MAJULAH SINGAPURA

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

27 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.

Having reflected carefully on the range of views expressed by delegations on the Final Draft of the second Annual Progress Report (APR) dated 26 July 2023, I have made some further revisions to the text in order to achieve the best possible overall balance that could facilitate a consensus outcome. These revisions are incorporated in the attached document A/AC.292/2023/CRP.1.

I would like to thank all delegations for their active participation and constructive contributions over the week to the drafting of the second APR. I am also encouraged by the fact that all delegations have underlined their commitment to work towards the successful adoption of the second APR.

It is my intention to present the attached CRP document for formal adoption at the meeting of the OEWG on Friday morning, 28 July 2023. This document is the culmination of our collective work over the last twelve months and it brings together a substantive and balanced package of action-oriented outcomes. The document also sets out a concrete road-map for our work over the next year. In summary, it is a meaningful outcome of the OEWG is within our grasp.

I should stress, however, that the document represents a fragile balance of diverse views and priorities and competing positions. I would therefore strongly advise delegations to resist the temptation to make further improvements and amendments to this document as this could easily unravel the delicate overall balance.

The final decision on achieving a consensus outcome lies in the hands of delegations. I therefore appeal to all delegations to demonstrate flexibility and to support the adoption of the attached document at the final meeting of the OEWG on Friday, 28 July 2023.

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 – A/AC.292/2023/CRP.1.

United Nations A/AC.292/2023/CRP.1

General Assembly

28 July 2023

English only

Open-ended working group on security of and in the use of information and communications technologies 2021-2025
Fifth substantive session, New York
24-28 July 2023

Draft Annual Progress Report

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

[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.

ICT environment".[6] These elements consolidate a cumulative and evolving framework[7] for responsible State behaviour in the use of ICTs providing a foundation upon which the current OEWG builds its work.

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 recognized that capacity-building is an important confidence-building measure, is 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 indispensable.

6. 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.

7. 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.

8. The OEWG welcomed the high level of participation of women delegates in its sessions and the prominence of a gender perspective in its discussions. 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.

9. 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 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.

[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.

B. Existing and Potential Threats

10. During the fourth, fifth as well as informal sessions of the OEWG, States continued discussions on existing and potential threats. In this regard, States recalled the scope of the OEWG's work to consider ICT threats in the context of international security and thus undertook discussions on existing and potential ICT threats through this specific lens. 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.

11. States recalled that a number of States are developing ICT capabilities for military purposes.[8] They also recalled that the use of ICTs in future conflicts between States is becoming more likely, and noted 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.[9]

12. 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 national, regional and global effects, as well as malicious ICT activities that target humanitarian organizations. The impact of ICT threats on multiple sectors, including the healthcare, maritime, aviation and energy sectors was particularly noted.

13. 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.[10] States expressed particular concern regarding malicious ICT activities that are aimed at interfering in the internal affairs of States.

14. Furthermore, States noted a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.[11]

15. States also expressed concern regarding the exploitation of ICT product vulnerabilities and the use of harmful hidden functions in particular where these issues impact international peace and security. States also noted the significant threat posed to the integrity of supply chains. States also highlighted the risk posed by malicious software such as ransomware, as well as wiper malware and trojans, and techniques such as phishing and distributed denial-of-service (DDoS) attacks.

16. States further expressed concern at the irresponsible and potentially malicious use, including by States, of available ICT capabilities. States also expressed concern at the use of ICT tools by malicious actors.

17. States noted that new and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity,[12] which could potentially have implications on the use of ICTs in the context of international security. Considering the growth and

[8] Report of the 2021 OEWG, A/75/816, Annex I, para 16.

[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 18.

[11] Report of the 2021 GGE, A/76/135, para 9, consensus GA resolution 76/19.

[12] First Annual Progress Report of the OEWG, A/77/275, para 11; Report of the 2021 GGE, A/76/135, para 11, consensus GA resolution 76/19.

aggregation of data associated with new and emerging technologies, States also noted the increasing relevance of data protection and data security. States noted with concern that it has become a serious challenge to ensure that vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes.

18. States also drew attention to the need for a gender perspective in addressing ICT threats and to the specific risks faced by persons in vulnerable situations. States continued to emphasize that the benefits of digital technology were not enjoyed equally by all and accordingly underlined the need to give due attention 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.

19. States recalled 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.[13]

20. 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.[14] 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 measures[15] and capacity-building initiatives under the cumulative and evolving framework for responsible State behaviour.

Recommended next steps

21. 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.

22. The OEWG to also convene a dedicated intersessional meeting, with the participation of relevant experts invited by the OEWG Chair and with due consideration given to equitable geographical representation, on existing and potential threats to security in the use of ICTs.

C. Rules, Norms and Principles of Responsible State Behaviour

23. 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 rules, norms and principles. 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 recalled that the mandate of the OEWG contained in General Assembly resolution 75/240, inter alia, “to further develop the rules, norms and principles of responsible behaviour of States and

[13] First Annual Progress Report of the OEWG, A/77/275, para 12; Report of the 2021 OEWG, A/75/816, Annex I, para 17.

[14] Report of the 2021 OEWG, A/75/816, Annex I, para 20.

[15] Report of the 2021 OEWG, A/75/816, Annex I, para 22.

the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour;"[16]

b) Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. States stressed that such norms reflect the expectations and standards of the international community regarding the behaviour of States in their use of ICTs and allow the international community to assess the activities of States.[17]

c) States underlined the importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII). States highlighted that ICT activity that intentionally damages CI or CII or otherwise impairs the use and operation of CI or CII to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population and can be escalatory.[18] States thus emphasized the need to continue to strengthen measures to protect all CI and CII from ICT threats and proposed increased exchanges on best practices with regard to CI and CII protection, including the sharing of national policies, and recovery from ICT incidents involving CI and CII. In this regard, States recalled General Assembly resolution 58/199 on the "Creation of a global culture of cybersecurity and the protection of critical information infrastructures" and its accompanying annex.[19] States also proposed to support developing countries and small States, in their identification of national CI and CII, where requested.

d) 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 include 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, as well as cooperative measures such as exchanges of good practices 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.

e) States noted the crucial role that the private sector plays in promoting openness and ensuring the integrity, stability and security 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 strengthen partnership with the private sector to collaboratively enhance the security of and in the use of ICTs. States should also continue to encourage the private sector 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.

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

   i) Surveying, on a voluntary basis, their national implementation of rules, norms and principles of responsible State behaviour, as well as capacity-building needs in that regard. States could share such studies through the report of the Secretary-General on developments in the field of ICTs in the context of international security as well as the National Survey of Implementation as contained in the recommendations of the 2021 OEWG report.[20]

[16] General Assembly resolution 75/240, operative paragraph 1

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

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

[19]Report of the 2021 GGE, A/76/135, para 48, consensus GA resolution 76/19.

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

ii) 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.

g) States stressed the need for further focused discussions on rules, norms and principles of responsible State behaviour in the use of ICTs.

h) 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 Report[21]) further to the recommendation contained in the 2021 OEWG report.[22]

Recommended next steps

24. States continue exchanging views at the OEWG on rules, norms and principles of responsible State behaviour in the use of ICTs, taking into account sub-paragraphs 23 (a)-(h) above, at the sixth, seventh and eighth sessions of the OEWG.

25. At the sixth, seventh and eighth sessions of the OEWG, States to also undertake focused discussions on: (a) strengthening measures to protect CI and CII from ICT threats, including exchanges on best practices to detect, defend against or respond to, and recover from ICT incidents, and to support developing countries and small States in their identification of national CI and CII, where requested; (b) further cooperation and assistance to ensure the integrity of the supply chain and prevent the use of harmful hidden functions.

26. States to elaborate additional guidance, including a checklist, on the implementation of norms, taking into account previous agreements. The OEWG Chair is requested to produce an initial draft of such a checklist for consideration by States.

27. The OEWG Chair is requested to convene a dedicated intersessional meeting to further discuss rules, norms and principles of responsible State behaviour in the use of ICTs taking into account sub-paragraphs 23 (a)-(h) above. 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 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 focused, in-depth 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.[23]

29. 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 paragraphs[24]:

[21] Report of the 2021 OEWG, A/75/816, Annex II.

[22] Report of the 2021 OEWG, A/75/816, Annex I, para 33.

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

[24] First Annual Progress Report of the OEWG, A/77/275, para 15(b)(i) and 15b(ii), and International Law section,

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.";[25]

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."[26]

30. 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 Article 2(3) of the UN Charter which states 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";[27] and Article 33(1) of the UN Charter which states that "the parties to any dispute, the 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".[28]

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".

Recommended Next Steps 2.

[25] Report of the 2021 OEWG, A/75/816, Annex I, para 80.

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

[27] Article 2(3) of the Charter of the United Nations.

[28] Article 33(1) of the Charter 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.[29]

31. States 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 sharing national views could contribute to building common understandings of how international law applies in the use of ICTs and encouraged the continued voluntary sharing of national views on international law which may include national statements and state practice on how international law applies in the use of ICTs by States. Furthermore, relevant studies and opinions of international legal experts may also assist States in developing such common understandings.

c) Acknowledging existing capacity-building initiatives in the area of international law, States further 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 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, and should be undertaken in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.

32. Noting the possibility of future elaboration of additional binding obligations, if appropriate, States discussed the need to consider whether any gaps exist in how existing international law applies in the use of ICTs and further consider the development of additional legally-binding obligations.

Recommended next steps

33. 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 29 (a) and 29 (b) above as well as proposals on the topic of international law contained in the 2021 OEWG report and Chair's summary, where relevant.

34. Building on discussions at the fourth and fifth sessions of the OEWG, States are invited to continue to voluntarily share their national views, which may include national statements and state practice, on how international law applies in the use of ICTs. The UN Secretariat is requested to make these views available on the OEWG website for the reference of all States and for further discussions by the OEWG at its sixth, seventh and eighth sessions.

35. 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 and national contexts, further arrange expert briefings on how international law applies in the use of ICTs.

36. States in a position to do so to continue to support, in a neutral and objective manner, additional efforts, including within the United Nations, to build capacity in the areas of international law, in order for all States to contribute to building common understandings of how international law applies to the use of ICTs, 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.

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

E. Confidence-Building Measures

37. 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,[30] 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 facilitate 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 elements 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:

i. Communication checks in the form of "Ping" tests;

ii. Voluntary information-sharing, including in the event of an urgent or significant ICT incident, facilitated through the global POC directory;

iii. Tabletop exercises to simulate the 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 on a voluntary basis.

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 and objective 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.[31] It was proposed that this issue could be further discussed within the OEWG.

e) States suggested that sharing national views on technical ICT terms and terminologies could enhance transparency and understanding between States.

f) 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.

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

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

g) 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

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

39. Recalling that in the first APR of the OEWG, States agreed to establish a global, inter-governmental, points of contact (POC) directory,[32] 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.

40. States to further discuss and engage in 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 37(b) and 37(c) of this report.

41. States recommend 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 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.

42. States are encouraged, on a voluntary basis, to share national views on technical ICT terms and terminologies to enhance transparency and understanding between States.

F. Capacity-Building

43. 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. 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 report[33] should be further mainstreamed into capacity-building initiatives on security in the use of ICTs. Furthermore, States continued to encourage efforts to promote gender-responsive capacity-building efforts including through the integration of a gender perspective into national ICT and capacity-building policies as well as the development of checklists or questionnaires to identify needs and gaps in this area.

b) States emphasized the value of South-South, triangular and sub-regional and regional cooperation, in complement with North-South cooperation.

c) The OEWG could promote better understanding of the needs of developing countries 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 cumulative and evolving framework for responsible State behaviour in the use of ICTs.

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

[33] Report of the 2021 OEWG, A/75/816, Annex I, para 56.

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

e) 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.

f) 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, as appropriate. 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.

g) 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. It was proposed that States could discuss the capacities that can help States in this regard. 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.

h) 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.[34] In this regard, States discussed a proposal to encourage further technical exchange on ICT threats in order to enhance the capacities of States to identify, detect, defend against and facilitate informed responses to malicious ICT activities, taking into account and complementing existing mechanisms, such as CERT-CERT channels.

i) 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 including for the purposes of training and research. 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

44. States continue exchanging views at the OEWG on capacity-building related to security in the use of ICTs, including on sub-paragraphs 43(a) to 43(i) 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.

[34] Report of the 2021 OEWG, A/75/816, Annex I, para 20.

45. **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.**

46. **The UN Secretariat is 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 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.**

47. **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 as appropriate.**

48. **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.**

49. **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 at the sixth session of the OEWG. The UN Secretariat is encouraged to consult with relevant entities in updating the course.**

50. **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 perspective into such capacity-building efforts.**

51. **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

52. 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.[35]

b) Further to the recommendation in the 2021 OEWG report[36] and in the first APR of the OEWG[37], States deepened discussions on 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. Other proposals were made for regular institutional dialogue, including a proposal for a future group, commission, committee or conference under the auspices of the United Nations.

53. 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 put forward proposals to 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 52(a) to 52(b).

Recommended next steps

54. 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.

55. States agree in principle that a future mechanism for regular institutional dialogue would be based on the following common elements, and agree to continue discussions on additional 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.

56. 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.

57. Other interested parties, including businesses, non-governmental organizations and academia could contribute to any future regular institutional dialogue, as appropriate.

58. States, at the sixth, seventh and eighth sessions of the OEWG, as well as in two dedicated intersessional meetings, to continue to engage in focused discussions within the framework of the OEWG to further discuss proposals on regular institutional dialogue, including the PoA. At these sessions, States will also engage in focused discussions, on the relationship between the PoA

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

[36] Report of the 2021 OEWG, A/75/816, Annex I, para 77.

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

and the OEWG, and on the scope, content and structure of a PoA.[38] 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.

59. 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.

H. Concluding Observations

60. States noted the increasing engagement and constructive participation of delegations from all regions in the work of the OEWG over the course of the past five substantive sessions. At these sessions, States contributed substantively to the work of the OEWG. States and groups of States also submitted working papers to the OEWG setting out their national and group positions, ideas and initiatives, on the issues under the mandate of the OEWG, as listed in Annex D.

• • • • •

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

Annex A: 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 on the use of ICTs in the context of international peace and security.

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 basis for the implementation of other CBMs that could help to promote an open, secure, stable, accessible and peaceful information and communications technologies (ICT) environment.

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 be complemented by the work of 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 including in the event of an urgent or significant ICT incident, to build confidence between States and reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents.

c) Increase communication and information sharing and enable States, including through related capacity-building, to facilitate the prevention, detection, response to and recovery from, *inter alia*, urgent or significant ICT incidents.

d) The POC directory could facilitate secure and direct communications between States to help prevent and address serious ICT incidents and de-escalate tensions in situations of crisis. Communication between POCs can help reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents, including those affecting critical infrastructure and that have national, regional or global impact. They can also increase information sharing and enable States to more effectively manage and resolve ICT incidents.[39]

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 POC directory.

7. **Directory Specifications.** The United Nations Office for Disarmament Affairs (UNODA) would serve as the manager of the POC directory, with the responsibility of developing and

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

operationalizing the technical aspects of the POC directory in accordance with the following specifications:

a) Information Schema:

i. States may nominate, 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 POC 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 POC 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 including in the event of an urgent or significant ICT incident, 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. Where appropriate, the diplomatic POC may be from an authorized national agency with responsibility for international cooperation.

b) The technical POC may establish communication with other technical POCs including in the event of an urgent or significant ICT incident with the aim of providing or requesting information or assistance. Such communication could, *inter alia*, take the form of a request for information or for specific action 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, *inter alia*, urgent or significant ICT incidents. Where appropriate, the technical POC may be an authorized national agency working on ICT security with responsibility for the prevention, detection, response to and recovery from ICT incidents 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 prejudge 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.[40]

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;[41] 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 be complemented by 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 establishing communication are members of the same regional organization with an operational POC directory, States could establish communication using either the global POC directory or the POC directory of the relevant regional organization. Where States establishing communication are not members of the same regional organization, States could establish communication using the global POC directory.

b) 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

c) Where appropriate, UNODA to explore the feasibility, in consultation with managers of existing directories, of technical synergies and the possibility of 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.

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

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

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 assistance plan, to be developed in line with the principles for capacity-building set out in Annex C, comprising the following voluntary elements to support developing countries in building the required technical capacities to effectively participate in the POC directory:

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 June 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, with the support of interested States and relevant entities, 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 interested States, 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, sub-regional and regional 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; and

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 parties, 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;

c) Further ideas to enhance the effective functioning of the POC directory and improve the directory's ability to facilitate communications between States; and

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 POC directory, States will review the operation of the POC directory and consider possibilities for improvements in its operation, where necessary, including through the exchange of experiences by States in using the POC directory. 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 POC 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.

. . . . .

Annex B: 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. Nominate national Points of Contact to the global POC directory, and operationalize and utilize the global POC directory

a) 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]

b) 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]

c) States are encouraged to operationalize and utilize the global POC directory in the following ways:

i) Communication checks in the form of "Ping" tests;

ii) Voluntary information-sharing, including in the event of an urgent or significant ICT incident, facilitated through the global POC directory;

iii) Tabletop exercises to simulate practical aspects of participating in a 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 POC directory on a voluntary basis.

v) Utilize the POC directory to establish communication between POCs, in accordance with the modalities of the POC directory.

CBM 2. 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 3. Share information, on a voluntary basis, such as national ICT concept papers, national strategies, policies and programmes, legislation and best 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 4. 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]

. . . . .

Annex C: Agreed Principles of Capacity-building[1]

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

Annex D: List of Working Papers setting out National and Group Positions, Ideas and Initiatives

(Listed in order of date of submission, with most recent submission first, as of 27 July 2023)

Rev1 Working Paper on Global Cyber Security Cooperation Portal Table submitted by India [TRACKED-CHANGE VERSION]
India

Rev1 Working Paper on Global Cyber Security Cooperation Portal submitted by India [CLEAN VERSION]
India

Applicability of international law, in particular the United Nations Charter, in the use of ICTs: areas of convergence submitted by a group of States
Multiple States (Australia, Colombia, El Salvador, Estonia, Uruguay)

Updated draft working paper on the establishment of a threat repository within the United Nations submitted by Kenya
Kenya

Position Paper on the Application of International Law in Cyberspace by Costa Rica
Costa Rica

Position Paper on the Application of International Law in Cyberspace by Ireland
Ireland

Updated Concept of the Convention of the United Nations Ensuring International Information Security submitted by Russian Federation (Cosponsors: Belarus, DPRK, Nicaragua, Syria, Venezuela)
Russian Federation

Working Paper on applicability of international law, in particular the UN Charter, in the use of ICTs: areas of convergence submitted by a Group of States
Multiple States (Australia, Colombia, El Salvador, Estonia)

Submission to the Secretary General’s report mandated by UN General Assembly Resolution A/RES/77/37 by France
France

Working paper on provisional operationalization of the PoC directory submitted by Iran (Islamic Republic of)
Iran (Islamic Republic of)

Draft working paper on the establishment of a threat repository within the UN submitted by Kenya
Kenya

Utilizing the UN Cyber Point of Contact Directory: Communications, Information-Sharing and Exercising submitted by Germany on behalf of a group of States
Multiple States (Argentina, Australia, Brazil, Canada, Chile, Czech Republic, Fiji, Germany, Israel, Kenya, Republic of Korea, Mexico, The Netherlands, Singapore, Uruguay)

Views on the future regular institutional dialogue on ICTs in the context of international security submitted by Brazil
Brazil

Confidence Building Measure No.1 on the establishment of a global intergovernmental PoC Directory proposal of the Russian Federation (Cosponsors: Belarus, Nicaragua)
Russian Federation

Concept paper on establishing under the auspices of the UN a regular institutional dialogue for all UN Member States on security of and in the use of ICTs (Cosponsors: Belarus, Nicaragua)
Russian Federation

Working Paper on Global Cyber Security Cooperation Portal submitted by India
India

Working paper on the scope, structure and content of the proposed Programme of Action to advance responsible state behaviour in the use of ICTs in the context of international security submitted by Egypt
Egypt

Position on the Application of International Law in Cyberspace submitted by Pakistan
Pakistan

Concept paper on Global Points of Contact Directory submitted by Venezuela
Venezuela (Bolivarian Republic of)

Position on the establishment of a Global Points of contact Directory submitted by Jordan
Jordan

View on the establishment of a Global Points of Contact Directory submitted by Spain
Spain

Views on the Points of Contact Directory submitted by Mexico
Mexico

Views on a global points of contact directory pursuant to the first annual progress report contained in A/77/275 submitted by Estonia
Estonia

View on the establishment of a global points of contact directory submitted by Slovakia
Slovakia

Preliminary views on a global points of contact directory submitted by Hungary
Hungary

Inputs on Global Points of Contact Directory pursuant to A/77/275 submitted by Morocco
Morocco

View on the Global Points of Contact Directory submitted by Republic of Korea
Republic of Korea

National views on global points of contact directory by Armenia
Armenia

Inputs on global points of contact directory by Mexico
Mexico

Contribution to the background paper on a global points of contact directory submitted by Senegal
Senegal

Views on the Points of Contact Directory at the United Nations submitted by Singapore
Singapore

Views on the Establishment of a Global Directory of Points of Contact submitted by Pakistan
Pakistan

View on global points of contact directory pursuant to A/77/275 submitted by Czech Republic
Czech Republic

Position on the global directory of points of contact submitted by Egypt
Egypt

View on the Global Points of Contact Network and Directory on ICT Security submitted by Italy
Italy

Establishing a Directory of Points of Contact submitted by India
India

National opinion on the Global Directory of National Points of Contact submitted by El Salvador
El Salvador

Preliminary position and recommendations on global points of contact directory submitted by Romania
Romania

Views on global points of contact directory pursuant to A/77/275 submitted by the United Kingdom
United Kingdom

Views on the establishment of a global cyber points of contact directory submitted by France
France

Implementing Cyber Confidence Measures Globally- Towards the UN point of Contact Directory submitted by Germany on behalf of a group of States
Multiple States (Australia, Brazil, Canada, Chile, Fiji, Germany, Israel, the Republic of Korea, Mexico, the Netherlands, Singapore and Uruguay)

Inputs for the background paper on a Points of Contact Directory submitted by South Africa
South Africa

Views on Global Points of Contact Directory submitted by Malaysia
Malaysia

Inputs on Global Directory of Points of Contact submitted by Colombia
Colombia

Inputs to Background Paper on Global Points of Contact Directory submitted by Germany
Germany

Non-Paper on Establishing a Global and Inter-Governmental Points of Contact Directory submitted by China
China

Concept paper on functional equivalence as an essential element for effective functioning of PoCs submitted by Iran (Islamic Republic of)
Iran (Islamic Republic of)

Concept paper on establishing a directory of Points of Contact submitted by the Russian Federation
Russian Federation

Updated Concept Paper on a Practical Approach to International Law submitted by Canada and Switzerland
Multiple States (Canada and Switzerland)

Concept Note submitted by Germany on behalf of a group of States on CBMs
Germany

Concept paper of the Russian Federation on establishing a directory of Points of Contact
Russian Federation

Proposal on capacity building by Colombia
Colombia

Joint Proposal on CBMs text by Australia, Brazil, Canada, Germany, Israel, Mexico, Netherlands, Republic of Korea, Singapore
Multiple States (Australia, Brazil, Canada, Germany, Israel, Mexico, the Netherlands, the Republic of Korea and Singapore)

Joint proposal for APR Rev.1 Threats Chapter by Australia, Botswana, Chile, Costa Rica, Denmark, Indonesia, Malaysia, NL, UK
Multiple States (Australia, Botswana, Chile, Costa Rica, Denmark, Indonesia, Malaysia, the Netherlands, and the United Kingdom)

Global Cyber Security Cooperation Portal: Concept Note
India

Joint amendments to the annual progress report- Bolivia, Cuba, Nicaragua, Venezuela
Multiple States (Bolivia, Cuba, Nicaragua, Venezuela)

Joint Position on draft annual progress report
Multiple States (Republic of Belarus, the Republic of Cuba, the Islamic Republic of Iran, Republic of Nicaragua, the Russian Federation, the Syrian Arab Republic and the Bolivarian Republic of Venezuela)

Introduction and Existing and Potential Threats Comments and Textual Proposals by Netherlands
Netherlands

APR Rev.1 - Text Proposals (Introduction, Threats, Norms) by Australia
Australia

Joint Working Paper on the Establishment of a UN Cyber Points of Contact Network submitted by a group of States
Multiple States (Australia, Brazil, Canada, Germany, Israel, the Republic of Korea, Mexico, the Netherlands and Singapore)

Position Paper on the Application of lnternational Law in Cyberspace submitted by Sweden
Sweden

The Cybersecurity Capacity Maturity Model: Driving needs assessments and national strategies submitted by multiple States
Multiple States (Australia, Botswana, Belize, Chile, Colombia, Dominican Republic, Ecuador, Fiji, Germany, Georgia, Iceland, Japan, Malawi, Mauritius, Netherlands, Norway, Paraguay, Peru, Rwanda, Switzerland, Tanzania, Uganda, United Kingdom, Vanuatu)

Advancing a Global Cyber Programme of Action: Options and Priorities submitted by Canada
Canada

A Practical Approach to International Law in the 2021-2025 OEWG submitted by Canada and Switzerland
Multiple States (Canada and Switzerland)

Working-Paper to advance the ongoing discussions within the UN OEWG on CBMs in Cyberspace
Multiple States

UN Table-Top Exercise Programme for National Cyber Points of Contact submitted by Singapore
Singapore

UN-Singapore Cyber Fellowship Concept Note submitted by Singapore
Singapore

International Law applicable in cyberspace submitted by Canada
Canada

Russian amendments to draft OEWG report of 22 June 2022
Russian Federation

Canada's Proposal for the Work of the 2021-25 United Nations OEWG on Developments in Field ICT security
Canada

China's Positions on International Rules-making in Cyberspace
China

Global Initiative on Data Security submitted by China
China

Submission to the First Substantive Session by Iran (Islamic Republic of)
Iran (Islamic Republic of)

International Law Applies to Operations in Cyberspace submitted by France
France

China's Views on the Application of the Principle of Sovereignty in Cyberspace
China

Estonian positions – 2021-25 UN OEWG -Developments in the Field of Information and Telecommunications in the Context of Intl Sec
Estonia

Working paper for a Programme of Action (PoA) to advance responsible State behavior in the use of ICTs submitted by a group of States
Multiple States (Argentina, Australia, Austria, Belgium, Bulgaria, Canada, Chile, Colombia, Croatia, Republic of Cyprus, Czech Republic, Denmark, Ecuador, Egypt, Estonia, France, Finland, Gabon, Georgia, Germany, Greece, Guatemala, Hungary, Iceland, Ireland, Italy, Japan, Latvia, Lebanon, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Morocco, Netherlands, Norway, Poland, Portugal, Republic of Korea, Republic of Moldova, Republic of North Macedonia, Romania, Salvador, Singapore, Slovakia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Arab Emirates, United Kingdom)

Italian Position Paper on International Law and Cyberspace
Italy

Concept of work of the UN Open-ended Working Group on security of and in the use of information and communications technologies submitted by Russian Federation
Russian Federation

On the Application of International Law in Cyberspace submitted by Germany
Germany

Contribution of the Russian Federation on rules, norms and principles of responsible behaviour of States in information space
Russian Federation

• • • • •