United Nations A/AC.292/2024/2

General Assembly

Distr.: General
22 January 2024

Original: English

Open-ended working group on security of and in the use of information and communications technologies 2021–2025
Seventh substantive session
New York, 4–8 March 2024

Mapping exercise to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels

Paper by the Secretariat

I. Introduction

1. In paragraph 46 of the progress report on the discussions of the working group on agenda item 5, contained in the annex to the document entitled "Developments in the field of information and telecommunications in the context of international security" (A/78/265), the United Nations Secretariat was requested to conduct a "mapping exercise", in consultation with relevant entities, in order to survey the landscape of capacity-building programmes and initiatives within and outside of the United Nations and at the global and regional levels, including by seeking the views of Member States. The Secretariat was further requested to produce a report with the findings of the "mapping exercise" and to present the report at the seventh session of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, to be held from 4 to 8 March 2024, so as to support States' efforts to take stock of existing capacity-building efforts and to encourage further synergies and coordination between such efforts. The present report is submitted pursuant to that request.

2. On 2 October 2023, the Office for Disarmament Affairs circulated a note verbale to all Permanent Missions to the United Nations drawing their attention to paragraph 46 of the above-mentioned report, inviting their views on the landscape of information and communications technologies capacity-building programmes and initiatives, within and outside of the United Nations and at the global and regional levels. A deadline for responses was set for 10 November 2023, and later extended to 16 November. As at 22 January 2024, the following States had submitted written views: Australia, Belgium, Brazil, Burkina Faso, Cambodia, Chile, Colombia, Cuba, Czechia, Estonia, France, Germany, India, Iran (Islamic Republic of), Netherlands (Kingdom of the), Lebanon, Mexico, Portugal, Qatar, Republic of Korea, Russian Federation, Singapore, Slovakia, Slovenia, Switzerland, Türkiye, United Kingdom of Great Britain and Northern Ireland, United States of America and Uruguay.

3. The Office for Disarmament Affairs further requested the views of relevant United Nations system entities through letters dated 2 October 2023. As at 22 January 2024, the following United Nations entities had submitted written views: International Telecommunication Union, Counter-Terrorism Committee Executive Directorate, United Nations Development Programme, United Nations Institute for Disarmament Research, United Nations Interregional Crime and Justice Research Institute, Office of Counter-Terrorism, Office of Information and Communications Technology, Office of Legal Affairs and United Nations Office on Drugs and Crime.

4. A call for inputs was also issued to relevant non-governmental stakeholder entities by email on 2 October 2023. As at 22 January 2024, the following stakeholder entities submitted written views: Association for Progressive Communications, Centre for Communication Governance at the National Law University of Delhi, DiploFoundation, Global Forum on Cyber Expertise, International Chamber of Commerce, Centre of Excellence for National Security of the S. Rajaratnam School of International Studies, SafePC Solutions, Third Eye Legal, Write Pilot. The European Union also submitted views. The following joint written submissions were also received: a joint submission from Argentina, Brazil, Chile, Colombia, Costa Rica, Ecuador, El Salvador, Guatemala, Dominican Republic, Paraguay and Uruguay; and a joint submission from the National Cyber and Information Security Agency of Czechia, the International Committee of the Red Cross (ICRC), the North Atlantic Treaty Organization (NATO) Cooperative Cyber Defence Centre of Excellence, the University of Exeter, the United States Naval War College and Wuhan University.

5. All written views received, including those received after the formal extended deadline, are available on the website of the open-ended working group on security of and in the use of information and communications technologies 2021–2025.[1] States are encouraged to consult the full written submissions provided by Member States, United Nations system entities and non-governmental stakeholder entities, as the present report does not represent an exhaustive inventory of all activities elaborated therein.

6. The present report draws primarily upon inputs received from the above-listed Member States, United Nations system entities and non-governmental stakeholder entities without prejudice to their individual positions. Additional information available from open sources is presented with a view to presenting a balanced and illustrative landscape of existing capacity-building programmes and initiatives within and outside of the United Nations and at the global and regional levels.

7. Examples of capacity-building programmes and initiatives are presented, first highlighting efforts at the regional and subregional levels, followed by information broadly categorized by theme. These descriptions do not represent an exhaustive inventory of all capacity-building initiatives and programmes, but rather seek to provide an overview landscape of activities in an illustrative manner. There is no prioritization or ranking of activities implied.

8. The present report concludes with observations and conclusions from the Secretariat with a view to supporting States in taking forward more effective, sustainable and efficient capacity-building initiatives at the global, regional and subregional levels.

II. Overview of State discussions and conclusions on capacity-building at the multilateral level

9. In the light of the evolving landscape of threats emanating from the use of information and communications technologies by States in the context of

[1] Available at https://meetings.unoda.org/meeting/57871/documents.

international security, States continue to underscore the urgency of enhancing the capacity of all States to observe and implement the cumulative and evolving framework for responsible State behaviour, as affirmed in the second annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025 (A/78/265).

10. States have highlighted the need to promote better understanding of the needs of developing States with the aim of narrowing the digital divide through tailored capacity-building efforts. States have underscored the pressing need for building capacity and good practices in a range of diplomatic, legal, policy, legislative and regulatory areas, in addition to technical skills, institution-building and cooperative mechanisms. States have variously emphasized the value of South-South, triangular and subregional and regional cooperation, as a complement to North-South cooperation. States have also recalled the value of the train-the-trainer approach through establishing specialized training and tailored curricula and professional certification, which will allow for passing on necessary knowledge and skills to relevant counterparts.

11. In the framework of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, States continue to make concrete, action-oriented proposals on capacity-building efforts, including, inter alia, a proposal to develop a Global Cyber Security Cooperation Portal, a proposal to encourage further technical exchange on information and communications technologies threats to identify, detect and facilitate informed responses to malicious activities, and a proposal to hold discussions on fostering meaningful engagement of and partnerships with non-governmental stakeholders in the area of capacity-building, including for the purposes of training and research.

12. The open-ended working group on security of and in the use of information and communications technologies 2021–2025 itself has been recognized as a platform to continue exchanging views and ideas related to capacity-building efforts, including how best to leverage existing initiatives in order to support States in developing institutional strength to implement the framework of responsible State behaviour.

13. States have continued to promote the mainstreaming of the principles of capacity-building in relation to State use of information and communications technologies in the context of international security contained in annex C to document A/78/265 and first elaborated in the final report of the Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.[2] By endorsing these principles, States have concluded that capacity-building should be a sustainable process, comprising specific results-based activities, while also having a clear purpose, be evidence-based, politically neutral, transparent, accountable and without conditions. Moreover, States have agreed that capacity-building should be undertaken with full respect for the principle of State sovereignty, be demand-driven, correspond to nationally identified needs and priorities and respect human rights and fundamental freedoms. In its second progress report (A/78/265), the open-ended working group recommended that States develop and share voluntary checklists and other tools to mainstream the implementation of the agreed principles of capacity-building.

14. Through the discussions of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, States have continued to raise awareness of the gender dimensions of security in the use of information and communications technologies and to promote gender-sensitive capacity-building at the policy level, as well as in the selection and operationalization

[2] A/75/816, annex I, para. 56.

of capacity-building projects. States have encouraged efforts to promote gender-responsive capacity-building efforts, including through the integration of a gender perspective into national information and communications technologies policies and capacity-building initiatives as well as the development of checklists or questionnaires to identify needs and gaps in this area.

15. States have posited that the United Nations could play an essential role in coordinating capacity-building efforts by taking stock of States' needs, identifying gaps through tools and surveys, and facilitating access by States to capacity-building programmes, including through the present "mapping exercise".

III. Regional, subregional and cross-regional cooperation

16. States have consistently reaffirmed that regional and subregional organizations play an important role in supporting the implementation of the framework for responsible State behaviour in the use of information and communications technologies, including through support to related capacity-building initiatives. States have variously reflected on the efforts that could be undertaken at the regional, subregional and cross-regional levels, including workshops, training courses and exchanges on best practices and lessons learned. States have also been encouraged to support capacity-building programmes, including in collaboration with, where appropriate, regional and subregional organizations.[3]

17. In terms of cross-regional cooperation, the Global Forum on Cyber Expertise is a multi-stakeholder community comprising more than 200 members and partners, including States from all regions, international and regional organizations, and actors from the private sector, civil society and academia. The Cybil Portal, a flagship initiative of the Global Forum on Cyber Expertise, is an online repository of international cyber capacity-building projects and hosts a library of resources for interested stakeholders.[4]

18. In November 2023, the Global Forum on Cyber Expertise hosted the inaugural Global Conference on Cyber Capacity-Building in cooperation with Ghana, the World Economic Forum, the World Bank and CyberPeace Institute. The Conference featured thematic and deep-dive regional sessions. The Conference produced an outcome document, the Accra Call for Cyber-Resilient Development, comprising a set of non-binding, voluntary, direction-setting actions that are aimed at: (a) strengthening the role of cyber resilience as an enabler for sustainable development; (b) advancing demand-driven, effective and sustainable cyber capacity-building; (c) fostering stronger partnerships and better coordination; and (d) unlocking financial resources and implementation modalities.[5] It was announced as part of the Conference that the next Global Conference on Cyber Capacity-Building would be held in Geneva in May 2025, with a goal of building on the progress initiated in Ghana.

19. In order to strengthen cooperation between the regions, the European Union – Latin American and Caribbean Digital Alliance hosts regulatory and cybersecurity dialogues, among other activities on digital and space issues. The Alliance aims to support digital transformation and innovation with a human-centric vision of digital economies and societies. In order to meet these objectives, the Alliance's activities include the establishment of a biregional digital policy dialogue, the expansion of the Building the Europe Link to Latin America (BELLA) programme (BELLA II), the implementation of a regional Copernicus strategy to enhance digital resilience by

[3] A/78/265, annex, para. 51.

[4] See https://cybilportal.org/about-cybil/.

[5] Available at https://gc3b.org/news/read-the-full-accra-call-for-cyber-resilient-development/.

supporting spatial data management capacity and strategic use, and the establishment of a regional European Union – Latin American and Caribbean digital accelerator to foster entrepreneurship and innovation.

20. An ongoing project entitled "Enhancing Security Cooperation in and with Asia" (ESIWA) supported by the European Union and funded by France and Germany, aims to increase convergences in policy and practices of the European Union and partner countries, to increase awareness and to support operational security dialogues.[6] The project undertakes activities in four thematic areas: counter-terrorism and preventing violent extremism, cybersecurity, maritime security and crisis management. Current participating States are India, Indonesia, Japan, the Republic of Korea, Singapore and Viet Nam.

21. In the Central and Eastern European region, the Western Balkans Cyber Capacity Centre was launched by France, Montenegro and Slovenia in May 2023.[7] The Centre aims to support six participating countries and areas in reinforcing institutional and operational cybercapacities. Activities include training courses, the development of cyber curricula and the exchanging of information and best practices to support practitioners in Western Balkan States in preventing, preparing for and responding to cyberthreats. In 2023, the Centre delivered training courses on cyber hygiene for public administrations, a mentoring programme for women in cyber policymaking and international negotiations, cybercrime courses for judicial authorities and police forces and a course for chief information security officers in critical infrastructures. At the time of writing, a further 12 training courses are scheduled for 2024. Similarly, a European Union project co-led by Czechia and Estonia is aimed at supporting cybersecurity capacity building in the Western Balkans through the development of: (a) cybersecurity governance and awareness; (b) strengthening legal frameworks, cybernorms and compliance with international law; (c) risk and crisis management; and (d) operational capacities, including by strengthening computer security incident response team. Another project of the European Union, entitled "Cybersecurity rapid response for Albania, Montenegro and North Macedonia " was implemented to support resilience to cyberincidents.

22. The Organization for Security and Cooperation in Europe (OSCE) Transnational Threats Department delivers activities to enhance participating States' capacities to tackle information and communication technologies security-related threats. The range of activities includes exercises to promote adequate national responses to incidents involving critical infrastructure, workshops on countering the use of the Internet for terrorist purposes, and training on the investigation and prosecution of cybercrimes.[8] In 2023, the Department held a training course on international cyberdiplomacy in Vienna, which was focused on building national capacities to engage in international cyberpolicy deliberations. As the implementer of the national cyberincident severity scales and related measures to protect critical infrastructures, OSCE supports the development of crisis communication and management procedures and incident classification methods among European, Central Asian and other countries. In addition, OSCE serves as a multilateral forum for several cyber cooperation and capacity-building discussions.

23. The Russian Federation holds annual seminars and online workshops with the Regional Forum of the Association of Southeast Asian Nations (ASEAN) on terminology in the field of security of and in the use of information and communications technologies, countering the use of information and communications technologies for criminal purposes and sustainable and secure development of the

[6] See www.eeas.europa.eu/sites/default/files/factsheet_eu_asia_security_july_2019.pdf.

[7] See https://cybilportal.org/projects/western-balkans-cyber-capacity-centre-wb3c/.

[8] See www.osce.org/secretariat/cyber-ict-security.

Internet and digital forensics. The Russian Federation also hosted trainings on the investigation of information and communications technologies-related embezzlement crimes at the Conference on Interaction and Confidence-Building Measures in Asia.

24. The International Telecommunication Union (ITU), in cooperation with the International Multilateral Partnership against Cyber Threats, established the Oman-ITU Regional Cybersecurity Centre, with the support of Oman.[9] The Centre aims to enhance capacities, capabilities, readiness, skills and knowledge in the areas of cybersecurity, critical infrastructure protection and capacity-building for the Arab region, based at the premises of the computer emergency response team of Oman.

25. The Inter-American Committee against Terrorism of the Organization of American States (OAS), through its Cybersecurity Programme, supports Member States in building technical, political and diplomatic capacities to prevent, identify, respond to and recover from cyberincidents and to promote responsible State behaviour in cyberspace.[10] Among other activities, the Programme assists in the development of national cybersecurity strategies and the establishment of national computer security incident response teams. It further provides assistance and training, toolkits and guides for policymakers, industry and civil society and operates the hemispheric network of computer security incident response teams in the Americas, which shares threat and intelligence information among 29 computer security incident response teams from 20 States members of OAS. The programme also supports greater mainstreaming of gender perspectives into cybersecurity policymaking and representation in multilateral processes.

26. The Ibero-American Cyber Defense Forum was convened in October 2023 in Brazil.[11] Some 13 States participated in the Forum, with the aim of deepening regional integration and cooperation to prevent, identify and address cyberthreats. Activities included simulation exercises and drills, including the Cyber Guardian 5.0 exercise and the development of a malware information-sharing platform.

IV. Non-exhaustive, illustrative overview of capacity-building initiatives by thematic area of focus

International law

27. States have acknowledged the particular need for capacity-building initiatives in the area of international law in the context of information and communications technologies security. States have underscored the urgent need to continue such capacity-building efforts, including with the aim of ensuring that all States are able to participate on an equal footing in the development of common understandings as to how international law applies in the use of information and communications technologies. Such efforts have included workshops, training courses and exchanges on best practices at the international, interregional, regional and subregional levels. States have also noted the value of providing capacity-building with a view to the preparation of national position papers on the applicability of international law to State use of information and communications technologies.

28. Globally available online resources on capacity-building in the area of international law include the Cyber Law Toolkit, developed by a consortium of the National Cyber and Information Security Agency of Czechia, ICRC, the Cooperative Cyber Defence Centre of Excellence of NATO, the University of Exeter, the United

[9] See www.itu.int/en/ITU-D/Cybersecurity/Pages/Global-Partners/oman-itu-arab-regional-cybersecurity-centre.spx.

[10] See www.oas.org/ext/en/security/prog-cyber.

[11] See https://dialogo-americas.com/articles/brazil-leads-ibero-american-cyber-defense-forum/.

States Naval War College and Wuhan University.[12] The Toolkit is available to government and legal professionals free of charge and currently consists of: (a) 28 scenarios exploring the applicability of international law to cyberoperations; (b) information on national positions on the application of international law to the uses of information and communications technologies, including in relation to sovereignty, non-intervention or what constitutes an attack under international humanitarian law; and (c) over 50 cyberincident pages providing information on recent attacks or ongoing armed conflicts.

29. The Oxford Process on International Law Protections in Cyberspace was launched in 2020 by the Oxford Institute for Ethics, Law and Armed Conflict in partnership with Microsoft.[13] At the time of writing, the Oxford Process has yielded five “Oxford statements on international law protections”, which are the product of collaborations between international legal experts globally to identify and clarify the rules of international law applicable to cyberoperations in a range of contexts, including with respect to protections for the health-care sector, the safeguarding of vaccine research, protection against electoral interference, and the regulation of information operations and activities and of ransomware operations.

30. Regarding the applicability of international humanitarian law to cyberspace, ICRC provides resources for policymakers, including research papers, workshops, symposiums and the establishment of an ICRC delegation for cyberspace, based in and supported by Luxembourg. Examples of recent activities include the launch of a humanitarian action programme in cooperation with the University of Cambridge Centre for Research in the Arts, Social Sciences and Humanities, the hosting of an international expert meeting on international humanitarian law and the growing involvement of civilians in cyber and other digital operations during armed conflicts with the Geneva Academy of International Humanitarian Law and Human Rights, held on 28 and 29 September 2023 in Geneva, and a round table on cyberwarfare in partnership with the Research Society of International Law, held on 17 May 2023 in Islamabad.

31. Australia, Netherlands (Kingdom of the) and Singapore, in association with Cyber Law International, have coordinated on the delivery of an international cyberlaw training course for State officials of States members of ASEAN and OSCE on the international law of cyberoperations.

32. The Japan International Cooperation Agency, through a training on capacity-building in international law and policy formation for the enhancement of measures to ensure cybersecurity, provides officials from government agencies and national computer emergency response teams from developing countries with the international law and policy knowledge and skills they need to effectively develop and implement cybersecurity policies.

33. States have also undertaken various consultations to allow space for dialogue on the applicability of international law. For example, OAS, in cooperation with the Inter-American Juridical Committee and ICRC, has hosted consultations on international law applicable to cyberspace.[14] In addition, in collaboration with the Institute for Law, Innovation and Technology at Temple University in Pennsylvania and with Microsoft, Mexico hosted three virtual workshops on the application of international law to cyberspace, the promotion of rules and norms for peaceful behaviour and bridging digital divides. The project produced a multi-stakeholder compendium of good practices and recommendations on the application of

[12] See https://cyberlaw.ccdcoe.org/wiki/Main_Page.

[13] See www.elac.ox.ac.uk/the-oxford-process/.

[14] See www.oas.org/en/sla/dil/International_Law_Applicable_to_Cyberspace_2022.asp.

international law to cyberspace, which was launched at the sixth substantive session of the open-ended working group on security of and in the use of information and communications technologies, in December 2023.

34. OSCE has convened executive courses on international law of cyberoperations, including a course held from 13 to 17 February 2023 in Skopje, in cooperation with the Kingdom of the Netherlands and with additional support from Italy, Slovakia, Switzerland, the United Kingdom of Great Britain and Northern Ireland and the Republic of Korea, and from Cyber Law International.

Policy, including development of national strategies

35. In annex B to its second annual progress report contained in document A/78/265, the open-ended working group on security of and in the use of information and communications technologies 2021–2025 agreed to an initial list of voluntary global confidence-building measures. Among those measures, one encourages States to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes. Moreover, States have acknowledged the importance of possessing the requisite capacity to put in place the required policies, legislation and strategies for a secure information and communications technologies environment. Against this backdrop, various capacity-building efforts have been undertaken to support States in formulating national policies, developing strategies and establishing the required institutions and structures with relevant competence in matters of information and communications technologies in the context of international security.

36. At the global level, the United Nations Institute for Disarmament Research (UNIDIR) hosts an annual cyberstability conference featuring discussions on promoting a secure and stable cyberspace, norms and international law and on supporting multilateral dialogue on cybersecurity issues. In past iterations, the conference has featured thematic briefings from scholars to support the elaboration of States' national views, including on legal questions related to the peaceful settlement of disputes in connection with State use of information and communications technologies, as well as policy and technical questions on the protection of critical infrastructure and services across sectors. Past conferences have also focused on related intergovernmental processes under United Nations auspices. The next cyberstability conference will take place on 29 February and 1 March 2024 in New York.

37. States have also recognized the value of the Cyber Policy Portal of UNIDIR, which serves as a useful format for States to voluntarily engage in transparency measures by sharing relevant information, policies, legislation and other good practices.[15] As of December 2023, 1,528 documents had been uploaded to the Cyber Policy Portal database, with documents available in 55 languages and information published regarding 897 capacity-building projects. There were approximately 23,000 visits to the Portal in 2023.

38. In December 2023, the Cyber Policy Portal integrated nearly 900 capacity-building projects from the Cybil Portal of the Global Forum on Cyber Expertise. The data exchange encompasses project details such as the title of the project, information on beneficiaries, funders and start and end dates of the project, and is available in the six official languages of the United Nations. The initiative enhances the security of and in the use of information and communications technologies through improving awareness of existing resources, facilitating collaboration among stakeholders and encouraging greater transparency in cyber capacity-building efforts.

[15] See https://cyberpolicyportal.org/.

39. ITU, in partnership with the World Bank, the United Nations Conference on Trade and Development (UNCTAD) and the Commonwealth Telecommunications Organisation, provides policy-related support in creating an effective national cybersecurity framework. To that end, the second edition of the *Guide to Developing a National Cybersecurity Strategy*, published by ITU in 2021,[16] provides policymakers with an overview of the strategy development process, taking into consideration their country's specific situation, cultural and societal values. In addition, ITU offers an online training course to prepare national policymakers and cybersecurity practitioners from the public and private sectors through four e-learning modules and an online tabletop exercise based on the Guide.[17] An updated national cybersecurity strategies repository containing national policies, action plans and other relevant elements that are related to cybersecurity is also available online.[18]

40. The United Nations-Singapore Cyber Fellowship Programme is held twice a year for a six-day session for nominated State officials to build capacities and networks on national cyber and digital security policy, strategy and operations. Following the first three iterations of the programme, two further sessions are planned for 2024. The programme has an alumni network of more than 70 fellows, representing 62 Member States.

41. The Kingdom of the Netherlands funded the Global Cyber Policy Dialogue series with the Observer Research Foundation America. Over two years, the project supported the development of national cybersecurity strategies and hosted regional cyberpolicy dialogues in South-East Asia, the Western Balkans, the Middle East and North Africa, Southern Africa and Latin America and the Caribbean. The project also aimed to promote secure digital transformation and public-private partnerships, identify capacity-building needs and gaps and support the continued development of norms of State behaviour in cyberspace.

42. As part of the Digital for Development Hub, the European Union, Germany, Expertise France, the International and Ibero-American Foundation for Administration and Public Policies and the Horn of Africa Initiative have collaborated to deliver an initiative for digital government and cybersecurity in the Horn of Africa region.[19] The project is aimed at assisting participating States (Djibouti, Kenya and Somalia) to strengthen the delivery of public sector services through secure digital channels. The project includes dialogues and information exchanges through a regional technical committee, as well as reviews of road maps and digitization projects under way in each State.

43. Bilaterally, France and Senegal have partnered in the Dakar-based regionally oriented national cybersecurity school that, among other activities, provides training, strengthens cooperation and raises awareness of cybersecurity among African States.[20] Also illustrative of many current bilateral programmes, Portugal supports ongoing strategic cooperation programmes in partnerships with Angola, Cabo Verde, Guinea-Bissau, Mozambique, Sao Tome and Principe and Timor-Leste, which strengthen legal and administrative structures to prevent, identify and respond to cybercrime, cyberterrorism and cyberincidents.

44. In Asia, the Global Cybersecurity Centre for Development, based in the Republic of Korea, provides assistance to States upon request to build cyberexpertise

[16] See https://ncsguide.org/the-guide/.

[17] See www.itu.int/en/ITU-D/Cybersecurity/Pages/cybersecurity-national-strategies.aspx.

[18] See www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies-repository.aspx.

[19] See www.fiiapp.org/en/proyectos_fiiapp/d4d-initiative-for-digital-governance-and-cybersecurity-idgc-for-the-horn-of-africa-initiative/.

[20] See www.diplomatie.gouv.fr/en/country-files/senegal/news/article/regionally-oriented-national-school-for-cyber-security-opens-in-dakar-senegal.

and cyberresilience in the public sector. Seminars can be provided on drafting national cybersecurity strategies and frameworks, establishing and operating national computer emergency response teams, detecting, analysing and responding to cyberincidents and sharing information on cyber trends and threats.[21] Recent seminars have been hosted in Costa Rica, the Lao People's Democratic Republic and Serbia on cybersecurity strategy development, incident handling, cybersafety and resilience, among other themes.

45. As part of its Cyber and Critical Tech Cooperation Programme, the Department of Foreign Affairs and Trade of Australia supports its eSafety Commissioner to develop global online safety resources and work with governments in Asia and the Pacific to develop national approaches to safeguarding citizens online.[22] Partnering with industries, academia, civil society, agencies of the Government of Australian and other like-minded donors, the programme supports over 25 countries across South-East Asia and the Pacific to advance and protect their collective interests in cyberspace.

46. In the Americas, in the framework of the North American Leaders' Summit, Canada, Mexico and the United States of America participated in a round table on cybersecurity to strengthen cooperation between the participating States in the development and implementation of cybersecurity policies, which was held in January 2023. From 8 to 14 October 2023, Colombia and Czechia co-convened discussions on the intersection between cybersecurity and artificial intelligence, with a focus on legislation, national policies and strategies.

47. The Cyber Diplomacy Initiative of the European Union (Cyber Direct) supports a broad range of policy support, research, outreach and capacity-building in the field of cyberdiplomacy, including by maintaining a cyberdiplomacy toolbox and hosting an annual European Cyber Diplomacy Dialogue.[23] Among many other programmes and initiatives, Cyber Direct hosts a fellowship programme for junior and mid-level cyber or digital experts from partner countries, namely, non-members of the European Union from the Eastern European Group, Africa Group, Latin America and Caribbean Group or Asia-Pacific Group.[24] Also in the region, a coalition between Estonia, Finland, Germany and Luxembourg, led by the Information System Authority of Estonia manages and implements the CyberNet initiative of the European Union, 2019–2025,[25] which has built a community of over 300 cyberexperts in over 40 areas of competence to support cyber capacity development.

48. The Geneva Centre for Security Sector Governance operates a cybersecurity governance programme that supports State actors with cybersecurity law and policymaking, to strengthen accountability frameworks and build capacities.[26] A recent project established a Western Balkans Cybersecurity Research Network that, among other activities, produces research into cybersecurity and human rights, the cybersecurity needs of vulnerable groups, and gender, in their respective national contexts. The Geneva Centre for Security Policy similarly provides cybersecurity training courses and workshops.[27] Also based in Geneva, DiploFoundation supports capacity development in the field of Internet governance and digital policy through providing online courses, workshops and simulation exercises in cybersecurity, data,

[21] See www.kisa.or.kr/EN/201.

[22] See www.internationalcybertech.gov.au/cyber-tech-cooperation-program.

[23] See https://eucyberdirect.eu/.

[24] See https://eucyberdirect.eu/news/eu-cd-fellowship.

[25] See www.eucybernet.eu/.

[26] See www.dcaf.ch/cybersecurity-governance.

[27] See www.gcsp.ch/.

artificial intelligence and other emerging issues and through promoting and developing digital tools for inclusive and impactful governance and policymaking.[28]

49. The Cyberspace4All project, supported by the Kingdom of the Netherlands, is aimed at promoting inclusivity and awareness through creating a shared language and references on international cybergovernance, raising awareness of key developments on cyber issues at the United Nations and helping inform State policies on cybernorms. In its first phase, the project has produced an issue of the *Journal of Cyber Policy*, short videos on cyber capacity-building and a podcast, entitled "Who rules cyberspace?". The second phase, jointly implemented by Chatham House, aims to provide recommendations on, build awareness of and support the implementation of United Nations norms and principles of capacity-building and responsible State behaviour in cyberspace.

50. Capacity-building in the area of cyber diplomacy has also been offered through various channels. For example, the Tallinn Summer School of Cyber Diplomacy is organized as part of the Multilateralism and Digitalization programme, in cooperation with the Ministry of Foreign Affairs of Estonia, the e-Governance Academy and the Estonian Centre for International Development. Its main objective is to provide training to diplomats working on cyber foreign policymaking, as well as other government officials interested in complex cyber issues. The Cybersecurity Programme of the Inter-American Committee against Terrorism of OAS similarly provides a cyberdiplomacy training programme to support officials working in this area. On the part of the Secretariat of the United Nations, the online cyberdiplomacy course currently available on the Disarmament Education Dashboard will be updated in 2024.[29]

Computer emergency response teams, technical training and other related support

51. States have consistently called for a concrete, action-oriented approach to capacity-building. States concluded that such concrete measures could include the provision of support to computer emergency response teams or computer security incident response teams and establishing specialized training and tailored curricula including train-the-trainer programmes and professional certification. States have also expressed concern that a lack of awareness of existing and potential threats and a lack of adequate capacities to detect, defend against or respond to malicious information and communications technologies activities may make them more vulnerable.

52. The importance of technical training for personnel in the field of information and communications technologies has also been highlighted, including in the areas of information security, methods of detecting and countering computer network attacks in open information systems, tactics, techniques and procedures for protecting information from unauthorized access, the collection of open source data, techniques for investigating crimes linked to information and communications technologies in relation to international peace and security and international cooperation in this field, computer forensics, countering the use of information and communications technologies and international postal services in drug trafficking and for the theft of funds, and the identification and investigation of illegal transactions with digital assets, including cryptocurrencies, and of their use for financing terrorism.

[28] See www.diplomacy.edu/.

[29] See https://cyberdiplomacy.disarmamenteducation.org/home/.

53. At the global level, ITU provides ongoing assistance to States to establish national computer emergency response teams.[30] Recent examples include the launches of such teams, facilitated by ITU, in the Bahamas, Barbados, Burkina Faso, Côte d'Ivoire, Cyprus, the Gambia, Ghana, Jamaica, Kenya, Kyrgyzstan, Lebanon, Malawi, Montenegro, Trinidad and Tobago, Uganda, the United Republic of Tanzania and Zambia. In each case, those teams serve as a central coordinating body to identify, manage and respond to cyberthreats.

54. The Forum of Incident Response and Security Teams maintains a network of over 700 participating computer emergency response teams to support cooperation to proactively and reactively respond to cybersecurity incidents. Among other activities, the Forum shares best practices among its members and promotes the development of technical colloquiums, classes, publications, web services, special interest groups and an annual incident response conference.[31]

55. The Secretary of the Ministry of Electronics and Information Technology of India, Alkesh Kumar Sharma, inaugurated the Group of 20 Cyber Security Exercise and Drill for over 400 domestic and international participants as part of India's presidency of the Group of 20. The Indian Computer Emergency Response Team held the Cyber Security Exercise and Drill in a hybrid format. International participants from some 12 countries participated online. Domestic participants from such sectors as finance, education, telecommunications, ports and shipping, energy and information and communications technologies attended both in person and virtually.

56. Through its term as Chair-in-Office of the Commonwealth, the United Kingdom conducted a range of capacity-building activities under the remit of the Commonwealth Cyber Security Programme in support of the aims of the 2018 Commonwealth Cyber Declaration.[32] The Programme supported States members of the Commonwealth to carry out national cybersecurity capacity self-assessments and provided technical assistance, training and advice on cybersecurity and cybercrime threats. Through the project, over 140 events were held in 32 countries, with over 6,000 people availing of training.

57. The ASEAN-Singapore Cybersecurity Centre of Excellence offers support to States members of ASEAN to promote cyber capacity-building in the region, through the provision of research, training, computer emergency response team-related technical support, exchanges of information on open-source cyberthreats, attacks and best practices, and through trainings and exercise.[33] Since its establishment, the Centre of Excellence has delivered over 50 programmes attended by more than 1,600 senior officials of participating States. Starting in 2024, the programmes of the Centre of Excellence will be available to States outside the ASEAN region. In order to support regular coordination and cooperation, the ASEAN Defence Ministers' Meeting-Plus Experts' Working Group on Cybersecurity has met regularly since 2016 as a platform for confidence-building and norms development among States members of ASEAN.

58. The ASEAN Cyber Capacity Programme is aimed at building capacity in States members of ASEAN, through the strengthening of resilience and regional responses

[30] See www.itu.int/en/ITU-D/Cybersecurity/Pages/national-CIRT.aspx.

[31] See www.first.org/.

[32] See https://assets.publishing.service.gov.uk/media/60538ad98fa8f55d38ea34c3/UK_Commonwealth_Cyber_Security_Programme_six_case_studies.pdf.

[33] See www.csa.gov.sg/News-Events/Press-Releases/2021/asean-singapore-cybersecurity-centre-of-excellence.

to threats.[34] Activities including workshops, seminars, the annual Singapore International Cyber Week, a joint United States-Singapore cybersecurity workshop and the ASEAN Ministerial Conference on Cybersecurity. At the eighth Singapore International Cyber Week in 2023, the Singapore Cyber Leadership and Alumni Programme was launched. Open to nominees from all States, the programme provides foundation, executive and advanced courses to officials so as to deepen their expertise on cyberdiplomacy concepts and processes, international law, norms in cyberspace and operational and technical considerations of international cyber policy. In addition, a "Cyber Leaders' Alumni Fellowship" is envisaged to connect former participants of capacity-building activities hosted by the Cybersecurity Centre of Excellence for a series of closed meetings on trends, international discourse on cybersecurity, as well as to exchange best practices on areas including workforce and skills development, legal frameworks and responsible cyberbehaviour.

59. The Republic of Korea has served as host to the Cybersecurity Alliance for Mutual Progress since its launch in 2016. The Alliance is focused on promoting cooperation and capacity-building between participating States.[35] At the time of writing, 67 organizations from 49 countries have joined the Alliance.

60. In 2023, the Korea Internet and Security Agency launched the ASEAN Cyber Shield project, in cooperation with Kangwon National University, Gangneung Wonju University and the University of Technology Brunei. The project aims to enhance cooperation between States members of ASEAN on cybersecurity, will operationalize an online cybersecurity curriculum in the region, produce research on cybersecurity certification schemes, host ASEAN hackathons and cybersecurity student exchanges.[36]

61. From 2017 to 2019, ITU conducted a project to support Pacific small island States in creating national, subregional and regional frameworks for cybersecurity and to enhance skills in these areas. The programme aimed to assess readiness for the establishment of national computer emergency response teams in Papua New Guinea, Samoa, Tonga and Vanuatu and designed and developed implementation plans for such teams. Through the project, ITU hosted training workshops to enhance awareness and skills, in which over 200 participants and over 70 organizations shared experiences in the field of incident response and protection of critical information infrastructures. The results of a stocktaking exercise were subsequently measured against the indicators in the Cybersecurity Capacity Maturity Model for Nations developed by the Global Cyber Security Capacity Centre of the Oxford Martin School, University of Oxford.[37]

62. As part of the Cyber and Critical Technology Cooperation Programme in Australia, the Pacific Cyber Security Operational Network[38] is an operational cybersecurity network of regional working-level cybersecurity experts in the Pacific. The Network maintains a register of operational cybersecurity points of contact and empowers members to share cybersecurity threat information, provides opportunities for technical experts to share tools, techniques and ideas, and is an enabler of cooperation and collaboration, particularly where a cybersecurity incident affects the region.

[34] See www.csa.gov.sg/docs/default-source/csa/documents/sicw-2016/factsheet_accp_final.pdf?sfvrsn=a45aecbb_0#:~:text=Cyber%20Capacity%20Programme-,The%20ASEAN%20Cyber%20Capacity%20Programme%20(ACCP)%20aims%20to%20build%20cyber,secure%20and%20resilient%20ASEAN%20cyberspace.

[35] See www.cybersec-alliance.org/camp/index.do.

[36] See wwwk.kangwon.ac.kr/english/contents.do?key=2356&.

[37] See https://gcscc.ox.ac.uk/the-cmm.

[38] See https://pacson.org/.

63. Various bilateral activities focused on technical capacities have also been undertaken. For example, the Cyber Security Capacity Building in the Pacific Programme in New Zealand provides bilateral support to Pacific island States in developing national cybersecurity strategies, building the capacities of computer emergency response teams, awareness-raising, drafting cybersecurity and cybercrime legislation in line with international standards, and investigating and prosecuting in line with such legislation. Recent conferences in the region include the International Symposium on Cybercrime Response, held in the Republic of Korea from 13 to 15 September 2023, and the Pacific Cyber Capacity Building and Cooperation Conference, held in Fiji from 2 to 4 October 2023.

64. Through the Cyber and Critical Technology Cooperation Programme Australia supports partners in the Pacific and South-East Asia in strengthening technical and governance resilience to cyberthreats.[39] Established in 2016, the Cooperation Programme was expanded in 2021 to include cooperation on critical technologies. As of November 2023, the programme has supported 126 projects in 21 countries in the region. Projects include activities to enhance cybersecurity capabilities, leverage technology in support of economic growth and development, advocate the protection of human rights and democracy online, prevent and prosecute cybercrime and support the implementation of the United Nations-endorsed normative framework for responsible State behaviour in the use of information and communications technologies in the context of international security. The Cyber Bootcamp Project, which was launched in August 2019 as part of the Cooperation Programme, was designed to provide practical expertise-building and skills training to government officials across South-East Asia on shared challenges and opportunities.

65. The Latin America and Caribbean Cyber Competence Centre established in 2022, supported by the European Union and based in the Dominican Republic, offers training and capacity-building in addressing cybersecurity and cybercrime to Latin American and Caribbean States. Activities include the provision of training materials and courses, awareness-raising and support to policymakers on national cybersecurity and digital transformation and on national and regional consultations on cybersecurity issues. Bilateral efforts have also been launched to support the establishment of national computer emergency response teams, including a project of the Brazilian Cooperation Agency in support of the creation of a cybersecurity incident response centre in Suriname.

66. From 2016 to 2019, the Global Cybersecurity Capacity Programme financed by the Republic of Korea and World Bank Partnership Facility provided tailored national and regional technical assistance to a cross-regional group of six States.[40] Each participating State underwent an assessment against the Cybersecurity Capacity Maturity Model for Nations, on the basis of which analytical reports, training, workshops and technical assistance were provided. The project was aimed at assisting participating States to strengthen the national cybersecurity environment, with the engagement of cybersecurity policymakers and relevant stakeholders. Impact assessments measured the effectiveness of interventions.

Additional areas of capacity-building

67. Capacity-building efforts in other cross-cutting and thematic areas are ongoing, including with a focus on specific groups such as women, youth, academics and industry. Other areas of focus include public awareness-raising, digital access and literacy and combating cybercrime.

[39] See www.internationalcybertech.gov.au/our-work/capacity-building.

[40] See www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp.

Gender and women's participation

68. Launched in 2020, the Women in International Security and Cyberspace Fellowship is a joint initiative of Australia, Canada, Netherlands (Kingdom of the), New Zealand, the United Kingdom and the United States.[41] It supports the attendance of women diplomats at sessions of the related intergovernmental processes under the auspices of the United Nations, including the open-ended working group on security of and in the use of information and communications technologies, and hosts negotiation skills training and workshops. In its second edition, the programme supports 35 women diplomats representing countries from across ASEAN, Asia and the Pacific, South America and the Commonwealth to participate in the meetings of the open-ended working group. Fellows also receive training from the United Nations Institute for Training and Research on multilateral negotiations, participate in an introduction to issues relevant to international security in cyberspace and receive mentoring from senior colleagues working on these issues at the United Nations in New York.

69. ITU currently manages a programme entitled "Her Cybertracks" that promotes the equal, full and meaningful representation of women in the field of cybersecurity.[42] The programme supports participants in building skills to engage in national and international cybersecurity policymaking, enhancing awareness and reducing barriers to women's participation in the field and increasing the participation and representation of women in the cybersecurity workforce. In South-East Asia, ITU has delivered a project to enhance the development of standards and frameworks in critical technologies that support women's engagement, inclusion and empowerment. The project supports policymaking, standards, frameworks and initiatives to mitigate biases and build trust and inclusion. The project deployed initially in Indonesia, Malaysia, the Philippines and Thailand, with a view to expanding to other States in the region.

70. ITU also offers a Women in Cyber Mentorship Programme. The first edition of the Programme was launched in 2021 on International Women's Day and was jointly organized by ITU, the Forum of Incident Response and Security Teams and the Equals Global Partnership for Gender Equality in the Digital Age (also known as EQUALS). Since its establishment, almost 300 women have been trained and mentored across 73 countries through the scheme.

Engagement of youth and awareness-raising

71. In order to raise awareness, engage and build the capacity of youth interested in information and communications technologies security, the computer emergency response team of Türkiye hosted a 24-hour online capture-the-flag cybersecurity competition, referred to as "Cyber Star ". Over 20,000 participants competed in the 2019 iteration, in teams and individually. The computer emergency response team also operates a cyberprogramme, referred to as "FETİH" to further develop skills of trainees who are aiming to enter the field.

72. Some States have noted efforts at the national level to raise awareness of the importance of good practices in the area of cybersecurity. For example, during the month of October, the National Guard of Mexico promotes activities as part of a national cybersecurity week, which is aimed at bringing together representatives of all relevant sectors to share good practices and experiences around the protection of

[41] See https://eucyberdirect.eu/good-cyber-story/women-and-international-security-in-cyberspace-fellowship.

[42] See www.itu.int/en/ITU-D/Cybersecurity/Pages/Women-in-Cyber/HerCyberTracks/Her-CyberTracks.aspx.

critical infrastructures, citizen security in cyberspace, the digital economy, privacy, and the harmonization of national legislative frameworks.

Engagement with industry and the private sector

73. States have variously underscored the value of public-private partnerships and engaging with industry partners to build cyberresilience. States have noted their efforts to conduct consultations with key public and private organizations to assess the overall level of national cybersecurity. In October 2023, the Kuban Cybersecurity Conference hosted representatives of higher educational institutions, State and municipal authorities, heads of infrastructure enterprises and facilities of the Russian Federation and members of the international community to discuss challenges, tasks and trends. The event also hosted a youth-focused competition under the title "KubanCTF-2023".[43]

74. Google has developed a cybersecurity road map for the consideration of States, drawing from lessons learned and best practices building global cloud and security solutions for governments and individual users. The aim of the road map is to support States in developing national cybersecurity strategies for the protection of critical infrastructure, citizens and economic prosperity.[44]

Resources and studies from academic institutions

75. The Hague Programme on International Cyber Security produces research on digital developments and cyber norms, hosts an annual academic conference and prepares a digest of academic research and debate.[45] Recent publications covered such themes as multi-stakeholder engagement in cybersecurity norm-making processes and responsible behaviour in cyberspace.

76. The Cybersecurity Capacity Maturity Model for Nations defines five dimensions of cybersecurity maturity and the steps necessary to reach them. The Model has been deployed more than 130 times in over 90 States since 2015, facilitated by the Global Cyber Security Capacity Centre in cooperation with international organizations, regional and other partner organizations. Looking ahead, the Global Cyber Security Capacity Centre is developing an additional metric as part of the Model to measure artificial intelligence capacities so as to support States in adapting to and employing artificial intelligence safely and sustainably.

Digital development, access and literacy

77. The United Nations Development Programme (UNDP) implements a variety of initiatives to support the building of digital infrastructure, promotion of digital literacy or implementation of e-governance solutions.[46] UNDP has introduced the digital readiness assessment with the aim of identifying and prioritizing digital interventions as part of a country's digital transformation journey. The assessment highlights the current digital context of a country – from a context where basic digital foundations may be lacking, or incomplete, through to the case of a country where digital is a central tenet of national growth and development (referred to as stages of digital readiness).

78. The Digital Access Programme of the Government of the United Kingdom of Great Britain and Northern Ireland seeks to catalyse more inclusive, affordable, safe

[43] See https://kubcsc.ru/en#events.

[44] See https://safety.google/intl/en_uk/.

[45] See www.thehagueprogram.nl/.

[46] See www.undp.org/digital.

and secure digital access for communities in Brazil, Indonesia, Kenya, Nigeria and South Africa.[47]

79. The Initiative for Digital Government and Cybersecurity in Horn of Africa Countries supports the Governments of Djibouti, Kenya and Somalia in strengthening e-governance and developing human-centred e-services. In July 2023, in partnership with Smart Africa through the Smart Africa Digital Academy, Burkina Faso organized certification training courses in cloud computing and cybersecurity.

80. The ITU “Cyber4Good” initiative aims to facilitate access to digital services and tools in the least developed countries, with the participation of private sector actors and the support of the Republic of Korea.[48] An output of the project will be the establishment of an ITU Cybersecurity Development Fund, operating in line with a governance model and under the direction of an advisory board. The Cyber Resilience for Development programme of the European Union supports public and private actors in strengthening cybersecurity and resilience on a global scale.[49]

81. The Digital Development Partnership of the World Bank supports inclusive digital transformation in over 80 countries globally.[50] The cybersecurity multi-donor trust fund, launched in 2021 and supported by Estonia, Germany, Japan and Netherlands (Kingdom of the), supports the digital development programme through research, programme support, risk assessment and mitigation in critical infrastructure and high-risk sectors. In cooperation with the African Union, the Digital Economy for Africa initiative of the World Bank supports the implementation of the African Union Digital Transformation Strategy, 2020–2030. Building on foundational pillars such as digital infrastructure, services, skills, a conducive policy and regulatory environment and innovation and entrepreneurship, the strategy identifies cybersecurity, privacy and personal data protection as a cross-cutting theme. It outlines detailed propositions to build capacity in digital development, access and literacy, including the promotion of human and institutional capacity-building through public awareness campaigns, professional training, research and development and computer emergency response teams.[51]

Combating cybercrime

82. The Global Programme on Cybercrime in the United Nations Office on Drugs and Crime was established in 2013. The mandate is set out in General Assembly resolution 65/230 and the Commission on Crime Prevention and Criminal Justice resolutions 22/7 and 22/8. The Global Programme has been operating on the basis of those resolutions, while it should be noted that a treaty is currently being negotiated by the General Assembly. The programme addresses the interrelated aspects of combating cybercrime: prevention, detection, investigation, prosecution and sentencing or adjudication.

83. The International Criminal Police Organization (INTERPOL), through its multi-stakeholder Cyber Fusion Centre, is currently leading the development and delivery of law enforcement-specific technical assistance and capacity-building for information and communications technologies and cybercrime issues. The Cyber Fusion Centre helps member countries to identify cyberthreats, develop prevention and disruption strategies and coordinate their response to such threats.

[47] See www.oecd.org/development-cooperation-learning/practices/leaving-no-one-behind-in-a-digital-world-the-united-kingdom-s-digital-access-programme-e8b15982/.

[48] See www.itu.int/net4/ITU-D/CDS/projects/display.asp?ProjectNo=2GLO21119.

[49] See https://cyber4dev.eu/.

[50] See www.digitaldevelopmentpartnership.org/.

[51] See www.worldbank.org/en/programs/all-africa-digital-transformation.

Combating the use of information and communications technologies for terrorist purposes

84. The Global Counter-Terrorism Programme on Cybersecurity and New Technologies assists Member States and international and regional organizations in developing and implementing effective responses to emerging challenges and opportunities provided by information and communications technologies in countering terrorism. The Programme is aimed at developing knowledge and raising awareness, as well as enhancing skills and capacities required for implementing policy responses, protecting critical infrastructure from terrorist activity involving information and communications technologies, and enhancing criminal justice capacities. More than 4,000 officials from 150 Member States have been trained through the Programme, with over 60 capacity-building workshops, and 12 knowledge products have been published as part of the Programme. Cybersecurity capacity-building assistance in the form of counter-terrorism cyberdrills and tabletop exercises has also been delivered as part of the Programme.

V. Observations and conclusions of the Secretariat

85. Capacity-building in the area of information and communications technologies in the context of international security rightly remains among the highest priorities of States. Capacity-building largely underpins the efforts undertaken across all related matters addressed by the open-ended working group on security of and in the use of information and communications technologies 2021–2025, namely addressing existing and emerging threats and unpacking the applicability of international law to State use of such technologies and promoting confidence-building measures. Many States have also emphasized the importance of addressing capacity-building in any future regular institutional dialogue under the auspices of the United Nations on information and communications technologies security. **In this regard, capacity-building should remain a fundamental and cross-cutting pillar of all related discussions by States at the United Nations on information and communications technologies security. Achieving progress in all related areas, from norms to international law to confidence-building measures, will require dedicated resources to implement corresponding capacity-building measures.**

86. The Secretary-General has underscored the critical importance of investing in digital literacy and digital infrastructure to close the digital divide (A/75/982). Likewise, States have continued to emphasize that the benefits of digital technology were not enjoyed equally by all and accordingly underlined the need to give due attention to the growing digital divide in the context of accelerating the implementation of the Sustainable Development Goals, while respecting the national needs and priorities of States. **Therefore, it is essential that capacity-building in the area of information and communications technologies effectively serves the needs and priorities of all States, particularly developing countries, with a view to closing the digital divide, including the gender digital divide. Capacity-building efforts should also serve as an enabler of sustainable development.**

87. The impact of rapid advances in science and technology on international peace and security is not yet fully known. The opportunities and risks created by the rapid development of emerging technologies, including artificial intelligence and quantum technologies, are expected to have profound implications for States' capacity-building needs and priorities at the technical and policy levels. On the one hand, the use of information and communications technologies capabilities, such as enhanced threat detection and analysis, automated incident response, enhanced malware detection and fraud detection and prevention tools, require increased capacity. On the other hand,

capacity-building efforts are crucial for States to have the necessary knowledge and skills to tackle challenges such as artificial intelligence-enabled malicious information and communications technologies activities, bias and discrimination that are inherent to artificial intelligence systems, and transparency issues. **Concrete capacity-building initiatives could focus on building literacy and expertise on the impacts of these emerging technologies, developing national strategies on the responsible design, development and use of emerging technologies, and international cooperation mechanisms to enhance cyberresilience through the transfer of knowledge, best practices and lessons learned.**

88. An ongoing challenge to effective and sustainable capacity-building efforts remains the potential for duplication. In this context, it is worthwhile to note that in decision 630 of the International Telecommunication Union Council, adopted in August 2023, ITU was mandated to develop a resource for Member States that includes, inter alia, information about capacity-building programmes that it implements, as well as other relevant programmes.[52] The resource is requested to be updated to take into account new challenges and developments. States have regularly raised the issue of harnessing synergies and leveraging existing initiatives in this regard. **In the light of the universal nature of the open-ended working group on security of and in the use of information and communications technologies, States are encouraged to use the dedicated intergovernmental process to further unpack how to avoid duplication with a view to the best possible matching of needs with resources.**

[52] Available at www.itu.int/md/S23-CL-C-0124/en.