for National Security (RSIS CENS)

- Norms Implementation Checklist Workshop for Non-aligned Movement (NAM) Member States and Group of Friends on e-Governance and Cybersecurity with UNODA, and RSIS CENS

- UN Singapore Cyber Fellowship (UNSCF) with UNODA (details below)

- International Telecommunication Union (ITU) Partner2Connect Digital Coalition

Industry and Academic Stakeholders, International Organisations

- ASCCE-Microsoft Hybrid Seminar: Cyberattacks, Hybrid War and our Collective Responsibility

- Cyber Incident Response and Threat Analysis with Temasek Polytechnic

- Engagements with GFCE (details below)

Expansion of Cyber Capacity-Building Programmes Beyond ASEAN from 2024

10 At the 8th Singapore International Cyber Week 2023, Deputy Prime Minister of Singapore Heng Swee Keat announced the **SG Cyber Leadership and Alumni Programme** as a structured programme to cater to participants at different stages of their cybersecurity journey. To support this new Programme, Singapore's earlier funding commitment of $30 million for cyber capacity-building will be extended by another three years, from 2024 to 2026.

11 The SG Cyber Leadership and Alumni Programme comprises training courses catered to participants at the Executive, Foundation and Advanced levels and is open to all countries. The programme also includes a Cyber Leaders' Alumni Fellowship.

12 The **Foundation course** is an introductory course focused on basic cyber diplomacy concepts, international law, and norms in cyberspace, as well as the operational and technical considerations of international cyber policy. It will also provide participants with an understanding of the cyber threat landscape and mitigation strategies. The **Executive course** aims to equip officials involved in cyber discussions at the multilateral level, such as at the UN OEWG, with the foundational operational and technical cyber policy knowledge necessary for their work. The **Advanced course** is targeted at senior officials who have attended the Foundation course and offers a deeper understanding and analysis of key cyber issues across the policy, legal, technical, and operational areas. Participants will also have hands-on, self-driven training featuring real-world case studies and keystone projects to bridge the gap between theoretical and practical implementation of cyber strategies. The interactive project-based approach explores cross-cutting issues, such as how operational processes protecting critical information infrastructure can influence regional incident response and cybersecurity policies, and how multilateral knowledge sharing of best practices can shape national cybersecurity technical norms and implementations.

13 The **Cyber Leaders' Alumni Fellowship** caters to senior officials who had previously participated in Singapore's capacity-building initiatives under the ASCCE. The Fellowship will be held at the sidelines of the Singapore International Cyber Week (SICW) and will bring together former course participants to participate in a series of closed-door meetings with experts and thought leaders on the latest trends and international discourse on cybersecurity. Participants will also get to exchange insights and best practices on issues of mutual interest, such as workforce and skills development, and legal frameworks on responsible cyber behaviour.

14 As part of the expansion of Singapore's capacity-building programmes beyond ASEAN, Singapore will be opening placements for applicants from the Pacific Islands Forum, Caricom and Africa member states.

Engagements with Global Forum on Cyber Expertise

15 The Global Forum on Cyber Expertise (GFCE) is a non-governmental organisation that aims to build cyber capacity-building to provide the necessary foundation for states to strengthen their cyber resilience. GFCE does this by coordinating regional and global cyber capacity-building projects, sharing knowledge and expertise, and matching individual needs for cyber capacity-building to offers of support as a clearing house function.

16 Singapore hosted the GFCE Southeast Asia Regional Meeting as a side-event at the SICW since 2021. The third meeting was held at the SICW in October 2023. Singapore also hosts the GFCE Southeast Asia Regional node, and is a Steering Committee member for GFCE's inaugural Global Conference on Cyber Capacity Building which will be held from 29 to 30 November 2023 in Accra, Ghana.

. . . . .