United Nations A/79/214*

General Assembly

Distr.: General
22 July 2024

Original: English

Seventy-ninth session
Item 93 of the provisional agenda**
Developments in the field of information and telecommunications in the context of international security

Developments in the field of information and telecommunications in the context of international security

Note by the Secretary-General

The Secretary-General has the honour to transmit to the members of the General Assembly the third annual progress report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025.

* Reissued for technical reasons on 2 October 2024.
** A/79/150.

24-13414* (E) 021024

Report of the open-ended working group on security of and in the use of information and communications technologies 2021–2025

I. Introduction

1. By its resolution 75/240, the General Assembly decided to convene, starting from 2021, with a view to ensuring the uninterrupted and continuous nature of the democratic, inclusive and transparent negotiation process on security in the use of information and communications technologies, under the auspices of the United Nations, a new open-ended working group on security of and in the use of information and communications technologies 2021–2025, 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 Assembly at its eightieth session.

2. The first annual progress report of the working group, on its organizational session and its first, second and third substantive sessions, was issued as document A/77/275. The second annual progress report of the working group, on its fourth and fifth substantive sessions, was issued as document A/78/265.

II. Organizational matters

A. Opening and duration of the sixth, seventh and eighth substantive sessions

3. The working group held its sixth substantive session from 11 to 15 December 2023, its seventh substantive session from 4 to 8 March 2024 and its eighth substantive session from 8 to 12 July 2024, at United Nations Headquarters.

4. The Office for Disarmament Affairs and the United Nations Institute for Disarmament Research provided substantive support for the working group. The Department for General Assembly and Conference Management provided secretariat services.

B. Attendance

5. Participants in the sixth, seventh and eighth substantive sessions are listed in documents A/AC.292/2023/INF/7, A/AC.292/2024/INF/2 and A/AC.292/2024/INF/4, respectively.

C. Officers

6. At its sixth, seventh and eighth substantive sessions, the working group was chaired by Mr. Burhan Gafoor (Singapore).

D. Organization of work

7. At the 1st meeting of the sixth substantive session, on 11 December 2023, the working group agreed on its organization of work as contained in document A/AC.292/2023/4. It also approved the participation in the working group of the non-governmental entities listed in document A/AC.292/2023/INF/6.

8. At the 1st meeting of the seventh substantive session, on 4 March 2024, the working group agreed on its organization of work as contained in document A/AC.292/2024/1. It also approved the participation in the working group of the non-governmental entities listed in document A/AC.292/2024/INF/1.

9. At the 1st meeting of the eighth substantive session, on 8 July 2024, the working group agreed on its organization of work as contained in document A/AC.292/2024/4. It also approved the participation in the working group of the non-governmental entities listed in document A/AC.292/2024/INF/3.

E. Documentation

10. A full list of all official documents, working papers, technical papers and other documents before the working group can be found at the dedicated website (https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021).

F. Proceedings of the working group

11. At its sixth substantive session, the working group considered agenda items 3, 5 and 6 at its 10 plenary meetings.

12. At its seventh substantive session, the working group considered agenda items 3, 5 and 6 at its 10 plenary meetings.

13. At its eighth substantive session, the working group considered agenda items 3, 5, 6 and 7 at its 9 plenary meetings.

14. From 13 to 17 May and on 1 July 2024, the Chair convened dedicated intersessional meetings to hear views on the topics under consideration by the working group, as contained in the mandate of the working group set out in General Assembly resolution 75/240 and the agenda of the working group (A/AC.292/2021/1), pursuant to Assembly decisions 77/512 and 78/541, featuring expert briefings on selected topics by experts drawn from a list of nominated experts submitted by delegations, with the participation of interested stakeholders.

15. On 9 May 2024, the Chair convened the first meeting of points of contact of the global points of contact directory, pursuant to document A/78/265 and General Assembly decision 78/541. The first meeting of points of contact also marked the formal launch of the global points of contact directory.

16. On 10 May 2024, the Chair convened the inaugural high-level global round table on information and communications technology security capacity-building, pursuant to General Assembly decision 78/541, to provide a platform for capacity-building

practitioners, State representatives and interested stakeholders to exchange ideas, share best practices and build partnerships with the aim of enhancing synergies and advancing the international community's work on capacity-building in concrete ways.

17. On 28 September 2023 and 31 January, 27 March and 10 June 2024, the Chair convened virtual informal meetings to provide delegations with briefings on elements under consideration by the working group.

18. On 13 December 2023 and 6 March and 10 July 2024, in accordance with the agreed modalities for the participation of stakeholders, dedicated stakeholder sessions were held during the 6th meeting of the sixth substantive session, the 6th meeting of the seventh substantive session and the 5th meeting of the eighth substantive session.

19. On 6 December 2023 and 28 February and 3 July 2024, the Chair convened informal consultative discussions with interested stakeholders, including businesses, non-governmental entities and academia, to hear views on the topics under consideration by the open-ended working group, as contained in the mandate of the working group set out in General Assembly resolution 75/240 and the agenda of the working group (A/AC.292/2021/1), and concrete ideas that the working group could consider going forward.

III. Adoption of the report

20. At its eighth substantive session, on 12 July 2024, the working group considered agenda item 7, entitled "Adoption of annual progress reports", and adopted the draft report of the open-ended working group (A/AC.292/2024/L.1). It also decided to include in its report the outcome of the discussions of the working group on agenda item 5, as contained in document A/AC.292/2024/CRP.1 (see annex).

21. A compendium of statements in explanation of position will be issued as document A/AC.292/2024/INF/5.

Annex*

Progress report on the discussions of the working group on agenda item 5

A. Overview

1. The sixth, seventh and eighth formal sessions as well as the dedicated 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 continues to be 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 and second annual progress reports (APRs) 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 framework[7] for responsible State behaviour in the use of ICTs providing a foundation upon which the current OEWG and the future permanent mechanism 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.

---

* Issued without formal editing.

[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 and A/78/265 respectively.

[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.

5. As discussions at the OEWG continue to deepen, States increasingly recognized the inter-connections between all the issues addressed under the OEWG. In this regard, States emphasized that the work of the OEWG and subsequently the future permanent mechanism would be integrated, policy-oriented and cross-cutting in nature.

6. 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.

7. The OEWG further emphasized that capacity-building is foundational to developing the resources, skills, policies and institutions necessary to increase the resilience and ICT security of States and to accelerate the digital transformation of States and the implementation of the 2030 Agenda for Sustainable Development. States further recognized that capacity-building supports the framework for responsible State behaviour in the use of ICTs and contributes to the building of an open, safe, secure, stable, accessible, peaceful and interoperable ICT environment. Given the rapid pace of developments in the digital landscape, needs-based capacity-building efforts need to be accelerated and constitutes one of the key functions of the future permanent mechanism, in order to bridge the digital divides and ensure that all States can safely and securely seize the benefits of digital technologies. In this regard, States reaffirmed the ICT security capacity-building principles as adopted in the 2021 OEWG report and contained in the Second APR.

8. 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.[8]

9. 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.[9]

10. 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.

11. This third 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 and second APRs, endorsed by consensus in General Assembly Decisions 77/512 and 78/541 respectively. 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 third APR 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 and second APRs. This third APR will be submitted to the General Assembly pursuant to the OEWG's mandate contained in resolution 75/240.

[8] First APR, para 4 and second APR, para 6.
[9] First APR, para 5 and second APR, para 7.

B. Existing and Potential Threats

12. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings 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 and second APRs, 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 a geopolitical environment that remains challenging.

13. States recalled that a number of States are developing ICT capabilities for military purposes. 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.[10]

14. States expressed concern regarding the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII) such as the healthcare, maritime, aviation, financial and energy sectors. Such CI and CII can potentially provide essential services across borders and jurisdictions and ICT attacks affecting them may have cascading national, regional and global effects.[11] States highlighted that it is each State's prerogative to determine which infrastructures it designates as critical.[12]

15. States underscored that malicious ICT activities affecting CI and CII that undermine trust and confidence between States as well as 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.[13]

16. States highlighted the need to secure undersea cables and orbit communication networks from malicious activity which could cause significant damage or disruption to telecommunications and potentially affect the technical infrastructure essential to the availability and integrity of the internet in large areas of the globe.

17. States also expressed concern regarding malicious ICT activity targeting international organizations and humanitarian organizations, which may disrupt the ability of these organizations to fulfil their respective mandates in a safe, secure and independent manner and undermine trust in their work.

18. 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.[14] States expressed particular concern regarding malicious ICT activities that are aimed at interfering in the internal affairs of States.[15]

19. States 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 ICT threat posed to the integrity of supply chains.[16]

20. States highlighted concern over the use of malicious software such as ransomware, wiper malware and trojans, and techniques such as phishing, man-in-the-middle and distributed denial-of-service (DDoS) attacks. Particular concern was expressed over ransomware attacks by an increasing number of malicious actors and in different regions of the world facilitated in part by the availability of hiring ransomware attacks

[10] Report of the 2021 OEWG, A/75/816, Annex I, para 16; Second APR, para 11.
[11] Second APR, para 12.
[12] 2021 OEWG report, A/75/816, para 18.
[13] Report of the 2021 OEWG, A/75/816, Annex I, para 18; Second APR, para 13.
[14] Second APR, para 14.
[15] Second APR, para 13.
[16] Second APR, para 15.

as a service. States further highlighted with concern that the increasing frequency, scale and severity of ransomware attacks causes harm, disrupts essential services to the public and may have an impact on international peace and security. States noted the need to comprehensively address all elements of the ransomware threat, including by pursuing ransomware actors, targeting the malicious software they use and its dissemination, and countering the illicit finance that supports their activities. States also highlighted with concern rising cryptocurrency theft and financing of malicious ICT activity using cryptocurrency which could potentially impact international security.

21. States noted the growing market for commercially-available ICT intrusion capabilities as well as hardware and software vulnerabilities, including on the dark web. States expressed concern that their ready availability to State and non-State actors was increasing the opportunity for their illegitimate and malicious use and making it potentially more difficult to mitigate and defend against the threats they pose, while emphasizing that such capabilities could be used in a manner consistent with international law. States further expressed concern that the dissemination of ICT intrusion capabilities by State and non-State actors could contribute to unintentional escalation and threaten international peace and security.

22. States noted that technologies are neutral in and of themselves, and new and emerging technologies such as Artificial Intelligence (AI) and Quantum Computing are expanding development opportunities. At the same time, their ever-evolving properties and characteristics could potentially have implications for the use of ICTs in the context of international security by creating new vectors and vulnerabilities in the ICT space. Such technologies could also increase the speed and enhance the targeting potential of malicious ICT activity.[17] Risks could also be exacerbated through the intersection of new technologies.

23. States expressed particular concern regarding the safety and security of AI systems as well as the data used for training machine learning and AI models as used in the context of ICT security. AI can be used to enhance ICT security, increase resilience, improve response time to ICT incidents and strengthen networks. States also highlighted that AI is likely to increase the volume and heighten the impact of ICT attacks through the evolution and enhancement of existing tactics, techniques and procedures. Such operations may increase the risk of cascading effects that may cause unintended harm, including to individuals and critical infrastructure. In this regard, States underscored that there was a need to better understand the risks associated with new and emerging technologies, including AI, in terms of how they related to ICT security, and to implement and strengthen security throughout the life cycle of these technologies, so as to fully seize the opportunities presented by such technologies. States also stressed that it is in the interest of all States to promote the use of new and emerging technologies for peaceful purposes.

24. Considering the growth and aggregation of data associated with new and emerging technologies, States also noted the increasing relevance of data protection and data security.[18]

25. 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.

26. States continued to draw 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 2030 Agenda for Sustainable Development, while respecting the national needs and priorities of States.[19]

27. 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.[20]

[17] 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.
[18] Second APR, para 17.
[19] Second APR, para 18.
[20] Second APR, para 19.

28. States continued to express concern that a lack of awareness of existing and potential threats and a lack of adequate capacities to detect, defend against and/or respond to malicious ICT activities may make them more vulnerable.[21] 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[22] and capacity-building initiatives under the cumulative and evolving framework for responsible State behaviour.[23]

Recommended next steps

29. **States to continue exchanging views at the OEWG on existing and potential threats to security in the use of ICTs in the context of international security, taking into account paragraphs 12 to 28 above, and to continue focused discussions on 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.**

30. **States are invited to submit working papers on possible ways to raise awareness and deepen understanding of existing and potential threats, and to identify possible cooperative measures and capacity-building initiatives to enable States to detect, defend against or respond to these threats. The UN Secretariat is requested to make these papers available on the OEWG website for the reference of all States and for further consideration by the OEWG at its forthcoming substantive sessions.**

C. Rules, Norms and Principles of Responsible State Behaviour

31. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings 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) 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.[24]

b) As set out in norm (c)[25], States continued to recognize that States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs, and would welcome further discussions in order to continue building common understandings through exchanges of national and regional experiences in this regard.

c) As set out in norms (f)[26] and (g)[27], 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

[21] Report of the 2021 OEWG, A/75/816, Annex I, para 20.
[22] Report of the 2021 OEWG, A/75/816, Annex I, para 22.
[23] Second APR, para 20.
[24] Report of the 2021 OEWG, A/75/816, Annex I, paras 64 and 65, Second APR, para23b).
[25] Norm (c): States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
[26] Norm (f); A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.
[27] Norm (g): States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

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.[28]

d) In view of the above, States 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. States highlighted that specific protective measures for CI and CII may include the voluntary designation of CI and CII,[29] comprehensive risk assessments, ICT awareness and training, as well as the development of relevant national regulatory requirements and guidelines. States highlighted that it is each State's prerogative to determine which infrastructures it designates as critical.[30] States emphasized the need to cultivate a culture of continuous improvement in order to adapt to evolving ICT threats to CI and CII. States further recognized that capacity-building can assist CI and CII operators in this regard.

e) As set out in norm (i)[31], 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.[32]

f) States also emphasized that security-by-design should be embedded in the development and manufacture of ICT products and that ensuring the integration of product security over speed-to-market should be encouraged.

g) States continued to note the crucial role that the private sector plays in promoting openness and ensuring the integrity, stability and security of the supply chain, and in preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. States further stressed that public-private partnerships were critical for the development and promotion of best practices in securing the integrity of the supply chain, and encouraged the sharing of information as well as best practices between States as well as with the involvement of relevant stakeholders. 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.[33]

h) States affirmed the importance of supporting and furthering efforts to implement norms by which States have committed to be guided at the global, regional and national levels.[34]

i) States took note of the Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs as contained in Annex A of this report. States suggested that the checklist may be viewed as a living document which could continue to be discussed and updated at the forthcoming OEWG sessions. In this regard, technical gaps between States, diverse national systems and regional specificities should be taken into account in the use of this checklist. States also recognized the guidance on implementation provided by the 2021 GGE report,[35] and further noted that

[28] Report of the 2021 GGE, A/76/135, para 42, consensus GA resolution 76/19; Second APR para 23c).
[29] States highlighted that it is each State's prerogative to determine which infrastructures it designates as critical (2021 OEWG report, A/75/816, para 18).
[30] 2021 OEWG report, A/75/816, para 18.
[31] Norm (i): States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.
[32] Second APR, para 23d).
[33] Second APR, para 23e).
[34] Report of the 2021 OEWG, A/75/816, para 27.
[35] A/76/135.

there were other available resources which could assist States in the implementation of existing rules, norms and principles. At the same time, States recognized that there is no one-size-fits-all solution to implementation.

j) States recalled 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 the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour;"[36]

k) Given the unique attributes of ICTs, States reaffirmed that additional norms could continue to be developed over time. States also concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.[37] In this regard, several proposals were put forward for possible new norms which are still being discussed by States.

l) In this regard, 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) further to the recommendation contained in the 2021 OEWG report. States also proposed that the current OEWG could continue its discussion on the possible development of additional norms.

Recommended next steps

32. **States to 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 31a) to 31l) above, at the forthcoming substantive sessions of the OEWG.**

33. **States to continue efforts to implement norms and to discuss and update the Voluntary Checklist of Practical Actions (Annex A) which is a living document, with a view towards reaching a consensus recommendation on the Voluntary Checklist by July 2025.**

34. **States to continue discussions on possible additional norms of responsible State behaviour in the use of ICTs at the forthcoming sessions of the OEWG building on discussions at previous OEWG sessions.**

D. International Law

35. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings 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 29 (a) and 29 (b) of the second APR, as well as proposals contained in the 2021 OEWG report and Chair's summary, where relevant.[38]

36. 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[39]:

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;

[36] General Assembly resolution 75/240, operative paragraph 1, Second APR, para 23a).
[37] 2021 OEWG report, A/75/816, para 29.
[38] Second APR, para 28.
[39] Second APR, para 29a) and 29b).

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.";[40]

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."[41]

37. 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.[42] Additionally, States reaffirmed that State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory. Existing obligations under international law are applicable to States' ICT-related activity. States exercise jurisdiction over the ICT infrastructure within their territory by, *inter alia*, setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats. [43]

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";[44] 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". [45]

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. [46]

[40] Report of the 2021 OEWG, A/75/816, Annex I, para 80.
[41] Report of the 2021 GGE, A/76/135, para 71(f), consensus GA resolution 76/19.
[42] Second APR, para 30a).
[43] Report of the 2021 GGE, A/76/135, para 71(b), consensus GA resolution 76/19.
[44] Article 2(3) of the Charter of the United Nations.
[45] Article 33(1) of the Charter of the United Nations.
[46] Report of the 2021 GGE, A/76/135, para 71(c), consensus GA resolution 76/19.

e) Additionally highlighted that conduct using ICTs that does not amount to a violation of the prohibition on the threat or use of force may, depending on the circumstances, be contrary to other principles of international law, such as State sovereignty or the prohibition on intervention in the internal or external affairs of States.

38. States also made additional concrete, action-oriented proposals on international law as follows:

a) States noted discussions on international law at the sixth, seventh and eighth sessions as well as at the intersessional meetings of the OEWG, and further welcomed the active participation of an increasing number of States at these discussions. States, noting that these discussions on international law have significantly deepened during the course of the OEWG, proposed that these discussions could continue to benefit from briefings from experts, such as from the International Law Commission or academia as appropriate, with due consideration given to equitable geographical representation and national contexts.

b) States, reaffirming that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment,[47] proposed that how international law applies in the use of ICTs as it relates to the specificities of the ICT environment could be discussed in further depth at the OEWG.

c) States further noted that sharing national views and positions on international law could contribute to building common understandings of how international law applies in the use of ICTs and strongly encouraged the continued voluntary sharing of such national views and positions by States which may include national statements and state practice on how international law applies in the use of ICTs. Furthermore, relevant studies and opinions of international legal experts may also assist States in developing such common understandings.[48]

d) Acknowledging existing capacity-building initiatives in the area of international law, States continued to underscore 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, conferences and exchanging 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 such capacity-building efforts should be made in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.[49]

e) 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.[50]

Recommended next steps

39. **States to 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 paragraphs 36 to 38 above as well as proposals on the topic of international law contained in the 2021 OEWG report and Chair's summary, where relevant.**

40. **Building on discussions at the sixth, seventh and eighth sessions of the OEWG, States are invited to continue to voluntarily share their national views and positions, 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 forthcoming substantive sessions.**

[47] 2021 OEWG report, para 34.
[48] Second APR, para 31b).
[49] Second APR, para 31c).
[50] Second APR, para 32.

41. **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 made in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.**

E. Confidence-Building Measures

42. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings 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) States continued to emphasize that CBMs are essential for enhancing mutual trust and predictability between States and in reducing tensions, misunderstanding and miscalculations. States also underscored the interlinkages that exist between CBMs and other aspects of the framework for responsible State behaviour in the use of ICTs.

b) States welcomed the launch of the Global Points of Contact (POC) Directory on 9 May 2024 and the first meeting of the Points of Contact held the same day. States also expressed appreciation for the first "ping" test of the Global POC Directory initiated by the Secretariat on 10 June 2024. States recalled the purposes and principles of the Global POC Directory as set out in Annex A of the Second APR[51], noting also that the Global POC Directory could support the taking forward of CBMs in general. In this regard, States emphasized the need to continue work to further develop and operationalize the Global POC Directory at the forthcoming OEWG sessions and subsequently under the auspices of the future permanent mechanism.

c) States highlighted that a step-by-step approach could be taken to develop the Global POC Directory based on experience from its operationalization. As a priority, all UN Member States who have not already done so were encouraged to nominate national POCs as soon as possible. Measures such as raising awareness of the importance of POCs for ICT security in the national political context and targeted capacity-building could contribute to ensuring that as many States as possible nominate POCs to the Global POC Directory. The OEWG encouraged States in a position to do so to provide support to POCs from developing countries to attend in-person OEWG POC meetings.

d) States also proposed that in order to optimize communication between States through the Global POC Directory, standardized templates could be developed to increase clarity and timeliness of communications between States. At the same time, States also noted that such templates should be flexible and voluntary so as not to unnecessarily encumber the use of the Global POC Directory particularly in urgent situations.

e) In addition to the already recommended CBMs contained in previous UN reports including Annex B of the second APR entitled "Initial List of Voluntary Global Confidence-Building Measures", States made proposals for additional global CBMs as contained in Annex B of this report.

f) States proposed that sharing national views on technical ICT terms and terminologies could enhance transparency and understanding between States. States could continue to share their views on such technical terms and terminologies.

[51] A/78/265.

g) It was proposed that aspects of confidence-building could continue to include engagement with other interested parties and stakeholders, including businesses, non-governmental organizations and academia, where appropriate.[52]

h) 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.[53] Furthermore, States also highlighted that OEWG could be a platform for the innovative exercising of CBMs.

Recommended next steps

43. **States to continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs, taking into account sub-paragraphs 42a) to 42h) above.**

44. **States to continue the further development and operationalization of the Global POC Directory at the forthcoming sessions of the OEWG and subsequently under the auspices of the future permanent mechanism. As a priority, all UN Member States who have not already done so are encouraged to nominate national POCs to the Global POC Directory as soon as possible. Additionally, States in a position to do so are encouraged to provide support to POCs from developing countries to attend in-person OEWG POC meetings.**

45. **States are encouraged to actively participate in the six-monthly "ping" tests for POCs as envisaged in Annex A of the Second APR.**[54]

46. **Further to Annex A of the Second APR,**[55] **the OEWG Chair to convene a simulation exercise in hybrid format, in partnership with interested States and UN entities and with the support of the UN Secretariat.**

47. **States to optimize communication through the Global POC Directory including through the development of standardized templates for use by States at their discretion. In this regard, the UN Secretariat, drawing from the inputs of States, as well as the experience of regional organizations where appropriate, is requested to develop an example of such a template by April 2025, with a view towards reaching a consensus recommendation.**

48. **Recalling the list of global CBMs contained in Annex B of the second APR,**[56] **States recommend that the CBMs as contained in Annex B of this report as additional voluntary global CBMs, acknowledging that States may implement CBMs according to their different national priorities and capacities. 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.**

49. **States are encouraged, on a voluntary basis, to continue to share national views on technical ICT terms and terminologies to enhance transparency and understanding between States.**[57]

F. Capacity-Building

50. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings of the OEWG, States continued discussions on ICT capacity-building in the context of international security. At these

[52] Second APR, para 37f).
[53] Second APR, para 37g).
[54] Para 8.
[55] Para 13e).
[56] A/78/265.
[57] Second APR, para 42.

sessions, States shared national experiences on international cooperation and capacity-building as well as ongoing bilateral, regional and global ICT capacity-building initiatives 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 ICT capacity-building in the context of international security. 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, recalling and reaffirming the ICT security capacity-building principles as adopted in the 2021 OEWG report, continued to highlight the need for further efforts to mainstream these principles into relevant capacity-building programming. 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.[58]

b) Emphasizing that there is no one-size-fits-all solution to capacity-building, States proposed that efforts to tailor capacity-building to a recipient State's needs, which may include the transfer of knowledge, skills and technology, on mutually-agreed terms, could be enhanced by a State's evaluation of its own current status of ICT security at the national level. Such measures would allow for the identification of gaps, as well as help to establish clear, achievable goals towards observing and adhering to the cumulative and evolving framework for responsible State behaviour in the use of ICTs. States also underlined the need to enhance the availability of capacity-building and leadership programmes on ICT security aimed at senior officials and decision-makers at the national level. In this regard, States continued to emphasize the value of South-South, triangular and sub-regional and regional cooperation, which does not replace but complements North-South cooperation.

c) States continued to discuss 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" platform for States, developed under the auspices of the UN. It was envisaged that the portal could be a platform for coordination between States on ICT security issues, and be flexible enough to evolve with the needs of States with regard to the framework for responsible behaviour in the use of ICTs as decided by States. Furthermore, the portal could be harmonized with existing and related online portals. The portal would subsequently support and facilitate the work of the future permanent mechanism and seek to achieve complementarities and avoid duplication with existing initiatives.

d) A proposal was also made for the development of a needs-based ICT security capacity-building catalogue to help States identify capacity-building needs, and to access information on how to apply for capacity-building programmes. Such a catalogue could also be integrated with the GCSCP portal if both initiatives were established by States.

e) States welcomed the High-level Global Roundtable on ICT capacity-building in the context of international security convened on 10 May 2024 in New York. The Roundtable added value to the OEWG discussions by raising the level of awareness of the urgency of ICT capacity-building among high-level government officials, while at the same time, the panel discussions with capacity-building practitioners contributed to fostering the exchange of information and best practices on action-oriented capacity-building issues. States proposed that similar roundtables on ICT capacity-building in the context of international security could continue to be convened on a regular basis in the future.

f) States acknowledged the mapping exercise[59] to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels by the UN Secretariat. In this regard, States underscored that further coordination of capacity-building efforts in ICT security was required, and that the United Nations could play an important role in such efforts. States noted these efforts should avoid duplication with similar initiatives. At the same time, while recognizing existing funding avenues for ICT capacity-building in the context of international security, it was proposed that States could continue to consider additional avenues of funding under the auspices of the future permanent mechanism

[58] Second APR, para 43a).
[59] A/AC.292/2024/2.

on ICT security in the context of international security, including through coordination with existing development programmes and relevant funding mechanisms.

g) States recognized that the OEWG itself could be an inclusive 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 and capacities to implement the framework for responsible State behaviour in the use of ICTs. States underscored that the OEWG could also be utilized as a platform for sharing best practices on ICT security capacity-building, as well as for continuing work to develop cooperative mechanisms to address threats in the use of ICTs. It was noted that this should be complementary to activities already taking place elsewhere in the UN system.

h) States, including through the OEWG, could continue to strengthen coordination and cooperation between States and other interested parties and stakeholders, including businesses, non-governmental organizations and academia. States also highlighted that youth could also be engaged in the work of the OEWG. States noted that other interested parties and stakeholders, including businesses, non-governmental organizations and academia, are already playing an important role through partnerships with States including for the purposes of training and research. Other interested parties and stakeholders, including businesses, non-governmental organizations and academia, could build on what is being done at the OEWG on capacity-building as well as offer feedback on these efforts.

i) States reaffirmed the importance of capacity-building not only as a cross-cutting issue of the OEWG's work, but also that it raises awareness and facilitates common understandings on the framework for responsible State behaviour in the use of ICTs.

Recommended next steps

51. **States to continue exchanging views at the OEWG on ICT capacity-building in the context of international security, including on sub-paragraphs 50a) to 50i) above.**

52. **The UN Secretariat is requested to prepare, for consideration by the OEWG, an initial report outlining a proposal for the development and operationalization of a dedicated Global ICT Security Cooperation and Capacity-Building Portal, taking into consideration related initiatives, with a view to optimizing synergies and avoiding duplication. States are invited to submit their views on the development of the portal, which would: a) be a practical and neutral, member State-driven and modular "one-stop shop" platform for States, developed under the auspices of the UN; b) be a repository for views and working papers submitted by States on topics related to security in the use of ICTs as well as include a calendar of events related to security in the use of ICTs; and c) include a needs-based ICT security capacity-building catalogue, leveraging on work done in existing portals where appropriate, to assist States in identifying capacity-building needs, and to access information on available resources to support identified needs. The UN Secretariat is requested prepare the initial report based on States views and on points a) to c) above, and is further requested to submit the report in time for consideration at the tenth substantive session of the OEWG in March 2025. The portal would subsequently support and facilitate the work of the future permanent mechanism.**

53. **In order to ensure sustained attention to the urgent issue of ICT security capacity-building, States to convene regular High-level Global Roundtables on ICT security capacity-building under the auspices of the future permanent mechanism to allow for strategic as well as action-oriented discussions on capacity-building in the context of ICT security. Such high-level meetings could include capacity-building practitioners, representatives of interested States, and other interested parties and stakeholders, including businesses, non-governmental organizations and academia, with due consideration given to equitable geographical representation. States in a position to do so are encouraged to provide support to representatives and experts from developing countries to attend the Roundtables.**

54. **States to further study the establishment of a United Nations voluntary fund, maximally leveraging on existing initiatives, to support the capacity-building of States on security in the use of ICTs. The fund would *inter alia,* facilitate the participation of national representatives and experts, particularly from**

developing countries, at relevant meetings under the future permanent mechanism on ICT security in the context of international security, as well as other goals identified by States. The UN Secretariat is requested to prepare, for consideration by the OEWG, an initial report outlining a proposal for the development and operationalization of this voluntary fund for consideration by States in time for consideration at the tenth substantive session of the OEWG in March 2025, with a view towards reaching a consensus recommendation on these details by July 2025 for operationalization under the auspices of the future permanent mechanism. In preparing this proposal, the UN Secretariat is requested to address, *inter alia*, issues related to the identification of an appropriate manager for the fund; financial and administrative requirements; eligibility and access by potential beneficiaries to the funds; monitoring and evaluation; and how the ICT security capacity-building principles will be mainstreamed into the implementation of the fund. The UN Secretariat is also requested to seek to achieve complementarities and avoid duplication with existing initiatives, and work on the basis that this fund may receive funding through public, private and philanthropic sources.

55. **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 parties and stakeholders, including businesses, non-governmental organizations and academia.**

G. Regular Institutional Dialogue

56. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings of the OEWG, States continued discussions on regular institutional dialogue further to the recommendations in the second APR.[60] 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:

a) Building on the objectives affirmed in relevant General Assembly resolutions, including *inter alia*, A/RES/78/16 and A/RES/78/237, relating to discussions on regular institutional dialogue within the OEWG, and on the recommendations in the 2021 OEWG Report[61] and in the first[62] and second APRs[63] of the OEWG, States deepened discussions on possible elements for the future permanent mechanism.

b) States expressed their willingness to continue discussions in order to find consensus on the establishment of a single-track future permanent mechanism. In this regard, States considered the paper prepared by the Chair entitled “Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security” which contains elements related to the guiding principles; functions and scope; structure; modalities and decision making of the future permanent mechanism.

57. States proposed that the future permanent mechanism facilitate the continued operationalization and further development of all existing initiatives set up under the auspices of the OEWG 2021-2025 and/or other previous processes, including, *inter alia*, the Global POC Directory and the Global Roundtable on ICT security capacity-building.

Recommended next steps

58. **States recommend the establishment of the future permanent mechanism based on the consensus elements contained in the paper entitled “Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security” as contained in Annex C of this report in order to ensure a seamless transition from the OEWG to the future permanent mechanism.**

[60] Paras 54-59.
[61] Report of the 2021 OEWG, A/75/816, Annex I, para 77.
[62] First APR, regular institutional dialogue section, recommended next steps, para. 2.
[63] Second APR, paras 54-59.

59. **States to continue discussions within the current OEWG and to submit recommendations in the Final Report of the OEWG to be adopted in July 2025 on: a) modalities on the participation of other interested parties and stakeholders, including businesses, non-governmental organizations and academia, in the future permanent mechanism; b) dedicated thematic groups of the future permanent mechanism; and c) other elements as required.**

60. **States recommend that the future permanent mechanism would facilitate the continued operationalization and further development of all existing initiatives set up under the auspices of the OEWG 2021-2025 and/or other previous processes, including, *inter alia*, the Global POC Directory and the Global Roundtable on ICT security capacity-building.**

. . . . .

Annex A: Voluntary Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs

1. In the second Annual Progress Report of the OEWG, States proposed the following recommended next step: "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."[64]

2. This checklist is intended as a voluntary capacity-building tool which States may wish to use as part of their efforts to implement the voluntary, non-binding norms of responsible State behaviour in the use of ICTs. States also recognized that the checklist could be a useful capacity-building tool for developing a baseline of capacities needed by States to build resilience in terms of ICT security. In this regard, this checklist could (a) serve as a starting point to support States' implementation efforts, (b) provide a useful assessment tool and assist in identifying priorities in tailored capacity-building efforts, and (c) function as a common reference to support the exchange of best practices in specific areas of ICT security. The checklist is a living document which could be updated periodically.

3. In general, the implementation of the voluntary, non-binding norms as a whole may require States to take some common, practical actions.

At the national level, these actions could include:

a) The establishment of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) and other national coordination structures and mechanisms;

b) The development of national ICT laws and policies including a national ICT strategy.

At the international level, actions by States to support the implementation of norms could include:

a) Participation in inclusive international, cross-regional, regional and sub-regional ICT processes related to ICT security;

b) Engaging in the exchange of information and best practices on different aspects of ICT security;

c) Offering and requesting assistance related to ICT incidents where relevant, utilizing avenues such as the Global Points of Contact Directory.

4. Capacity-building is key for all States to be able to take these practical actions and is therefore a central pillar to achieving the global implementation of norms. At the same time, States recognize that there is no one-size-fits-all solution to norms implementation and therefore technical gaps between States, diverse national systems and regional specificities should be taken into account in the use of this checklist for the implementation of norms.

5. This checklist of practical actions is non-exhaustive in nature. Any use of this checklist by States is completely voluntary. In the development and use of this checklist, States recall and reaffirm the previous agreements which are the elements that consolidate a cumulative and evolving framework for responsible State behaviour in the use of ICTs.[65]

[64] Second annual progress report (APR) of the current OEWG, A/78/265, paragraph 26.

[65] States reaffirmed the consensus first and second APRs of the current OEWG (A/77/275 and A/78/265 respectively), the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security (A/75/816) and the consensus reports of the 2010, 2013, 2015, and 2021 GGEs (A/65/201, A/68/98, A/70/174 and A/76/135). See the Second APR report, A/78/265, para 3.

Norm a

Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Put in place or strengthen national policy, legislation and corresponding review processes to support or facilitate international cooperation.[66]

☐ 2. Put in place or strengthen national structures and mechanisms[67] to detect, defend against or respond to, and recover from ICT incidents.

☐ 3. Put in place or strengthen whole-of-government cooperative and partnership arrangements and policies to support or facilitate international cooperation.[68]

☐ 4. Put in place or strengthen cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.[69]

☐ 5. Voluntarily survey national efforts and share national experiences on the implementation of norms.[70] This could be done 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.[71]

Action requiring international cooperation

☐ 6. Participate, where relevant, in the work of regional and sub-regional organizations which foster cooperation between States on the use of ICTs in the context of international security.[72]

Suggestion for additional actions

- Consider participating in inclusive and transparent mechanisms such as the Global Points of Contact Directory to foster cooperation and information sharing.

[66] 2021 GGE report, A/76/135, para 21, consensus GA resolution 76/19.
[67] A/76/135, para 21. Additional note: Such structures and mechanisms may include: A national centre or responsible agency or entity that leads on ICT security matters; and/ or Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
[68] A/76/135, para 21.
[69] A/76/135, para 21.
[70] A/76/135, para 21.
[71] First APR of the OEWG, A/77/275, Recommended Next Steps section on Rules, Norms and Principles of Responsible State Behaviour, para 3.
[72] Acknowledging that 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. (First and Second APR of the OEWG (A/77/275, para 5 and A/78/265 para 7 respectively)

Norm b

In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Establish or strengthen relevant national structures, ICT-related policies, processes, legislative frameworks and coordination mechanisms, to assess the severity and replicability of an ICT incident. This may include partnerships and other forms of engagement with relevant stakeholders.[73]

☐ 2. In case of ICT incidents, consider all aspects in the assessment of the incident.[74] Supported by substantiated facts, these can include:
- The incident's technical attributes;
- Its scope, scale and impact;
- The wider context, including the incident's bearing on international peace and security; and
- The results of consultations between the States concerned.[75]

☐ 3. Put in place processes for responding to malicious ICT activity attributable to another State that are in accordance with a State's obligations under the Charter of the United Nations and other international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts.[76]

Actions requiring international cooperation

☐ 4. Put in place cooperation between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, to strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.[77]

☐ 5. Use multilateral, regional, bilateral and multistakeholder platforms to exchange practices and share information on national approaches to attribution, including how States can distinguish between different types of attribution, and on ICT threats and incidents.[78]

☐ 6. All parties involved in an ICT incident are encouraged to consult among each other through relevant competent authorities.[79]

[73] A/76/135, para 26.
[74] Attribution is a complex undertaking and a broad range of factors should be considered before establishing the source of an ICT incident. Caution is called for, including consideration of how international law applies, to help avert misunderstandings and escalation of tensions between States (A/76/135, para 22).
[75] A/76/135, para 24.
[76] A/76/135, para 25.
[77] A/76/135, para 27.
[78] A/76/135, para 28.
[79] A/76/135, para 23.

☐ 7. Put in place processes for the peaceful settlement of disputes[80] regarding ICT incidents through negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice.[81]

Suggestion for additional actions

- Consider utilizing, where appropriate, multilateral communications channels at the diplomatic and technical levels, such as the Global Points of Contact Directory, for information sharing and consultations between States in the case of an ICT incident.

[80] A/76/135, para 25.
[81] The Charter of the United Nations, Article 33(1).

Norm c

States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. If an internationally wrongful act occurs within a State's territory, the State would take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective, and in a manner consistent with international and domestic law. It is not expected that the State could or should monitor all ICT activities within their territory.[82]

☐ 2. Establish and make use of structures and mechanisms to formulate and respond to requests for assistance in the case of an ICT incident.[83]

Actions requiring international cooperation

☐ 3. In the case of an ICT incident, the following steps could be undertaken:
- An affected State should notify the State from which the activity is emanating.[84]
- The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein.[85]
- The notified State should make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed.[86]

Suggestion for additional actions

- Consider utilizing, where appropriate, multilateral communications channels at the diplomatic and technical levels, such as the Global Points of Contact Directory, for information sharing and to seek or respond to requests for assistance in the case of an ICT incident.

[82] A/76/135, para 30(a).
[83] A State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may consider seeking assistance from other States or the private sector in a manner consistent with international and domestic law. States should act in good faith and in accordance with international law when providing assistance and not use the opportunity to conduct malicious activities against the State that is seeking the assistance or against a third State. (2021 GGE report, A/76/135, para 30(b)).
[84] A/76/135, para 30(c).
[85] A/76/135, para 30(c).
[86] A/76/135, para 30(c). An ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State for the incident. 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. (2021 GGE report, A/76/135, para 30(d) and Second APR, A/78/265, Annex A, para 10).

Norm d

States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs including the proper handling of the chain of custody, in accordance with obligations under international law.[87]

☐ 2. Put in place national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs.[88]

Actions requiring international cooperation

☐ 3. Strengthen and further develop mechanisms that can facilitate exchanges of information between relevant national, regional and international organizations in order to raise ICT security awareness among States and reduce the operating space for online terrorist and criminal activities.[89]

☐ 4. Use existing processes, initiatives and legal instruments and consider additional procedures or communication channels to facilitate the exchange of information and assistance for addressing criminal and terrorist use of ICTs.[90]

☐ 5. Provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.[91]

[87] A/76/135, para 33.
[88] A/76/135, para 32.
[89] A/76/135, para 33.
[90] A/76/135, para 35.
[91] A/76/135, para 33.

Norm e

States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations.[92]

☐ 2. Take note of the need to address new challenges and dilemmas that have emerged around the use of ICTs by States which may have particularly negative impacts on the exercise and enjoyment of human rights, including as reflected in new GA resolutions.[93]

☐ 3. Consider investing in and advancing technical and legal measures to guide the development and use of ICTs in a more inclusive and accessible manner that does not negatively impact members of individual communities or groups, taking into account the implications new and emerging technologies may have on human rights and ICT security.[94]

☐ 4. Engage with stakeholders which contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline.[95]

[92] A/76/135, para 36.
[93] A/76/135, paras 37 and 38.
[94] A/76/135, para 40.
[95] A/76/135, para 41.

Norm f

A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Determine which infrastructures or sectors to deem critical within your State's jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.[96]

☐ 2. Put in place relevant policy and legislative measures at the national level to ensure that ICT activities conducted or supported by a State and that may impact the critical infrastructure of or the delivery of essential public services in another State are consistent with this norm, used in accordance with their international legal obligations, and subject to comprehensive review and oversight. [97]

Action requiring international cooperation

☐ 3. Cooperate with other States regarding the protection of critical infrastructure that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet.[98]

[96] A/76/135, para 44.
[97] A/76/135, para 46.
[98] A/76/135, para 45.

Norm g

States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Ensure the safety and security of ICT products throughout their lifecycle.[99]

☐ 2. Classify ICT incidents in terms of their scale and seriousness.[100]

Actions requiring international cooperation

☐ 3. Encourage cross-border cooperation with relevant critical infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure.[101]

As part of actions to implement norm g, States may also consider taking into account the list of elements contained in the annex of General Assembly resolution 58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures as follows:

☐ 1. Have emergency warning networks regarding ICT vulnerabilities, threats and incidents.

☐ 2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.

☐ 3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.

☐ 4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.

☐ 5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.

☐ 6. Ensure that data availability policies take into account the need to protect critical information infrastructures.

☐ 7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.

[99] A/76/135, para 50.
[100] A/76/135, para 50.
[101] A/76/135, para 49.

☐ 8. Conduct training and exercises to enhance response capabilities and to test continuity and contingency plans in the event of an information infrastructure attack, and encourage stakeholders to engage in similar activities.

☐ 9. Have adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks on critical information infrastructures and to coordinate such investigations with other States, as appropriate.

☐ 10. Engage in international cooperation, when appropriate, to secure critical information infrastructures, including by developing and coordinating emergency warning systems, sharing and analysing information regarding vulnerabilities, threats and incidents and coordinating investigations of attacks on such infrastructures in accordance with domestic laws.

☐ 11. Promote national and international research and development and encourage the application of security technologies that meet international standards.

Suggestion for additional actions

- Consider determining the structural, technical, organizational, legislative and regulatory measures and contingency plans necessary to protect national critical infrastructure and restore functionality if an incident occurs.

Norm h

States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Establish national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security.[102]

Actions requiring international cooperation

☐ 2. Where required to mitigate malicious ICT activity aimed at CI and CII, seek or offer assistance bilaterally, or through regional or international arrangements, taking into account due regard for sovereignty.[103]

☐ 3. Seek the services of the private sector to assist in responding to requests for assistance where appropriate.[104]

☐ 4. Engage in cooperative mechanisms that define the means and mode of ICT crisis communications and of incident management and resolution, including through establishing common and transparent processes, procedures and templates.[105]

Suggestion for additional actions

- Consider utilizing, where appropriate, multilateral communications channels at the diplomatic and technical levels, such as the Global Points of Contact Directory, for information sharing and to seek or respond to requests for assistance in the case of an ICT incident.

[102] A/76/135, para 53. Additional note: Such structures and mechanisms may include: A national centre or responsible agency or entity that leads on ICT security matters; and/ or Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
[103] A/76/135, paras 51 and 52.
[104] A/76/135, para 52.
[105] A/76/135, paras 54 and 55.

Norm i

States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Put in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management, consistent with a State's international obligations, taking into account a variety of factors, including the benefits and risks of new technologies.[106]

☐ 2. Establish 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.[107]

☐ 3. Establish measures to enhance the integrity of the supply chain, including by requiring ICT vendors to incorporate safety and security in the design, development and throughout the lifecycle of ICT products. Consider establishing independent and impartial certification processes.[108]

☐ 4. Put in place legislative and other safeguards that enhance the protection of data and privacy.[109]

☐ 5. Put in place measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.[110]

☐ 6. Strengthen partnership with the private sector to collaboratively enhance the security of and in the use of ICTs. 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.[111]

Actions requiring international cooperation

☐ 7. Increase attention to national policy and in dialogue with other States and relevant actors at the United Nations and other fora on how to ensure all States can compete and innovate on an equal footing, so as to enable the full realization of ICTs to increase global social and economic development and contribute to the maintenance of international peace and security, while also safeguarding national security and the public interest.[112]

---

[106] A/76/135, para 57(a).
[107] Second APR (A/78/265), para 23d).
[108] A/76/135, para 58(a).
[109] A/76/135, para 58(b).
[110] A/76/135, para 58(c).
[111] Second APR (A/78/265), para 23(e).
[112] A/76/135, para 57(c).

☐ 8. Participate in inclusive, transparent multilateral processes on 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. [113]

[113] Second APR (A/78/265), para 23(d).

Norm j

States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Put in place vulnerability disclosure policies and programmes including a coordinated vulnerability disclosure process to minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities.[114]

☐ 2. In consultation with relevant industry and other ICT security actors, develop guidance and incentives, consistent with relevant international technical standards, on:
- The responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes;
- The types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and
- How to handle sensitive data and ensure the security and confidentiality of information.[115]

☐ 3. Put in place measures which facilitate international cooperation on the responsible reporting of ICT vulnerabilities including requests for assistance between countries and emergency response teams, consistent with domestic legislation.[116]

☐ 4. Put in place legal protections for researchers and penetration testers. [117]

Actions requiring international cooperation

☐ 5. Put in place or participate in impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against any misuse.[118]

☐ 6. Use existing multilateral, regional and sub-regional bodies and other relevant channels and platforms involving different stakeholders for developing a shared understanding of the mechanisms and processes for responsible vulnerability disclosure.[119]

[114] A/76/135, para 61.
[115] A/76/135, para 63.
[116] A/76/135, para 61.
[117] A/76/135, para 62.
[118] A/76/135, para 62.
[119] A/76/135, para 64.

Norm k

States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Voluntary, practical actions for implementing this norm

Actions at the national level

☐ 1. Consider categorizing CERTs/CSIRTs as part of national critical infrastructure.[120]

☐ 2. Put in place a national ICT security incident management framework with designated roles and responsibilities, including for CERTs/CSIRTs, to facilitate cooperation and coordination among CERTs/CSIRTs and other relevant security and technical bodies at the national, regional and international levels.[121]

☐ 3. Include policies, regulatory measures or procedures in the national ICT security incident management framework that clarify the status, authority and mandates of CERTs/CSIRTs and that distinguish the unique functions of CERTs/CSIRTs from other functions of government.[122]

☐ 4. Consider publicly declaring or putting in place measures affirming that authorized emergency response teams will not be used to engage in malicious international activity and acknowledge and respect the domains of operation and ethical principles that guide the work of authorized emergency response teams.[123]

Action requiring international cooperation

☐ 5. Facilitate cooperation and coordination among CERTs/CSIRTs and other relevant security and technical bodies at the national, regional and international levels including through national ICT security incident management frameworks.[124]

[120] A/76/135, para 66.
[121] A/76/135, para 68.
[122] A/76/135, para 68.
[123] A/76/135, para 67.
[124] A/76/135, para 68.

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 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.

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

In addition to the Global CBMs listed above States have included the following as additional voluntary global CBMs:

CBM 5. Promote information exchange on cooperation and partnership between States to strengthen capacity in ICT security and to enable active CBM implementation

Capacity-building programmes are an important avenue of collaboration which could strengthen relationships as well as build trust and enhance confidence between States.

CBM 6. Engage in regular organization of seminars, workshops and training programmes on ICT security

The regular organization of seminars, workshops and training programmes on relevant issues related to ICT security with the inclusive representation of States could increase communication and mutual understanding and contribute to confidence-building.

CBM 7. Exchange information and best practice on, *inter alia,* the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building

Exchange of information and best practice on, *inter alia*, the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building could build trust and enhance confidence between States.

CBM 8. Strengthen public-private sector partnerships and cooperation on ICT security

A range of technical capabilities and knowledge are required to detect, defend against and respond to and recover from ICT incidents. In this regard, public-private sector partnerships and cooperation, including regular dialogue and the exchange of good practice, could contribute to confidence-building.

Annex C: Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security

1. This paper sets out elements for the establishment at the United Nations of a future permanent mechanism on ICT security in the context of international security following the conclusion of the work of the Open-Ended Working Group on security of and in the use of ICTs 2021-2025 (OEWG). The permanent mechanism will be open-ended and action-oriented in nature; it 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 [125] with the aim of continuing to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment. [126]

2. Building on the objectives affirmed in relevant General Assembly resolutions, including *inter alia*, A/RES/78/16 and A/RES/78/237, relating to discussions on regular institutional dialogue within the OEWG, States recommend the establishment of the future permanent mechanism based on the consensus elements contained in this paper so as to ensure a seamless transition to the new mechanism.

Guiding Principles

3. The establishment of the future permanent mechanism would be guided by the elements recommended by consensus in the OEWG, including the common elements recommended by consensus in paragraphs 55 to 57 of the second Annual Progress Report (APR) of the OEWG and reproduced below.

4. The future permanent mechanism 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.

5. 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.

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

7. States 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, States noted that regional efforts are complementary to the work of the future permanent mechanism. [127]

[125] Second APR, para 55c).
[126] Second APR, para 55b).
[127] First APR, A/77/275, para 5 and Second APR, A/78/265, para 7.

Functions and Scope

8. The future permanent mechanism would address the issue of ICT security in the context of international security with the aim of promoting an open, secure, stable, accessible, peaceful and interoperable ICT environment.

9. While ensuring continuity and building upon the outcomes of the Open-ended Working Group 2021-2025 and previous OEWG and GGE agreements, the functions of the open-ended action oriented permanent mechanism are to strengthen the ICT security capacity of all States, including to develop and implement the cumulative and evolving framework for responsible State behaviour in the use of ICTs; to advance implementation of the cumulative and evolving framework for responsible State behaviour in the use of ICTs; to further develop the cumulative and evolving framework for responsible State behaviour in the use of ICTs; and, guided by the functions listed above, the open-ended action-oriented permanent mechanism will address, through facilitating discussions of an integrated, policy-oriented and cross-cutting nature, the following issues, *inter alia*, existing and potential threats; voluntary, non-binding norms of responsible State behaviour and the ways for their implementation, recognizing that additional norms could be developed over time; to continue to study how international law applies in the use of ICTs, noting the possibility of future elaboration of additional binding obligations, if appropriate, and 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;[128] to develop and implement confidence-building measures; and to develop and implement capacity-building.

10. Taking into account the functions of the future permanent mechanism, States recognized that international cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use.[129] Furthermore, as capacity-building cuts across the issues of ICT security and acts as an enabler which strengthens ICT resilience and the ability of States to detect, defend against or respond to malicious ICT activities, action-oriented approaches to capacity-building such as the matching of needs with resources and technical assistance will be an important function of the future permanent mechanism. Additionally, States recognize that capacity-building is also necessary to enable States to participate in the future permanent mechanism in an inclusive manner and on equal footing.

11. The future permanent mechanism would promote engagement and cooperation with interested parties and stakeholders, including businesses, non-governmental organizations and academia, learning from and building on the experience of the OEWG process. The participation of other interested parties and stakeholders, including businesses, non-governmental organizations and academia, at the future permanent mechanism will be guided by:

(a) The aim of promoting inclusive discussions at the future permanent mechanism, drawing on relevant expertise to support the work of the mechanism as appropriate;

(b) Substantive plenary sessions, dedicated thematic groups, dedicated intersessional meetings and review conferences would include opportunities for consultation between States and other interested parties and stakeholders, including businesses, non-governmental organizations and academia;

(c) The overarching principle that the future permanent mechanism is a state-led process where negotiations and decisions on ICT security remain the prerogative of States; and

(d) States to continue discussions within the current OEWG and to submit recommendations in the Final Report of the OEWG to be adopted in July 2025 on modalities on the participation of other interested parties and stakeholders, including businesses, non-governmental organizations and academia, in the future permanent mechanism.

Structure

12. The future permanent mechanism would be structured in a five-year cycle consisting of two biennial cycles followed by a one-year review cycle. The meetings of the future permanent mechanism are as follows:

[128] Second APR, para 32.
[129] 2015 GGE report, para 19.

a) **Substantive Plenary Sessions:** One substantive plenary session to be convened per year during each biennial cycle, with each session lasting at least one week in duration. Substantive plenary sessions would carry out discussions in accordance with the functions and scope set out above, as well as consider the work and recommendations of dedicated thematic groups.

b) **Dedicated Thematic Groups**: Dedicated thematic groups to be established by decisions of the future permanent mechanism for conducting focused discussions, as required. The dedicated thematic groups would report to the substantive plenary sessions with updates and recommendations. States to continue discussions within the current OEWG on dedicated thematic groups of the future permanent mechanism and to submit recommendations in the Final Report of the OEWG to be adopted in July 2025.

c) **Dedicated Intersessional Meetings**: The Chair of the future permanent mechanism, in consultation with States, could also convene dedicated intersessional meetings to engage in additional discussions on specific issues or to discuss reports and recommendations, as necessary.

d) **Review Conference:** A Review Conference to be convened every fifth year to review the effective functioning of the future permanent mechanism and provide strategic direction and guidance for the substantive plenary sessions and dedicated thematic groups over the subsequent four years. Additionally, at the Review Conference, any modifications to the elements of the future permanent mechanism contained in this document could also be decided by States on the basis of consensus.

13. For each biennial cycle, the future permanent mechanism will be led by a Chair elected to serve for a period of two years on the basis of equitable geographical representation. In addition, a Chair will be elected to serve for a period of one year on the basis of equitable geographical representation to lead the one-year Review Conference process.

14. To facilitate inclusive participation, meetings of the future permanent mechanism, including the substantive plenary sessions, meetings of any dedicated thematic groups, and dedicated intersessional meetings would not be held in parallel, with the possibility of some meetings being convened in a hybrid format.

Modalities

15. The future permanent mechanism would operate as follows:

a) The permanent mechanism to be established as a subsidiary body of the UN General Assembly reporting to the First Committee.

b) The UN Office for Disarmament Affairs to serve as the Secretariat of the permanent mechanism.

c) An e-portal and/or website to be established to support and facilitate the work of the permanent mechanism.

d) The Global POC Directory will serve as a voluntary standing tool for use by States.

e) Formal meetings of the permanent mechanism to be convened at UNHQ in New York.

16. To ensure a seamless transition from the work of the OEWG to the future permanent mechanism, States recommend the following arrangements:

a) An organizational session to be convened no later than March 2026 to carry out, *inter alia*, (i) the election of the Chair of the future permanent mechanism, (ii) the adoption of the agenda, (iii) the establishment of dedicated thematic groups, and (iv) the adoption of other modalities as required.

b) The first substantive plenary session to be convened no later than June 2026.

Decision Making

17. The future permanent mechanism would take all decisions based on the principle of consensus. Based on consultations with States, decisions could be put forward by the Chair for adoption by States on a consensus basis at any time during a substantive plenary session, with decisions to be formalized as soon as they are decided upon by the future permanent mechanism.