



PERMANENT MISSION OF THE REPUBLIC OF SINGAPORE
UNITED NATIONS | NEW YORK

12 July 2023

Excellency,

I have the honour of addressing you in my capacity as Chair of the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025 (OEWG), established pursuant to General Assembly resolution 75/240 adopted on 31 December 2020.

I would like to once again express my appreciation to delegations for their contributions at the virtual open-ended informal “town-hall” meeting held on 27 June 2023 to discuss the Zero Draft of the second Annual Progress Report (APR) of the OEWG. The comments made at the “town-hall” were thoughtful and constructive, and provided me with much material for further reflection. I would also like to thank the various delegations that subsequently submitted written comments further elaborating their positions and suggesting improvements to the Zero Draft.

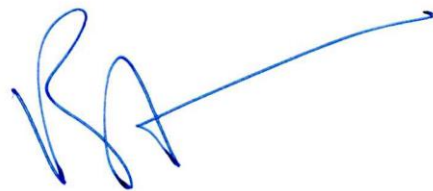
Having thoroughly reviewed the comments made at the “town-hall” and the written inputs received, I am pleased to issue a revised draft of the second APR (Rev. 1) ahead of the fifth substantive session of the OEWG taking place from 24 to 28 July 2023. In preparing the Rev. 1 draft, I have carefully considered how best to incorporate the full range of views and preferences expressed by delegations, while working towards a balanced text that could potentially command consensus. I hope all delegations will consider the Rev. 1 draft from this perspective, and exercise flexibility and understanding in this regard.

As I indicated in my letter dated 30 June 2023, I have allocated time at the fifth substantive session for a first and second reading of the draft second APR. To make the most productive use of the time we have available, I encourage delegations to review the Rev. 1 draft over the coming days and come prepared for the first reading. In considering your responses to the Rev. 1 draft at the first reading, I urge delegations to approach our discussions not only from the perspective of your delegation’s preferences, but also from the perspective of what could ultimately command consensus

amongst all delegations. I ask delegations to bear in mind that in a consensus process, it is neither possible nor realistic to expect that we can fully satisfy the preferences of each and every delegation. In this regard, I hope all delegations will exercise restraint in any changes you may propose to the Rev. 1 draft, given that such a spirit of moderation on the part of delegations will be a vital element in our efforts to reach consensus.

I look forward to continuing to work closely with delegations to adopt a meaningful and substantive second APR by consensus at the fifth substantive session of the OEWG, in accordance with our mandate as established in General Assembly resolution 75/240.

Please accept, Excellency, the assurances of my highest consideration.



Burhan Gafoor

Chair

Open-Ended Working Group on
security of and in the use of
information and
communications technologies
2021-2025

All Permanent Representatives and Permanent Observers to the United Nations
New York

Enclosure:

- Annex A – Rev. 1 draft of the second Annual Progress Report of the OEWG

SECOND ANNUAL PROGRESS REPORT OF THE OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES 2021–2025, SUBMITTED TO THE 78TH SESSION OF THE GENERAL ASSEMBLY PURSUANT TO GENERAL ASSEMBLY RESOLUTION 75/240

A. Overview

1. The fourth and fifth formal sessions as well as informal intersessional meetings of the Open-ended Working Group (OEWG) on the security of and in the use of Information and Communications Technologies (ICTs) 2021-2025 took place in a geopolitical environment that remains challenging, with rising concerns over the malicious use of ICTs by State and non-state actors that impact international peace and security.
2. At these sessions, States recalled the consensus decisions and resolutions of the General Assembly in which States agreed they should be guided in their use of ICTs by the OEWG and GGE reports.¹ In this regard, States further recalled the contributions of the first OEWG, established pursuant to General Assembly Resolution 73/27, which concluded its work in 2021, through its final report agreed by consensus,² as well as noted the Chair's summary and list of non-exhaustive proposals annexed to the Chair's summary, and recalled the contributions of the sixth Group of Governmental Experts (GGE), established pursuant to General Assembly Resolution 73/266, which concluded its work in 2021, through its final report agreed by consensus.³
3. Furthermore, States reaffirmed the consensus first annual progress report (APR) of the current OEWG,⁴ the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security and the consensus reports of the 2010, 2013, 2015, and 2021 GGEs.⁵ States recalled and reaffirmed that the reports of these Groups "recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time", and that "specific confidence-building, capacity-building and cooperation measures were recommended". States also recalled and reaffirmed that "international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment".⁶ These elements consolidate a cumulative and evolving framework⁷ for responsible State behaviour in the use of ICTs providing a foundation upon which the current OEWG builds its work.

¹ GA decisions 77/512 and 75/564, GA resolutions 70/237 and 76/19.

² A/75/816.

³ A/76/135.

⁴ A/77/275.

⁵ A/65/201, A/68/98, A/70/174 and A/76/135.

⁶ Report of the 2021 OEWG, A/75/816, Annex I, para 7.

⁷ Report of the 2021 GGE, A/76/135, para 2, consensus GA resolution 76/19.

4. The OEWG recalled its mandate contained in General Assembly resolution 75/240 as follows: “Acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour; to consider initiatives of States aimed at ensuring security in the use of information and communications technologies; to establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States; to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, *inter alia*, data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the General Assembly at its eightieth session.” In this regard, the OEWG acknowledged the importance of addressing its mandate in a balanced manner and the need to give due attention to both further develop common understandings between States on security in the use of ICTs, as well as to further the implementation of existing commitments.
5. The OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner, in accordance with the modalities agreed by silence procedure on 22 April 2022 and formally adopted at the first meeting of the third session of the OEWG on 25 July 2022, and in line with its mandate contained in General Assembly Resolution 75/240 to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia.
6. The OEWG recognized that regional and sub-regional organizations could continue to play an important role in implementing the framework for responsible State behaviour in the use of ICTs. In addition, regional, cross-regional and inter-organizational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. As not all States are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to its work.
7. The OEWG welcomed the high level of participation of women delegates in its sessions and the prominence of a gender perspectives in its discussions.⁸ The OEWG underscored the importance of narrowing the “gender digital divide” and of promoting the full, equal and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security.
8. This second APR includes concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment, and in this regard builds upon the first APR (A/77/275), endorsed by consensus in General Assembly Decision 77/512. In recognition that the OEWG is in the process of on-going deliberations and that substantive discussions under the OEWG will continue until the completion of its mandate in 2025, this second APR of the Group is not intended to be a comprehensive summary of discussions by States, but

⁸ Report of the 2021 OEWG, A/75/816, Annex I, para 12.

aims to capture concrete progress made at the OEWG to date, building also on the roadmap for discussion contained within the first APR. This second APR will be submitted to the General Assembly pursuant to the OEWG's mandate contained in resolution 75/240.

B. Existing and Potential Threats

9. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on existing and potential threats. States, recalling the threats identified in the first APR, the 2021 OEWG report and the GGE reports, reiterated increasing concern that threats in the use of ICTs in the context of international security have intensified and evolved significantly in the current challenging geopolitical environment.
10. States recalled that a number of States are developing ICT capabilities for military purposes.⁹ They also recalled that the use of ICTs in future conflicts between States is becoming more likely, **and expressed concern that ICTs have already been used in conflicts in different regions**. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States.¹⁰

[10 bis] **States further expressed particular concern regarding the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII), including CI and CII that provide essential services across borders and jurisdictions, which can have cascading domestic, regional and global effects, as well as malicious ICT activities that target humanitarian organizations. The vulnerability of the healthcare, maritime and aviation sectors was particularly noted.** [Text moved from below, with amendments]

[10 ter] **States also highlighted that malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern.**¹¹

[10 quater] **States also expressed concern regarding misinformation and disinformation (including through the use of deepfakes), data security, the exploitation of ICT product vulnerabilities and the use of harmful hidden functions in particular where these issues impact international peace and security. In this regard, States also noted the significant threat posed by malicious ICT activities targeting supply chains. States also highlighted the risk posed by malicious ICT tools and techniques such as ransomware, wiper malware, phishing and trojans.** [Text moved from below, with amendments]

⁹ Report of the 2021 OEWG, A/75/816, Annex I, para 16.

¹⁰ Report of the 2021 OEWG, A/75/816, Annex I, para 16.

¹¹ Report of the 2021 OEWG, A/75/816, Annex I, para 18.

11. States further expressed concern at the irresponsible and potentially malicious use of commercially available ICT capabilities, as well as the proliferation, **including by States,** of ICT capabilities that can be utilized by malicious actors, including through the growth of illegal markets **and open sources** offering access to, *inter alia*, software vulnerabilities, spyware, sophisticated high-end offensive ICT tools and “hacker for hire” services.
12. ~~States further expressed particular concern over the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII), including CI and CII that provide essential services across borders and jurisdictions, as well as malicious ICT activities that targeted humanitarian organisations. The vulnerability of the healthcare, maritime and aviation sectors was particularly noted. In this regard, States also noted the significant threat posed by malicious ICT activities targeting supply chains. [Text moved above]~~
13. ~~States also expressed concern regarding misinformation, data security, the exploitation of ICT product vulnerabilities and the use of harmful hidden functions. They also highlighted the risk posed by malicious ICT tools and techniques such as ransomware, wiper malware, phishing and trojans, particularly where the reach and severity of ICT incidents utilizing such tools and techniques have the potential to impact international peace and security. [Text moved above]~~
14. States noted that developments in technology such as quantum computing and artificial intelligence, and the increasing reliance on cloud technology, while neutral in and of themselves, could **potentially have implications for the use of ICTs in the context of international security, including by increasing** ~~increase~~ vulnerabilities and expanding **ing ICT** ~~attack~~ vectors.
15. In view of the evolving landscape of threats in the use of ICTs in the context of international security and given the speed of technological development, a proposal was put forward to develop a **voluntary** repository of threats to ICT security in the context of international security. It was further proposed that such a repository could collate objective, **practical and neutral** information voluntarily contributed by States regarding threats in the use of ICTs in the context of international security in order to raise awareness ~~and facilitate a discussion on cooperative measures to address them.~~
16. States also drew attention to the ~~gender dimensions of~~ **need for a gender perspective in addressing** ICT threats and **to** the specific risks faced by vulnerable groups. States continued to emphasize that the benefits of digital technology were not enjoyed equally by all and accordingly underlined the need to address the growing digital divide in the context of accelerating the implementation of the sustainable development goals.
17. States recalled and reiterated that any use of ICTs by States in a manner inconsistent with their obligations under the framework of responsible State behaviour in the use of ICTs, which includes voluntary norms, international law, and CBMs, undermines international peace and security, trust and stability between States.

18. States 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 ICT activities may make them more vulnerable.¹² In light of the evolving landscape of threats in the use of ICTs in the context of international security, and recognizing that no State is sheltered from these threats, States underscored the urgency of raising awareness and deepening understanding of such threats, and of further developing and implementing cooperative measures¹³ under the cumulative and evolving framework for responsible State behaviour to address them.

Recommended next steps

19. States continue exchanging views at the OEWG on existing and potential threats to security in the use of ICTs with the potential to impact international peace and security, and discuss possible cooperative measures to address these threats, acknowledging in this regard that all States committing to and reaffirming observation and implementation of the framework for responsible State behaviour in the use of ICTs remains fundamental to addressing existing and potential ICT-related threats to international security.
20. States recognized the need to share objective information on ICT threats in the context of international security in an inclusive, accessible, ~~and universal~~ and neutral manner. In this regard, States to engage in focused discussions ~~on further developing the proposal for a repository of threats to ICT security as a way to explore proposals~~ to raise awareness and enhance information sharing among States on ICT threats in an objective, practical and neutral manner. ~~States to also consider how such a repository could be synergized with the information sharing foreseen between technical POCs in the global POC directory, as well as other existing relevant and appropriate information sharing and capacity building initiatives.~~
21. The OEWG to convene *a dedicated intersessional meeting* ~~focused discussions~~, with the participation of relevant experts invited by the OEWG Chair and with due consideration given to equitable geographical representation, on developments in new technologies such as quantum computing and artificial intelligence in order to exchange views and build knowledge on the potential impact of these technologies on the use of ICTs in the context of international security.

C. Rules, Norms and Principles of Responsible State Behaviour

22. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on rules, norms and principles of responsible state behaviour. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on ~~the~~ rules, norms and principles. The following is a non-exhaustive list of

¹² Report of the 2021 OEWG, A/75/816, Annex I, para 20.

¹³ Report of the 2021 OEWG, A/75/816, Annex I, para 22.

proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

- a) States underlined the importance of ~~voluntary norms f, g and h~~ on the protection of Critical Infrastructure (CI). States highlighted that ICT activity that intentionally damages CI or otherwise impairs the use and operation of CI to provide services to the public can have cascading domestic, regional and global effects.¹⁴ ~~It poses an elevated risk of harm to the population and can be escalatory, possibly leading to conflict.~~¹⁵ States thus emphasized the need to continue to strengthen measures, **including norms f, g and h**, to protect all CI from ICT threats, and proposed increased exchanges on best practices with regard to CI protection and recovery from ICT incidents involving CI.
- b) States continued to emphasize that cooperation and assistance could be strengthened to ensure the integrity of the supply chain and prevent the use of harmful hidden functions. Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include¹⁶:
 - i) “Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice.”¹⁷
 - ii) “Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels on supply chain risk management; developing and implementing globally interoperable common rules and standards for supply chain security; and other approaches aimed at decreasing supply chain vulnerabilities.”¹⁸
- c) States noted the role that the private sector plays in ensuring the integrity of the supply chain and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. It was proposed that, in addition to the steps and measures outlined above, States should continue to encourage the private sector and civil society to play an appropriate role to improve the security of and in the use of ICTs, including supply chain security for ICT products, **in accordance with the national laws and regulations of the countries within which they operate.**¹⁹
- d) States ~~proposed that~~ **discussed a proposal for a possible** glossary of technical ICT terms and terminologies ~~would~~ **that could** assist States in developing common understandings on rules, norms and principles. ~~In this regard, the establishment of a voluntary glossary of national definitions of technical ICT terms was proposed.~~

¹⁴ Report of the 2021 GGE, A/76/135, para 42, consensus GA resolution 76/19.

¹⁵ Report of the 2021 GGE, A/76/135, para 42, consensus GA resolution 76/19.

¹⁶ Report of the 2021 GGE, A/76/135, para 57, consensus GA resolution 76/19.

¹⁷ Report of the 2021 GGE, A/76/135, para 57(b), consensus GA resolution 76/19.

¹⁸ Report of the 2021 GGE, A/76/135, para 57(d), consensus GA resolution 76/19.

¹⁹ Report of the 2021 GGE, A/76/135, para 59, consensus GA resolution 76/19.

e) States underscored the need to further assist States in implementing the rules, norms and principles of responsible State behaviour. It was proposed that States could consider:

- i) Participating, on a voluntary basis, in the development and utilization of additional guidance or checklists on norms implementation, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE reports.
- ii) Identifying their capacity-building needs including by surveying, on a voluntary basis, their national implementation of rules, norms and principles of responsible State behaviour using the report of the Secretary-General on developments in the field of ICTs in the context of international security and/or the National Survey of Implementation as contained in the recommendations of the 2021 OEWG report.²⁰

[iii) bis] **Identifying and studying challenges associated with the implementation of the rules, norms, and principles of responsible State behaviour to better inform capacity-building efforts.**

- f) States proposed that a discussion could be convened under the OEWG to discuss (a) the elaboration of existing norms; and (b) the possibility that additional norms could continue to be developed over time, noting that the further development of norms and the implementation of existing norms were not mutually exclusive but could take place in parallel.²¹
- g) Regarding the consideration of proposals under this topic, States proposed to continue discussing the list of non-exhaustive proposals made on the elaboration of rules, norms and principles of responsible State behaviour (annexed to the Chair's Summary in the 2021 OEWG Report²²) further to the recommendation contained in the 2021 OEWG report.²³

Recommended next steps

- 23. States continue exchanging views at the OEWG with the aim of developing common understandings on, as well as facilitating the implementation of, rules, norms and principles of responsible State behaviour in the use of ICTs. States to also engage in focused discussions on the proposals from the non-exhaustive list in sub-paragraph 22(g) above at the sixth, seventh and eighth sessions of the OEWG.**
- 24. At the sixth, seventh and eighth sessions of the OEWG, States to also undertake focused discussions on: (a) strengthening measures to protect CI from ICT threats, including exchanges on best practices with regard to CI protection and the recovery from ICT incidents involving CI;**

²⁰ Report of the 2021 OEWG, A/75/816, Annex I, paras 64 and 65.

²¹ Report of the 2021 OEWG, A/75/816, Annex I, para 29.

²² Report of the 2021 OEWG, A/75/816, Annex II.

²³ Report of the 2021 OEWG, A/75/816, Annex I, para 33.

(b) further cooperation and assistance to ensure the integrity of the supply chain and prevent the use of harmful hidden functions.

25. ~~States agree to establish a voluntary glossary of national definitions of technical ICT terms to promote mutual understanding.~~ States are encouraged, on a voluntary basis, to share submit national definitions of commonly-used technical ICT terms drawn from previous consensus reports, including, *inter alia*, the following terms: (a) ICTs; (b) ICT infrastructure; (c) ICT environment; and (d) malicious use of ICTs, ~~to~~ with the UN Secretariat, which is requested to ~~make the voluntary glossary of national definitions available~~ compile the submissions on the OEWG website.
26. States agree to elaborate additional guidance on the implementation of norms, taking into account previous agreements, including the 2021 GGE report. Such additional guidance would include the development of a norms implementation checklist to assist States, in particular developing countries and small States, in their efforts to implement the norms of responsible State behaviour in the use of ICTs. The OEWG Chair is requested to produce an initial draft of such a checklist for consideration by States, including by drawing on the experiences of relevant efforts currently underway on the development of such checklists.
27. The OEWG Chair is requested to convene an informal intersessional meeting to discuss (a) the elaboration of existing norms; and (b) the possible development of additional norms ~~possibility that additional norms could continue to be developed over time~~. In this regard, the OEWG Chair could invite relevant experts from regional and sub-regional organizations, businesses, non-governmental organizations and academia, with due consideration given to equitable geographical representation, to give ~~make~~ briefings at these discussions.

D. International Law

28. During the fourth and fifth as well as informal sessions of the OEWG, States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, and further reaffirming that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability and promoting an open, secure, stable, accessible and peaceful ICT environment, continued discussions on how international law applies to the use of ICTs. The OEWG held, for the first time, focused discussions on topics from the non-exhaustive list in sub-paragraphs 15(a)-(b) of the first APR as well as proposals contained in the 2021 OEWG report and Chair's summary, where relevant.²⁴

[28 bis] In undertaking these focused discussions, States were guided by the recommendation in the first APR that States engage in focused discussions on topics from the non-exhaustive list in the following paragraphs²⁵:

²⁴ First Annual Progress Report of the OEWG, A/77/275, International Law Section, Recommended Next Steps 2.

²⁵ First Annual Progress Report of the OEWG, A/77/275, para 15(b)(i) and 15b(ii), and International Law section, Recommended Next Steps 2.

- a) *“The OEWG could convene discussions on specific topics related to international law. Such discussions should focus on identifying areas of convergence and consensus. A non-exhaustive, open list of topics proposed by States for further discussion under international law includes: How international law, in particular the Charter of the United Nations, applies in the use of ICTs; sovereignty; sovereign equality; non-intervention in the internal affairs of other States; peaceful settlement of disputes; State responsibility and due diligence; respect for human rights and fundamental freedoms; whether gaps in common understandings exist on how international law applies; and proposals contained in the 2021 OEWG report and Chair’s summary where relevant.”*
- b) *The OEWG noted the recommendations in the 2021 OEWG report and 2021 GGE report respectively as follows:*
 - i) *“Throughout the OEWG process, States participated consistently and actively, resulting in an extremely rich exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States, including the possibility of additional legally binding obligations. The diverse perspectives are reflected in the attached Chair’s Summary of the discussions and specific language proposals under agenda item “Rules, norms and principles”. These perspectives should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240.”*²⁶ [Text moved from below]
 - ii) *“The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognized the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict.”*²⁷ [Text moved from below]

29. At the OEWG’s ***focused*** discussions on how international law applies to the use of ICTs, States, *inter alia*:

- a) Reaffirmed the principles of State sovereignty and sovereign equality.
- b) Reaffirmed Articles 2(3) and 33(1) of the UN Charter which state respectively that “all Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”²⁸ and that “the parties to any dispute, the

²⁶ Report of the 2021 OEWG, A/75/816, Annex I, para 80.

²⁷ Report of the 2021 GGE, A/76/135, para 71(f), consensus GA resolution 76/19.

²⁸ Article 2(3) of the Charter of the United Nations.

continuance of which is likely to endanger the maintenance of international peace and security, shall, first of all, seek a solution by negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice”.²⁹

- c) Reaffirmed Article 2(4) of the UN Charter which states that “all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations”.
- d) Further reaffirmed that in accordance with the principle of non-intervention, States must not intervene directly or indirectly in the internal affairs of another State, including by means of ICTs.³⁰
- e) ~~At the OEWG discussions on how international law applies to the use of ICTs, States also recalled the recommendations in the 2021 OEWG report and 2021 GGE report as noted in the first APR³¹ as follows:~~
 - i) ~~Throughout the OEWG process, States participated consistently and actively, resulting in an extremely rich exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States, including the possibility of additional legally binding obligations. The diverse perspectives are reflected in the attached Chair’s Summary of the discussions and specific language proposals under agenda item “Rules, norms and principles”. These perspectives should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240.”;³² [text moved above]~~
 - ii) ~~“The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognized the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict.”³³ [text moved above]~~

²⁹ Article 33(1) of the Charter of the United Nations.

³⁰ Report of the 2021 GGE, A/76/135, para 71(c), consensus GA resolution 76/19.

³¹ First Annual Progress Report of the OEWG, A/77/275, para 15(b)(i) and 15b(ii).

³² ~~Report of the 2021 OEWG, A/75/816, Annex I, para 80.~~

³³ ~~Report of the 2021 GGE, A/76/135, para 71(f), consensus GA resolution 76/19.~~

30. States, ~~reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs,~~ also made additional concrete, action-oriented proposals on international law as follows:
- a) States noted that the intersessional discussions deepened and enriched ongoing discussions on how international law applies to the use of ICTs and proposed additional sessions to be convened in the next intersessional period of the OEWG.
 - b) States further noted that state practice as well as the studies and opinions of international legal bodies could contribute to common understandings of how international law applies in the use of ICTs and encouraged the continued sharing of national views on international law including on state practice related to the use of ICTs by States.
 - c) States also further underscored the urgent need for continued capacity-building efforts in the area of international law including with the aim of ensuring that all States are able to participate on an equal footing on the development of common understandings on how international law applies in the use of ICTs. Such capacity-building efforts could include workshops, training courses, exchanges on best practices at the international, inter-regional, regional and sub-regional levels, as well as draw from the experiences of relevant regional organizations, as appropriate.

Recommended next steps

31. States continue to engage in focused discussions at the OEWG on how international law applies in the use of ICTs *drawing from topics from the non-exhaustive list in sub-paragraphs 28 bis (a) and 28 bis (b) above as well as proposals on the topic of international law contained in the 2021 OEWG report and Chair's summary, where relevant.*
32. Building on discussions at the fourth and fifth sessions of the OEWG, States are invited to continue to voluntarily share their national views as well as relevant state practice on how international law applies in the use of ICTs. The UN Secretariat is requested to compile these views, as well as national views previously submitted to the OEWG, and to make these views available in a compendium posted on the OEWG website for the reference of all States and for further discussions by the OEWG at its sixth, seventh and eighth sessions.
33. *The OEWG Chair is also requested to convene a dedicated intersessional meeting on how international law applies in the use of ICTs. In this context, the OEWG Chair could, with due consideration given to equitable geographical representation, further arrange expert briefings from representatives of relevant international legal bodies on how international law applies in the use of ICTs in order to better inform the OEWG's deliberations. States to undertake additional focused discussions on international law topics from the non-exhaustive list in paragraphs 28 and 29 above as well as proposals on the topic of international law contained in the 2021 OEWG report and Chair's summary. The OEWG Chair is also requested to convene*

~~informal intersessional meetings on these topics.~~

34. States in a position to do so to continue to support, in a neutral and objective manner, additional efforts to build capacity in the areas of international law, ~~and national legislation and policy~~, in order for all States to contribute to building common understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community. Such capacity-building efforts should be undertaken in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.

E. Confidence-Building Measures

35. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on confidence-building measures (CBMs). States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on CBMs. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:
- a) Recalling that in the first APR States agreed to establish, building on work already done at the regional level, a global, inter-governmental, points of contact (POC) directory,³⁴ States proposed that the OEWG should agree to adopt the paper entitled “Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory” as contained in Annex A of this report as the next steps in the operationalization of the global POC directory.
 - b) States recognized that the establishment and operationalization of the global POC directory is an important step forward in building confidence between States at the global level. States further recognized that the global POC directory can provide a framework for the implementation of other CBMs at the global level that could help to promote an open, secure, stable, accessible and peaceful ICT environment. In this regard, States, recalling the recommendations for CBMs contained in consensus reports, proposed that an initial list of voluntary, global CBMs could be drawn from these reports for implementation by States, including through the global POC directory.
 - c) In addition to already agreed CBMs contained in previous UN reports, States also proposed additional measures which could over time also be recognized as additional CBMs at the global level. These include the following four proposals for CBMs building upon the global POC directory, noting that all of these proposals have also been included as operational elements in the paper contained in Annex A of this report:

³⁴ First Annual Progress Report of the OEWG, A/77/275, Confidence Building Measures section, Recommended next steps, para 2.

- i. Communication checks in the form of “Ping” tests;
 - ii. Voluntary information-sharing, particularly in the event of ~~urgent and significant~~ ICT security incidents **with possible implications for international peace and security**, facilitated through the global POC directory;
 - iii. Tabletop exercises to simulate practical aspects of participating in a global POC directory; and
 - iv. Regular in-person or virtual meetings of POCs to share practical information and experiences on the operationalization and utilization of the global POC directory.
- d) States highlighted the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery, responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.³⁵ It was proposed that this issue could be further discussed within the OEWG.
- e) It was proposed that aspects of confidence-building could continue to include engagement with regional and sub-regional organizations and interested stakeholders, including businesses, non-governmental organizations and academia where appropriate.
- f) States continued to emphasize that the OEWG itself served as a CBM, providing a forum for discussing issues on which there is agreement and issues on which there is not yet agreement.

Recommended next steps

- 36. States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs.**
- 37. Recalling that in the first APR of the OEWG, States agreed to establish a global, inter-governmental, points of contact (POC) directory,³⁶ States further agree to adopt the paper entitled “Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory” as contained in Annex A of this report as the next steps in the operationalization of the global POC directory.**
- 38. States to further discuss the operationalization and utilization of the global POC directory at the sixth, seventh and eighth sessions of the OEWG, including in the context of sub-paragraphs 35(b) and 35(c) of this report.**
- 39. States endorse the initial, non-exhaustive list of voluntary global CBMs, contained in Annex B, drawn from CBMs agreed by consensus in the 2021 OEWG report and in the first and second**

³⁵ Report of the 2021 GGE, A/76/135, para 60, consensus GA resolution 76/19.

³⁶ First Annual Progress Report of the OEWG, A/77/275, Confidence Building Measures section, Recommended next steps, para 2.

APRs of the current OEWG. The OEWG Chair is requested to facilitate continued discussions on how to develop, add to and operationalize these CBMs, including, *inter alia*, through (a) related capacity-building, and (b) the global POC directory.

F. Capacity-Building

40. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on ICT capacity-building in the context of international security. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on such capacity-building efforts. States stressed **that capacity-building is also an important confidence-building measure and a topic that cuts across all the pillars of the OEWG's work and** that a holistic approach to capacity-building in the context of ICT security was essential. In this regard, the need for sustainable, effective and affordable solutions was also emphasized. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:
- a) States proposed that the principles of capacity-building as adopted in the 2021 OEWG report³⁷ should be further mainstreamed into capacity-building initiatives on security in the use of ICTs. Furthermore, States continued to encourage efforts to promote gender-sensitive capacity-building efforts including through the integration of ~~the~~ a gender **perspective** ~~dimension~~ into national ICT and capacity-building strategies as well as the development of checklists or questionnaires to identify needs and gaps in this area.
 - b) States highlighted that short-term capacity-building on ICTs in the context of international security was required to address urgent threats and that long-term capacity-building was also required to address structural requirements and ensure sustainability. In this regard, the value of South-South, South-North, triangular, peer-to-peer and regionally-focused cooperation was also emphasized.

[b) bis] The OEWG could promote better understanding of the needs of developing States with the aim of narrowing the digital divide through tailored capacity-building efforts, so as to work towards ensuring that all States have the necessary capacity to observe and implement the initial framework for responsible State behaviour in the use of ICTs.³⁸
 - c) States underscored that further coordination of capacity-building efforts in ICT security was required and the UN could play an important role in this regard including through taking stock of States' capacity-building needs **and identifying capacity-building gaps** through tools and surveys and facilitating access by States to capacity-building programmes. It was proposed that the UN Secretariat collate existing capacity-building programmes and initiatives related to security in the use of ICTs within and outside of the United Nations and at the global and regional

³⁷ Report of the 2021 OEWG, A/75/816, Annex I, para 56.

³⁸ **First Annual Progress Report of the OEWG, A/77/275, paragraph 17(c).**

levels, to facilitate further discussions in the OEWG on ways to enhance greater synergy, coordination and access to capacity-building programmes offered.

- d) While recognizing existing funding for capacity-building efforts on security in the use of ICTs, States could at the same time continue to consider additional avenues of funding specifically targeted at capacity-building related to ICT security including through potential coordination and integration with existing development programmes and funds.
- e) States discussed the initiative to develop a Global Cyber Security Cooperation Portal (GCSCP), proposing that it could be practical and neutral, member State-driven and a modular “one-stop shop” tool for States, developed under the auspices of the UN. There were also suggestions that this portal could be synergized with other existing portals, such as those developed and maintained by UNIDIR and the Global Forum on Cyber Expertise (GFCE). States further proposed that a repository of best practices in ICT security capacity-building could be integrated into the initiative for a GCSCP. In this regard, States also stressed the importance of building knowledge and understanding of previous agreements in the OEWG and GGE reports to inform their current work.
- f) States recognized that the OEWG itself could be a platform to continue exchanging views and ideas related to ICT security capacity-building efforts including on how best to leverage existing initiatives in order to support States in developing institutional strength to implement the framework of responsible State behaviour in the use of ICTs. Building on the useful roundtable on capacity-building convened by the OEWG Chair in May 2023, it was further proposed that further roundtables on capacity-building could be convened under the auspices of the OEWG, with the participation of relevant stakeholders and practitioners to exchange best practices on capacity-building related to international ICT security. **In this regard, it was proposed that States could discuss the development of an initial list of capacities required by States for the implementation of the framework of responsible State behaviour in the use of ICTs.**
- g) States, including through the OEWG, could continue to strengthen coordination and cooperation between States and interested stakeholders, including businesses, non-governmental organizations and academia. States noted that stakeholders are already playing an important role through partnerships with States for the purposes of training, research, and facilitating access to internet and digital services. States further recognized that capacity-building was also required on how to identify and engage meaningfully with stakeholders in order to strengthen policy making and establish trust to cooperate with stakeholders in addressing ICT security incidents.

Recommended next steps

- 41. States continue exchanging views at the OEWG on capacity-building related to security in the use of ICTs, including on sub-paragraphs 40(a) to 40(g) above. States to also continue focused discussions on how the principles of capacity-building as adopted in the 2021 OEWG report**

(reproduced in Annex C) can be further mainstreamed within capacity-building initiatives on security in the use of ICTs.

42. The OEWG Chair is requested to engage with relevant UN entities and international organizations offering capacity-building programmes on security in the use of ICTs and encourage them to align their capacity-building programmes, where relevant and appropriate and in accordance with their respective mandates, to further support States in their implementation of the framework for responsible state behaviour in the use of ICTs and efforts to build an open, secure, stable, accessible and peaceful ICT environment.
43. The UN Secretariat is requested to conduct a “mapping exercise” 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 UN Secretariat is further requested to produce a report with the findings of this “mapping exercise”, and to present this report at the seventh session of the OEWG to support States’ efforts to take stock of existing ICT security capacity-building efforts and to encourage further synergies and coordination between such efforts.
44. States to continue to discuss the proposal for a Global Cyber Security Cooperation Portal (GCSCP) as a “one-stop shop” tool for States, developed under the auspices of the UN. Further discussions could take place on how to synergize this portal with other existing portals such as those developed and maintained by UNIDIR and GFCE.
45. The OEWG Chair is requested to convene a dedicated Global Roundtable meeting on ICT security capacity-building during the intersessional period to allow for an exchange of information and best practices. This roundtable meeting could include capacity-building practitioners as well as representatives of interested States, and interested stakeholders, including businesses, non-governmental organizations and academia, with due consideration given to equitable geographical representation.
46. In order to build knowledge and understanding of previous agreements in the OEWG and GGE reports which would inform the current work of States at the OEWG, States in a position to do so are encouraged to support the UN Secretariat in updating the Cyber Diplomacy e-learning course for diplomats, with the aim of producing an updated course in 2024. The UN Secretariat is requested to update States ~~on the progress of the course update~~ at the sixth session of the OEWG.
47. Interested States are encouraged to develop and share voluntary checklists and other tools to assist States in mainstreaming the capacity-building principles from the 2021 OEWG report into capacity-building initiatives related to ICT security, as well as to develop and share tools that would assist States in incorporating a gender dimension perspective into such capacity-building efforts.

48. States in a position to do so are invited to continue to support capacity-building programmes, including in collaboration, where appropriate, with regional and sub-regional organizations and other interested stakeholders, including businesses, non-governmental organizations and academia.

G. Regular Institutional Dialogue

49. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on regular institutional dialogue. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on regular institutional dialogue. This non-exhaustive list of proposals with varying levels of support from States may be further elaborated upon and supplemented at forthcoming OEWG sessions:
- a) States continued to underscore that the OEWG could play a role in raising awareness, building trust and deepening understanding in areas where no common understandings have yet emerged. Furthermore, the OEWG should build incrementally on previous agreements. States recognized the centrality of the OEWG as the mechanism within the United Nations for dialogue on security in the use of ICTs.³⁹
 - b) Further to the recommendation in **the 2021 OEWG report⁴⁰ and in** the first APR of the OEWG⁴¹, States continued to discuss the proposal to establish a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs in the context of international security. States also discussed the relationship between the PoA and the OEWG, and the scope, content and structure of a PoA. States highlighted that the PoA aims to strengthen international security and stability in the ICT security domain through actionable proposals and enhanced support for tailored capacity-building efforts. The PoA would be established as a permanent, action-oriented, inclusive, transparent, and results-based mechanism, building on previous outcomes and in line with the cumulative and evolving framework.
 - c) A proposal was ~~also made for establishing a future permanent group, commission, or conference, or convention which would address the full range of issues on the security of and in the use of ICTs, and focus on practical implementation of the current OEWG's recommendations. The mandate of such a group might include~~ **that might consider** the implementation of rules, norms and principles ~~including by preparing a draft legally binding international instrument on ICTs, confidence-building measures and the establishment of mechanisms to assist States in enhancing their ICT capacities.~~

[c] bis] **States recalled the recommendation of the 2021 OEWG Report that: "Throughout the OEWG process, States participated consistently and actively, resulting in an extremely rich**

³⁹ First Annual Progress Report of the OEWG, A/77/275, para 18(a).

⁴⁰ **Report of the 2021 OEWG, A/75/816, Annex I, para 77.**

⁴¹ **First Annual Progress Report of the OEWG, A/77/275, Regular Institutional Dialogue section, Recommended next steps, para 2.**

exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States, including the possibility of additional legally binding obligations. The diverse perspectives are reflected in the attached Chair's Summary of the discussions and specific language proposals under agenda item "Rules, norms and principles". These perspectives should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240."⁴²

- d) Recognizing that various possible options for regular institutional dialogue have been suggested, it was proposed that as an initial step to building confidence and convergence, States could identify some common elements that could underpin the development of any future mechanism for regular institutional dialogue on security in the use of ICTs, while at the same time continuing further discussions on the proposals identified in sub-paragraphs 49(b) to and 49(c) bis.

Recommended next steps

50. States continue exchanging views at the OEWG on regular institutional dialogue and on proposals by States to facilitate regular institutional dialogue on security in the use of ICTs, with the objective of elaborating common understandings on the most effective format for future regular institutional dialogue with the broad participation of States under the auspices of the United Nations.
51. States agree in principle that a future mechanism for regular institutional dialogue would be based on the following common elements:
- a) It would be a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee of the United Nations General Assembly.
 - b) The aim of the future mechanism would be to continue to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment.
 - c) The future mechanism would take as the foundation of its work the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports.
 - d) It would be an open, inclusive, transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environment.
52. States recognized the importance of the principle of consensus regarding both the establishment of the future mechanism itself as well as the decision-making processes of the mechanism itself.

⁴² Report of the 2021 OEWG, A/75/816, Annex I, para 80.

53. States, at the sixth, seventh and eighth sessions of the OEWG, as well as in a dedicated intersessional meeting, to continue to engage in focused discussions within the framework of the OEWG to further elaborate the PoA with a view towards its possible establishment as a mechanism to advance responsible State behavior in the use of ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs. At these sessions, States will also engage in focused discussions, on the relationship between the PoA and the OEWG, and on the scope, content and structure of a PoA.⁴³ These focused discussions at the sixth, seventh and eighth sessions would build upon the focused discussions undertaken in this regard at the fourth and fifth sessions of the OEWG. To further inform these focused discussions, the UN Secretariat is also requested to brief the OEWG at its sixth session on the report of the Secretary-General submitted to the General Assembly at its seventy-eighth session.
54. States in a position to do so to continue to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant UN processes.

.

⁴³ First Annual Progress Report of the OEWG, A/77/275, Regular Institutional Dialogue section, Recommended next steps, para 2.

**[DRAFT] Elements for the Development and Operationalization of a Global, Intergovernmental
Points of Contact Directory**

1. In accordance with the First Annual Progress Report (APR) of the OEWG contained in A/77/275, in which “States agree to establish, building on work already done at the regional level, a global, intergovernmental, points of contact directory”, this paper sets out elements that can guide the development and operationalization of such a directory.

Purposes and Principles

2. A global, intergovernmental, points of contact directory (POC directory), would serve as a Confidence-Building Measure (CBM) in itself and also provide a framework for the implementation of other CBMs that could help to promote an open, secure, stable, accessible and peaceful information and communications technologies (ICT) environment and reaffirm the observation and implementation by States of the cumulative and evolving framework for responsible State behavior in the use of ICTs.⁴⁴

3. The POC directory is envisioned to be **voluntary**, practical and neutral in nature, developed and implemented in accordance with the principles of sovereignty, sovereign equality, the settlement of disputes by peaceful means, and non-intervention in the internal affairs of other States.

4. The POC directory will **take into account and complement the work of** ~~not duplicate the functions undertaken by~~ Computer Emergency Response Teams (CERTs) and Computer Security Incident Response Teams (CSIRTs) networks.

5. The main purposes of the POC directory are to:

- a) Enhance interaction and cooperation between States, and in doing so, promote international peace and security as well as increase transparency and predictability.
- b) Facilitate coordination and communication between States in the event of an ~~urgent or significant~~ ICT incident **with possible implications for international peace and security, to build confidence between States and** reduce tensions and prevent misunderstandings and

⁴⁴ First Annual Progress Report of the OEWG, A/77/275, Existing and Potential Threats **section**, Recommended Next Steps, paragraph 1

misperceptions that may stem from ICT incidents, ~~thus contributing to the goal of preventing conflict between States.~~

- c) Increase **communication and** information sharing and enable States, including through related capacity-building, to facilitate the prevention, detection, response to and recovery from ~~urgent or significant ICT incidents that impact~~ **with possible implications for** international peace and security.

Modalities

6. **Access and Participation.** Participation in the POC directory, including the submission of information, would be on a voluntary basis. States wishing to participate in the POC directory would be granted access to the directory.

7. **Directory Specifications.** The United Nations Office for Disarmament Affairs (UNODA) would serve as the manager of the directory, with the responsibility of developing and operationalizing the technical aspects of the POC directory in accordance with the following specifications:

- a) Information Schema:
 - i. States may nominate, ~~either, and~~ where possible, both diplomatic and technical POCs to the directory.
 - ii. States may nominate either an authorized national entity/institution or a specific designated representative of an authorized national entity/institution as their POC.
 - iii. States may provide information on the entity/institution, contact information (telephone number and email), name and designation of the respective POC (where applicable), and operational language(s) of the POC.
 - iv. Each directory entry may be submitted in any UN official language; in addition, the submission of an unofficial English translation is encouraged.
- b) Information Protection: The directory would be hosted online on a securely protected website. The directory will not host confidential information transmitted or exchanged between POCs. Communication between POCs, including the transmission of confidential information, would take place through mutually-agreed channels, including secure channels where appropriate.
- c) Information Access: States may request login credentials for the website from UNODA through their Permanent Missions in New York. For general information purposes, a public page providing a general overview of the POC directory's mandate would be made available on the UNODA website.

- d) Information Management: States may provide updates to information contained in the directory on a rolling basis in the event of changes to their submitted information.

8. **Directory Maintenance.** The directory manager is requested to conduct “ping” tests every six months to verify that the information in the directory is up-to-date. As part of the “ping” test, POCs will be contacted by the directory manager and requested to respond with a message indicating receipt of the directory manager’s request within 48 hours. In the absence of a response to the “ping” test, the directory manager would make every effort to contact the relevant authorities of that State to encourage them to update their information.

9. **Roles of the diplomatic and technical POCs.** The diplomatic and technical POCs are envisaged to have differentiated roles. Accordingly, diplomatic POCs would communicate with other diplomatic POCs and technical POCs would communicate with other technical POCs. Coordination between POCs from the same State is encouraged. **States may consider the following suggested functions while defining the roles of their POCs in accordance with their national policies and legislation.**

- a) The diplomatic POC may establish communication with other diplomatic POCs in the event of an ~~urgent or significant~~ ICT incident with **possible** implications for international peace and security, with the aim of preventing misunderstandings and reducing tensions. If necessary, diplomatic POCs may consider the option of bringing the incident to the attention of higher-level officials, within their respective national governmental structures, so that further communication could take place between States, as appropriate.
- b) The technical POC may establish communication with other technical POCs in the event of an ~~urgent or significant~~ ICT incident with **possible** implications for international peace and security, with the aim of providing or requesting information or assistance. Technical POCs may also, on a voluntary basis, exchange best practices, lessons learned, and other relevant information, with other technical POCs on how to facilitate the prevention, detection, response to and recovery from ~~urgent or significant~~ ICT incidents with **possible** implications for international peace and security. Where appropriate, the technical POC may be an authorized national agency working on ICT security such as the national CERT/CSIRT.

10. **Interaction between POCs.** The decision on how to respond to communications received via the POC directory and the content to be communicated in response is to be determined by each State. Any information exchanged is voluntary and in line with the respective domestic circumstances, requirements and legislation of the States involved. Any subsequent cooperation and/or information sharing, including the channel through which relevant communication would take place, would proceed according to mutual agreement. Initial acknowledgement of receipt of a communication does not imply agreement with the information contained therein or prejudice the position of the responding State, nor does it prejudice any communication that may follow. Additionally, notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself.⁴⁵

⁴⁵ Report of the 2021 GGE, A/76/135, para30(d), consensus GA resolution 76/19

- a) POCs may wish to use standardized procedures when interacting with other POCs. As an initial step to facilitate communication, POCs may consider utilizing, on a voluntary basis, the “Procedure for Inquiry” and “Procedure for Responding to an Inquiry” contained in the Appendix; and
- b) POCs may also wish to use standardized templates when interacting with other POCs. Such standardized templates can indicate the types of information required when sending a communication, including technical data and the nature of the request, but be flexible enough to allow for communication, even if some information is unavailable;⁴⁶ States would continue work to develop such standardized templates in accordance with the step-by-step approach for improving the POC directory.

11. **Sharing of Information.** Information exchanged between POCs should remain confidential. POCs involved in the exchange of information should only share that information with third parties by mutual consent. POCs are encouraged to keep a record of all information exchanged.

12. **Interaction with other directories.** The POC directory is a global, intergovernmental platform which could benefit from existing efforts at the regional and sub-regional levels as relevant and appropriate. In this regard, States recognized that not all States are members of regional and sub-regional organizations and that not all such organizations have a POC directory. To avoid duplication of effort, States are encouraged to give due consideration to harnessing synergies vis-a-vis existing regional directories as well as existing CERT/CSIRT directories, where appropriate:

- a) Where States have already nominated diplomatic and technical POCs to other regional directories, States are encouraged to nominate the same diplomatic and technical POCs to the POC directory; and
- b) Where appropriate, managers of existing directories are encouraged to work with UNODA to explore the feasibility of technical synergies and regular information updating between such directories and the POC directory, through appropriate and protected communication channels, where agreed by all contributors to the respective existing directory.

Capacity-Building

13. Guided by the first APR’s recommendation for States to “engage in discussions on initiatives for related capacity-building” with regard to the establishment of the POC directory, States agree to a dedicated action plan comprising the following elements to support first developing countries in building the required technical capacities to effectively participate in the POC directory:

⁴⁶ Report of the 2021 GGE, A/76/135, para 77(b), consensus GA resolution 76/19

Actions by UN Secretariat

- a) The UN Secretariat is requested to develop, in partnership with interested States, a “POC 101” online tutorial on the practical aspects of getting started and participating in a POC directory, in order to encourage States to nominate national POCs and to facilitate States’ use of the POC directory;
- b) The UN Secretariat is requested to seek views from States on the capacities required to participate in the POC directory which could include views on capacity-building experiences drawn from participating in other POC directories. On this basis, the UN Secretariat is requested to prepare an initial background paper no later than January 2024 (i) reflecting views submitted by States; (ii) identifying capacities required for the effective participation of POCs in the POC directory; and (iii) proposing suitable actions for building such capacities, including, *inter alia*, tailored programs for identified POCs;
- c) The UN Secretariat, in partnership with UNITAR and UNIDIR, and with the support of interested States, is requested develop a series of tailored “e- learning” modules addressing the capacities required for the effective participation of POCs in the POC directory, as identified by the UN Secretariat’s background paper;

Actions by OEWG and OEWG Chair

- d) States to engage in further focused discussions, at the forthcoming sessions of the OEWG, on potential follow-up actions drawing upon the information presented in the UN Secretariat’s background paper. In these discussions, States to also take stock of the initiatives compiled on the OEWG website in accordance with paras 13(f) and 13(g), and consider what additional initiatives may be required to build the capacities identified in the UN Secretariat’s background paper;
- e) The OEWG Chair to convene a simulation exercise, in partnership with UNIDIR and interested States, no later than December 2023, utilizing basic scenarios to allow representatives from States to simulate the practical aspects of participating in a POC directory, and to better understand the roles of diplomatic and technical POCs;

Actions by interested States, on a voluntary basis

- f) Leveraging on South-South, South-North, triangular, and regionally focused cooperation, States could convene technical expert meetings of States preparing to participate in the POC directory, in an in-person or hybrid format, at the sub-regional, regional, cross-regional and global levels to discuss and share experiences relating to participation in POC directories. States are invited to communicate, as soon as possible, such initiatives to the UN Secretariat, which is requested to compile and publicize them on the OEWG website on an ongoing basis;

- g) States and/or group of States in a position to do so could support capacity-building with regard to the POC directory, including in collaboration, where appropriate, with regional and sub-regional organizations and other interested stakeholders, including businesses, non-governmental organizations and academia. These States are invited to communicate, as soon as possible, their initiatives to the UN Secretariat, which is requested to compile and publicize them on the OEWG website on an ongoing basis; and States are encouraged to give designated POCs priority consideration for participation in their capacity-building programmes where relevant.

Further Work

14. The initial operationalization of the POC directory should be achieved as quickly as possible. Further improvement of the POC directory would proceed in an incremental and step-by-step manner, with such efforts undertaken in line with the purposes and principles set out above. In this regard, States could simultaneously continue discussions on:

- a) Initiatives to encourage and expand voluntary participation by States in the POC directory;
- b) Communication protocols, including the proper handling of information exchanged and the possible further development of templates and interaction procedures; and
- c) Further ideas to enhance the effective functioning of the POC directory and improve the directory's ability to facilitate communications between States.
- d) Further capacity-building efforts aimed at enabling the full participation of States in the POC directory.

15. The OEWG Chair is requested to convene regular in-person or virtual meetings of POCs, beginning with a meeting of diplomatic POCs, to be followed by a meeting of diplomatic and technical POCs, to share practical information and experiences on the operationalization and utilization of the POC directory.

16. Following the initial operationalization of the directory, States will review the operation of the POC directory and consider possibilities for improvements in its operation, where necessary. In this regard, the OEWG Chair is requested to convene a dedicated meeting of the OEWG in 2024 to allow participating States to review the operation and implementation of the POC directory and consider improvements, taking into account the purposes and principles of the directory.

.

Appendix to Annex A entitled “Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory”

Procedure for Inquiry

POCs may use the following steps to request information from another participant regarding an ICT security incident:

1. Call or email the relevant point of contact and provide your name and affiliation.
2. Provide as much information as possible regarding the nature of the incident.
3. Ask for additional information about the incident and provide your contact information. Indicate time sensitivity as appropriate.
4. Nominate preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.

Procedure for Responding to an Inquiry

POCs may follow these steps to respond to an inquiry about an ICT security incident:

1. Provide an immediate response to the ICT security incident query (if possible), or:
2. Inform the point of contact that you will look into the ICT security incident and follow up with additional information. Provide an estimated timeframe for a response, as appropriate; and
3. Agree on preferred channel of communication and nominate the agency within your country that will become the primary point of contact for this specific incident.

.

Initial List of Voluntary Global Confidence-Building Measures

The following is an initial, non-exhaustive list of voluntary global Confidence-Building Measures. These global CBMs are drawn from the Final Report of the 2021 Open-ended Working Group and the first and second APRs of the OEWG. Additional global CBMs may be added to this list over time, as appropriate, reflecting discussions within the OEWG.

CBM 1. Continue exchanging views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States

- a) States concluded that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs.
[2021 OEWG report, A/75/816, paragraph 43]
- b) States explore mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations.
[2021 OEWG report, A/75/816, paragraph 52]
- c) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.
[2021 OEWG report, paragraph 53]
- d) States continued to emphasize that the OEWG itself served as a CBM.
[First APR of the OEWG, paragraph 16(e)]

CBM 2. Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and good practices, on a voluntary basis

- a) States, on a voluntary basis, continue to inform the Secretary-General of their views and assessments and to include additional information on lessons learned and good practice related to relevant CBMs at the bilateral, regional or multilateral level.
[2021 OEWG report, paragraph 48]

- b) States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate, including through the Cyber Policy Portal of the United Nations Institute for Disarmament Research.

[2021 OEWG report, paragraph 50]

- c) States are encouraged to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 5]

CBM 3. Encourage opportunities for the cooperative development and exercise of CBMs

- a) States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.

[2021 OEWG report, paragraph 49]

- b) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.

[2021 OEWG report, paragraph 53]

- c) States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs.

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 1]

CBM 4. Nominate national Points of Contact to the global POC directory

- a) States, which have not yet done so, consider nominating a national Point of Contact, inter alia, at the technical, policy and diplomatic levels, taking into account differentiated capacities. States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level.

[2021 OEWG report, paragraph 51]

- b) States agree to establish, building on work already done at the regional level, a global, inter-governmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and sub-regional experiences where appropriate.

[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 2]

CBM 5. Operationalize and utilize the global POC directory

- a) Communication checks in the form of “Ping” tests;
- b) Voluntary information-sharing, particularly in the event of ICT security incidents, facilitated through the global POC directory;
- c) Tabletop exercises to simulate practical aspects of participating in a POC directory; and
- d) Regular in-person or virtual meetings of POCs to share practical information and experiences on the operationalization and utilization of the POC directory.

[The elements in CBM 5 are drawn from the “Elements for the Development and Operationalization of a Global, Intergovernmental Points of Contact Directory” contained in Annex A paragraphs 8, 9, 13(e) and 15]

.

Agreed Principles of Capacity-building¹

Taking into consideration and further elaborating upon widely accepted principles, States concluded that capacity-building in relation to State use of ICTs in the context of international security should be guided by the following principles:

Process and Purpose

- Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
- Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- Access to relevant technologies may need to be facilitated.

Partnerships

- Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.
- As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
- The confidentiality of national policies and plans should be protected and respected by all partners.

People

- Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.
- The confidentiality of sensitive information should be ensured.

¹ As agreed in the 2021 OEWG Final Report, A/75/816, paragraph 56

• • • • •