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

10 July 2025

Excellency,

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

I would like to thank delegations for their comments on the Final Draft of the OEWG's Final Report dated 9 July 2024. I have reflected carefully on the views expressed by delegations and have made some adjustments to the text in order to fine-tune the overall balance with the aim of reaching consensus. The revised text is incorporated in document A/AC.292/2025/CRP.1 as enclosed.

This document represents my best attempt to formulate the balance that is required to reach consensus within the constraints of the positions and views expressed by delegations. Having heard the views of all delegations, my sense is that consensus remains possible but the path to consensus is extremely narrow. In this regard, I call on all delegations to resist any temptation to request further changes as doing so could set off a cycle of further amendments that would swiftly unravel the fine balance in this document.

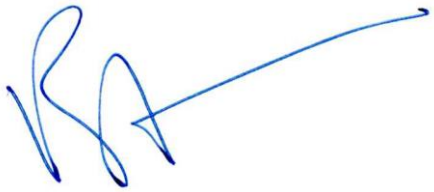
It is my intention to present the CRP document for formal adoption at the ninth meeting of the eleventh and final substantive session of the OEWG on the morning of Friday, 11 July 2025. I want to reiterate the utmost importance of securing consensus adoption of this document tomorrow in order to bring our

318 East 48th Street, New York, NY 10017, United States of America | T +1 (212) 826 0840 F +1 (212) 826 2964 | mfa.gov.sg/newyork

work over the past five years to a successful conclusion and to ensure a smooth and seamless transition to the single-track Global Mechanism.

The final decision on the future of the UN's efforts in this domain now lies in the hands of delegations. I appeal to all delegations to exercise utmost flexibility in any way possible so as to support the consensus adoption of the CRP document at our meeting on the morning of Friday, 11 July 2025.

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



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

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

Enclosure:

- Annex A – A/AC.292/2025/CRP.1

United Nations A/AC.292/2025/CRP.1

General Assembly

11 July 2025

English only

Open-ended working group on security of and in the use of information and communications technologies 2021-2025
Eleventh substantive session, New York
7-11 July 2025

Draft Final Report

A. Overview

1. The ninth, tenth and eleventh formal sessions 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 has become very challenging, with rising concerns over the malicious use of ICTs by State and non-state actors that impact international peace and security.

2. States noted that the final year of the OEWG's mandate coincided with the 80th anniversary of the founding of the United Nations (UN), an important milestone for the international community and the multilateral system. States reflected on the decades of work at the United Nations in the field of ICT security, including the work of the OEWG, and reaffirmed the value and importance of an inclusive, transparent and democratic intergovernmental platform to build understanding, foster dialogue and strengthen cooperation on security of and in the use of ICTs. In this regard, States acknowledged that the OEWG made a positive contribution to promoting common understandings and served as a vehicle for building trust and confidence.

3. States noted the increasing engagement and constructive participation of delegations from all regions in the work of the OEWG on the issue of security of and in the use of ICTs over the course of the past eleven substantive sessions. At these sessions, States contributed substantively to the work of the OEWG, and agreed by consensus to the first, second and third annual progress reports. These three annual progress reports build on each other and, in conjunction with the final report, will form the foundation upon which discussions will continue in the future permanent mechanism.

4. In concluding the work of the OEWG, States recalled the consensus decisions and resolutions of the General Assembly in which States agreed that 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

[1] GA decisions 77/512 and 75/564, GA resolutions 70/237 and 76/19.
[2] A/75/816.

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]

5. Furthermore, States reaffirmed the consensus first, second and third 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 had built its work, and which will be continued by the future permanent mechanism.

6. 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, States acknowledged that the OEWG had addressed its mandate in a balanced manner and had given 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.

7. States recognised that the discussions at the OEWG have deepened over the last few years, leading to the consensus adoption of the first, second and third annual progress reports. As their discussions deepened, 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.

8. In the course of their discussions in the OEWG, States recognized that capacity-building is an important confidence-building measure, and is a topic that cuts across all the pillars of the OEWG's work and that a holistic approach to capacity-building on security of and in the use of ICTs was essential. In this regard, States emphasized that the need for sustainable, effective and affordable solutions was indispensable and urged the future permanent mechanism to ensure continuity by building on the outcomes and common understandings reached in the OEWG.

9. States 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

[3] A/76/135.
[4] A/77/275, A/78/265 and A/79/214 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.

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.[8] In this regard, States reaffirmed the continued value and relevance of the ICT security capacity-building principles, as adopted in the 2021 OEWG report and contained in the Second APR, for the work of the future permanent mechanism.

10. States noted that the OEWG engaged 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.[9]

11. 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 its work.[10]

12. States noted and welcomed the increasing level of participation of women delegates in the OEWG and the prominence of a gender perspective in its discussions. In this regard, States underscored the importance of continuing to narrow 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]

13. This final report includes concrete actions and cooperative measures to address ICT threats and captures concrete progress made at the OEWG to promote an open, secure, stable, accessible and peaceful and interoperable ICT environment, whilst building upon the first, second and third APRs, endorsed by consensus in General Assembly Decisions 77/512 and 78/541 and General Assembly Resolution 79/237 respectively, as well as the consensus reports of the 2010, 2013, 2015, and 2021 GGEs.[12] States agreed that the OEWG had throughout the course of its work, served as an important confidence-building measure and enhanced understanding between countries in the area of ICT security in concrete and action-oriented ways. States further agreed that the future permanent mechanism should build on the work of the OEWG and continue to serve such a purpose. This final report will be submitted to the General Assembly pursuant to the OEWG's mandate contained in resolution 75/240.

B. Existing and Potential Threats

14. During the ninth, tenth and eleventh 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, second and third 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 has become very challenging. In their discussions, States recognized the need to continue to address the diverse landscape of ICT threats in a manner that represents the realities of all countries and regions.

[8] Third APR, para 7.
[9] Third APR, para 8.
[10] Third APR, para 9.
[11] Third APR, para 10.
[12] A/65/201, A/68/98, A/70/174 and A/76/135.

15. States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in conflicts between States is becoming more and more likely, and noted that ICTs have already been used in conflicts in different regions[13] which affects military forces as well as civilians and civilian objects. In this regard, States also highlighted the need to use ICTs in a manner consistent with international law and to promote their use for peaceful purposes.

16. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a very disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States.[14] States also noted that ICT criminal activity could increase in scale and severity such that it seriously disrupts the work of governments and international organizations and could potentially impact international peace and security.

17. States expressed serious concern regarding the increase in malicious ICT activities impacting critical infrastructure (CI) and critical information infrastructure (CII). While emphasizing that it is each State's prerogative to determine which infrastructures it designates as critical and that all CI and CII need to be protected, States also highlighted with concern ICT incidents that target specific sectors. Such CI and CII can potentially provide essential services across borders and jurisdictions and malicious ICT attacks affecting them may have cascading national, regional and global effects,[15] and underlined the need to protect such cross-border CI.

18. States continued to underscore 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.[16]

19. States continued to highlight 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]

20. States expressed concern that industrial control systems (ICS), operational technology (OT), 5G networks, the Internet of Things (IoT), data centres, cloud computing services, technologies at the network perimeter, such as virtual private networks (VPNs), firewalls and routers, as well as managed service providers, are increasingly vulnerable to malicious ICT activity which may have widespread consequences.

21. States expressed serious concern regarding malicious ICT activity targeting international organizations and humanitarian organizations, including their in-country missions, 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]

22. States continued to note a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State, including States in transitional phases or emerging from armed conflicts. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.[19] States expressed particular concern regarding malicious ICT activities that are aimed at interfering in the internal affairs of States.[20]

[13] Third APR, para 13.
[14] Report of the 2021 OEWG, A/75/816, Annex I, para 16; Third APR, para 13.
[15] Third APR, para 14.
[16] Report of the 2021 OEWG, A/75/816, Annex I, para 18; Third APR, para 15.
[17] Third APR, para 16.
[18] Third APR, para 17.
[19] Third APR, para 18.
[20] Third APR, para 18.

23. 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.[21] In this context, States highlighted the critical importance of security-by-design throughout the lifecycle of ICT products and services as a fundamental measure to mitigate such risks.

24. 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 as a service.[22] States also expressed concern over ransomware targeting CI and CII as well as State institutions. Moreover, 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 continued to note 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 peace and security.

25. 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.[23] States emphasized that without meaningful action, these threats were expected to increase as the market grows and diversifies further. States also emphasized that measures taken against this threat should not be detrimental to the ability of States, in particular developing countries, to access and utilize ICT tools for purposes consistent with international law.

26. States noted that technologies are neutral in and of themselves,[24] 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 both vulnerabilities as well as security solutions in the ICT space. It was also noted that AI models, such as Large Language Models (LLMs) and generative models, while providing exponential opportunities, have also reduced barriers to entry for the undertaking of malicious ICT activities, including through AI-generated malware and deep fakes. States also underscored the need to ensure the safety and security of AI systems as well as the data used to train AI models. Risks could also be exacerbated through the intersection of new technologies. States thus highlighted the need to advance the development and deployment of, and prepare for the migration to post-quantum cryptographic solutions.

27. Considering the growth and aggregation of data associated with new and emerging technologies, including IoT, AI and cloud computing, States also noted the increasing relevance of data protection and data security.[25]

28. 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

[21] Third APR, para 19.
[22] Third APR, para 20.
[23] Third APR, para 21.
[24] Third APR, para 22.
[25] Third APR, para 24.

benefits of digital technology were not enjoyed equally by all and accordingly underlined the need to give due attention to the growing digital divide in the context of accelerating the implementation of the 2030 Agenda for Sustainable Development, while respecting the national needs and priorities of States.[26]

29. 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.[27] 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,[28] concrete actions and capacity-building initiatives under the cumulative and evolving framework for responsible State behaviour.[29] In order to combat these threats, States encouraged the strengthening of cooperation between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) as well as the building of their capacities, and also proposed the strengthening of public-private sector partnerships. States further encouraged the enhancing of dialogue on ICT security between different sectors at the national level including technical, diplomatic and legal sectors.

Recommendations

30. **States to continue discussions at the future permanent mechanism on existing and potential threats to security in the use of ICTs in the context of international security, and to continue discussions on possible cooperative measures to address these threats, acknowledging in this regard that all States committing to and reaffirming the 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.**

C. Rules, Norms and Principles of Responsible State Behaviour

31. During the ninth, tenth and eleventh sessions as well as the dedicated intersessional meetings of the OEWG, States continued discussions on rules, norms and principles of responsible State behaviour.

32. 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.[30]

33. States reaffirmed that norms do not replace or alter States' obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.[31] Furthermore, States acknowledged that the work of the OEWG has contributed to strengthening the cumulative and evolving framework of responsible State behaviour, which provides a foundation for the future permanent mechanism.

[26] Third APR, para 26.
[27] Report of the 2021 OEWG, A/75/816, Annex I, para 20.
[28] Report of the 2021 OEWG, A/75/816, Annex I, para 22.
[29] Third APR, para 28.
[30] Report of the 2021 OEWG, A/75/816, Annex I, paras 64 and 65; Third APR, para 31a).
[31] Report of the 2021 OEWG, A/75/816, Annex I, para 25.

34. States, reaffirming their commitment to the cumulative and evolving framework for responsible State behaviour in the use of ICTs, reiterated the following:

a) As set out in norm (c)[32], 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.[33]

b) As set out in norms (f)[34],(g)[35] and (h)[36], States continued to underline the importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII). States highlighted that ICT activity that intentionally damages CI or CII or otherwise impairs the use and operation of CI or CII to provide services to the public can also have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population and can be escalatory.[37]

c) As set out in norm (h), States should respond to appropriate requests for assistance by another State whose CI is subject to malicious ICT acts. Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm. In this regard, common templates for requesting assistance and responding to such requests can ensure that the State seeking assistance provides as complete and accurate information as possible to the State from which it seeks the assistance, thereby facilitating cooperation and timeliness of response.[38]

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 and lessons learned 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,[39] 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.[40] States further recognized that capacity-building can assist CI and CII operators in this regard. States also recognized the need to encourage voluntary exchanges between relevant government authorities and CI and CII operators, in accordance with the national legislation of States, to facilitate better cooperation in the protection of CI and CII.

[32] Norm (c): States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs.
[33] Third APR, para 31b).
[34] 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.
[35] Norm (g): States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.
[36] 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.
[37] Report of the 2021 GGE, A/76/135, para 42, consensus GA resolution 76/19; Second APR para 23c); Third APR, para 31c).
[38] Report of the 2021 GGE, A/76/135, para 54, consensus GA resolution 76/19.
[39] 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).
[40] 2021 OEWG report, A/75/816, para 18.

e) As set out in norm i)[41], 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.[42]

f) Furthermore, under norm i), States also proposed safeguarding against the potential for the illegitimate and malicious use by State and non-State actors of commercially available ICT intrusion capabilities by taking steps to ensure that their development, facilitation, dissemination, purchase, transfer, export or use is consistent with international law.

g) Also under norm i), States continued to emphasize 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.[43]

h) 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.[44]

35. 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.[45] States further encouraged whole-of-government coordination in this regard and the raising of awareness of these norms at the national level. States recognized that the technical gaps between States, diverse national systems and regional specificities should be taken into account.

36. States also discussed a non-exhaustive list of proposals on rules, norms and principles with varying levels of support from States as follows:

a) States discussed the Voluntary Checklist of Practical Actions at Annex A of the third APR for the voluntary implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs, while reaffirming States' prerogative to structure their implementation efforts in accordance with national policies and circumstances.

b) States noted the value of developing targeted ICT security capacity-building programmes to address challenges to implementation or gaps in capacity. In this regard, technical gaps between States, diverse national systems and regional specificities should be taken into

[41] 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.
[42] Third APR, para 31e).
[43] Third APR, Para 31f).
[44] Third APR, para 31g).
[45] Report of the 2021 OEWG, A/75/816, para 27.

account in the use of the voluntary checklist. States also recognized the guidance on implementation provided by the 2021 GGE report,[46] and further noted that 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.

c) 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".[47]

d) 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. In this regard, several proposals were also put forward for possible new norms which are still being discussed by States.[48]

e) States also proposed that the future permanent mechanism could continue the discussion on the possible development of additional norms.

Recommendations

37. States to continue discussions at the future permanent mechanism on rules, norms and principles of responsible State behaviour in the use of ICTs.

38. States to continue discussing and updating, at the future permanent mechanism 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 the OEWG's third APR, with a view to its finalization, recognizing that it is the prerogative of States to structure their implementation efforts in accordance with national policies and circumstances.

D. International Law

39. During the ninth, tenth and eleventh 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.[49]

40. 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[50]:

a) "The OEWG could convene discussions on specific topics related to international law. Such discussions should focus on identifying areas of convergence and consensus. A non-exhaustive, open list of topics proposed by States for further discussion under international law includes: How international law, in particular the Charter of the United Nations, applies in the use of ICTs; sovereignty; sovereign equality; non-intervention in the internal affairs

[46] A/76/135.
[47] Third APR, para 31j).
[48] Third APR, para 31k).
[49] Third APR, para 35.
[50] First APR, International Law Section, recommended next step 2.

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.";[51]

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."[52]

41. 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.[53] 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. [54]

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";[55] 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 peacse 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".[56] [57]

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".[58]

[51] Report of the 2021 OEWG, A/75/816, Annex I, para 80.
[52] Report of the 2021 GGE, A/76/135, para 71(f), consensus GA resolution 76/19.
[53] Third APR, para 37a).
[54] Report of the 2021 GGE, A/76/135, para 71(b), consensus GA resolution 76/19.
[55] Article 2(3) of the Charter of the United Nations.
[56] Article 33(1) of the Charter of the United Nations.
[57] Third APR, para 37b).
[58] Third APR, para 37c).

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.[59]

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.[60]

42. States noted that discussions on international law have significantly deepened during the course of the OEWG and welcomed the active participation of an increasing number of States in these discussions. At these discussions, States expressed views, without prejudice to their positions, on, *inter alia*, sovereignty, State responsibility, due diligence, and international humanitarian law, as well as the proposals contained in paragraph 43 below.

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

a) States noted discussions on international law at the ninth, tenth and eleventh sessions as well as at the intersessional meetings of the OEWG, and further welcomed the continued active participation of an increasing number of States at these discussions. States continued to note that these discussions on international law have significantly deepened during the course of the OEWG, and 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.[61]

b) 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. [62]

c) In this regard, States welcomed the voluntary sharing by States of national views and positions on how international law applies to the use of ICTs. States noted and discussed the various views made available on the website of the OEWG in line with relevant recommendations contained in previous APRs.

d) Acknowledging existing capacity-building initiatives on 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. States proposed that such capacity-building efforts should be made in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report and reaffirmed in the second APR, and could include:

i. Workshops, conferences and the exchanging of best practices at the international, inter-regional, regional and sub-regional levels;

ii. The development of online and in-person training courses and modules as well as online resource libraries on how international law applies in the use of ICTs in order to improve

[59] Report of the 2021 GGE, A/76/135, para 71(c), consensus GA resolution 76/19; Third APR, para 37d).
[60] Third APR, para 37e).
[61] Third APR, para 38a).
[62] Third APR, para 38c).

accessibility and promote wider participation, with due respect for gender balance and geographical representation;

iii. Strengthening collaboration with academics, civil society and the private sector to tailor international law capacity-building programmes in the context of the evolving ICT landscape; and

iv. Partnering with regional and sub-regional organizations to implement capacity-building initiatives that address localized needs and leverage regional expertise.

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. [63]

Recommendations

44. States to continue discussions at the future permanent mechanism on how international law applies in the use of ICTs.

45. States are encouraged to continue to voluntarily share their national views and positions, which may include national statements and State practice, on how international law applies to the use of ICTs. The UN Secretariat is requested to make these views available on the website of the future permanent mechanism for the reference of all States.

46. 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 and as reflected in the second APR.

E. Confidence-Building Measures

47. During the ninth, tenth and eleventh 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:

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.[64]

b) States continued to express their strong support and commitment to the Global Points of Contact (POC) Directory which was launched on 9 May 2024. States also expressed appreciation for the continued six-monthly "ping" test of the Global POC Directory initiated by the UN Secretariat. States recalled the purposes and principles of the Global POC Directory as set out in Annex A of

[63] Third APR, para 38e).
[64] Third APR, para 42a).

the Second APR,[65] noting also that the Global POC Directory could support the taking forward of CBMs in general. States underscored the need to continue developing and operationalizing the Global POC directory and expressed support for the smooth transition of the Global POC directory from under the auspices of the OEWG to the future permanent mechanism.

c) States continued to highlight that a step-by-step approach be taken to develop the Global POC Directory under the auspices of the future permanent mechanism 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.[66] In the course of their discussions in the OEWG, States in a position to do so were encouraged to provide support to POCs from developing countries to attend in-person POC meetings under the future permanent mechanism. States emphasized that comprehensive capacity-building is needed in order to ensure that all States are able to participate meaningfully in the Global POC Directory.

d) States emphasized the important role of CBMs in the protection of CI and CII and proposed further study of concrete measures on how CBMs can be used in the case of severe ICT incidents affecting CI and CII.

e) States noted the "Template for Communication – Example provided by the Secretariat pursuant to A/79/214" developed by the UN Secretariat, and expressed their readiness to further discuss and develop this template at the future permanent mechanism. At the same time, States also noted that the use of such templates should be flexible and voluntary so as not to unnecessarily encumber the use of the Global POC Directory, particularly in urgent situations. States proposed that further guidance could be developed on the type of information that could be shared between POCs to facilitate productive communication. In this regard, States also underscored that technical requests made through the Global POC Directory should be factual and objective in nature.

f) States recalled the simulation exercise organized from 10 to 11 and 17 to 18 March 2025 by the OEWG Chair, in partnership with interested States and with the support of the UN Office for Disarmament Affairs (UNODA), the UN Institute for Disarmament Research (UNIDIR) and the International Telecommunications Union (ITU).[67]

g) States emphasized the importance of encouraging implementation of the "Initial List of Voluntary Global Confidence-Building Measures" contained in Annex B of the third APR. In this regard, States encouraged practical steps for the implementation of CBMs including fostering dialogue between States on CBM implementation; the voluntary sharing of information nationally, sub-regionally, regionally and globally; and the sharing of lessons learned and best practices.

h) States continued to propose 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.[68]

i) 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.[69]

[65] A/78/265.
[66] Third APR, para 42c).
[67] Third APR, para 46.
[68] Third APR, para 42f).
[69] Third APR, para 42g).

j) States continued to emphasize that the OEWG itself served as an important CBM, providing a forum for discussing issues on which there is agreement and issues on which there is not yet agreement.[70] In this regard, States highlighted that the future permanent mechanism could likewise serve as a CBM as well as a platform for the implementation of CBMs.

k) States reaffirmed the progress made on the development and implementation of CBMs in the OEWG, in particular the initial list of eight voluntary global CBMs as adopted in the third APR. States reaffirmed the importance of continuing discussions on the development and implementation of CBMs at the future permanent mechanism and in that regard took note of proposals that were put forward, including relating to the facilitation of access for all States to ICT security products and tools.

Recommendations

48. States to continue discussions at the future permanent mechanism on the development and implementation of CBMs.

49. States to continue the further development and operationalization of the Global POC Directory at the future permanent mechanism, and in that regard, States to continue discussing ways to improve the work of the Global POC Directory and are encouraged to actively participate in the six-monthly "ping" tests for POCs as envisaged in Annex A of the Second APR. States who have not already done so are encouraged to nominate national POCs to the Global POC Directory as soon as possible.

50. The UN Office of Disarmament Affairs is requested to convene regular simulation exercises in hybrid format, with the support of interested States and in partnership with relevant UN entities as appropriate.

51. States to continue discussing the "Template for Communication – Example provided by the Secretariat pursuant to A/79/214"[71] developed by the UN Secretariat as a voluntary tool to facilitate communication between POCs and to engage in further discussion on other templates.

52. 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.[72]

F. Capacity-Building

53. During the ninth, tenth and eleventh 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 sessions, States continued to share national experiences as well as working papers 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:

a) States, recalling and reaffirming the ICT security capacity-building principles as adopted in the 2021 OEWG report and contained in the second APR, 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

[70] Third APR, para 42h).
[71] Available on the OEWG website.
[72] Second APR, para 42.

policies as well as the development of checklists or questionnaires to identify needs and gaps in this area.[73]

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 beyond technical personnel to include policymakers, educators, law enforcement as well as leadership programmes on ICT security aimed at community leaders, senior officials and decision-makers at the national level.[74] In this regard, States commended the UN-Singapore Cyber Fellowship Programme as a useful initiative to advance this objective. At the same time, States highlighted the need to build better understanding across policy, operational, technical, legal and diplomatic domains to support decision and policy-making.

c) States emphasized that focusing capacity-building efforts on strengthening human resources, institutional capacity and infrastructure would ensure sustainability and build long-term resilience in a State's ICT security capacities, particularly for States which currently have limited ICT infrastructure and expertise. States also proposed, where appropriate, the voluntary standardization of curriculum or scope of technical ICT security capacity-building programming in order to ensure that the same standard of expertise is attained by beneficiary States. States further proposed that a collaborative approach to capacity-building including the co-designing of ICT security capacity-building activities would build trust and ensure the activities are tailored to the needs of the recipients. States continued to underscore the value of South-South, triangular and sub-regional and regional cooperation, which does not replace but complements North-South cooperation.[75] States reiterated the valuable contributions of South-South and triangular cooperation in ICT security capacity-building and encouraged the expansion of such mechanisms, which complement but do not replace North-South cooperation, taking into account shared experiences and specificities.

d) States proposed that mentorship programmes, such as to provide ongoing technical advice, could be developed as a longer-term supplement to training programmes. Such mentorship programmes could be aimed at fostering technical expertise, including within Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs), on topics such as forensic analysis and incident management and response to enhance readiness against evolving IT threats. In this regard, States also proposed strengthening cooperation between CERTs and CSIRTs, including, where appropriate, through enhanced information sharing, joint training programmes, and mutual assistance arrangements, with particular support for developing country teams. States also proposed that developing countries should have ready access to tools and resources that could enable them to detect, defend against or respond to ICT threats.

e) States discussed the initial report[76] prepared by the UN Secretariat outlining a proposal for the development and operationalization of a dedicated Global ICT Security Cooperation and Capacity-Building Portal (GSCCP). Taking into account para 50c) of the Third APR, States further discussed that the dedicated GSCCP, when established, could initially serve as: (a) the official website of the future permanent mechanism; (b) a central location for providing practical information on ICT security events to foster the active participation of States; and (c) a platform to facilitate the sharing of information relating to best practices and capacity-building. Access to the Global POC Directory could also be facilitated through the GSCCP. The GSCCP should evolve over time to cater to the needs of States.

[73] Third APR, para 50a).
[74] Third APR, para 50b).
[75] Third APR, para 50b).
[76] A/AC.292/2025/1.

f) States welcomed the proposal 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. States noted that such a catalogue would be a useful tool to help reduce overlapping or duplicative capacity-building efforts. Such a catalogue could be integrated with the GSCCP.[77]

g) States made further proposals for initiatives to support capacity-building, including a Digital Tool to support States' national implementation of the voluntary, non-binding norms of responsible State behaviour, including the implementation of the norms checklist, and could also be integrated into the GSCCP if agreed by States.

h) States noted the initial report prepared by the UN Secretariat outlining a proposal for the development and operationalization of a UN voluntary fund,[78] maximally leveraging on existing initiatives to support the participation of developing countries in the future permanent mechanism and the capacity-building needs of States on security in the use of ICTs without duplicating the remit of existing funds.

i) States continued to highlight that the High-level Global Roundtable on ICT security capacity-building in the context of international security, first convened on 10 May 2024 in New York, 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 security capacity-building in the context of international security with representation of high-level government officials or relevant governmental and non-governmental experts could continue to be convened on a regular basis[79] under the auspices of the future permanent mechanism.

j) States recognized that the OEWG served as an inclusive platform for the exchange of 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 acknowledged that the OEWG had been a useful 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 and recognized the need to continue this work in the future permanent mechanism.

k) States, including through the future permanent mechanism, 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.[80] States recognized the diverse capacity-building needs of States and also recognized the ICT security capacity-building programmes provided by a wide range of States, and stakeholders, including businesses, non-governmental organizations and academia. States also commended the Women in International Security and Cyberspace fellowship for enabling more women to meaningfully participate in the work of the OEWG, as well as the OEWG delegates sponsorship programme for enabling more representatives to meaningfully participate in the work of the OEWG.

[77] Third APR, para 50d).
[78] A/AC.292/2025/2.
[79] Third APR, para 50e).
[80] Third APR, para 50h).

l) States reaffirmed that capacity-building is an issue that cuts across the OEWG's mandate and one that requires continued focused discussions at the future permanent mechanism, particularly given its value in raising awareness and facilitating common understandings on the framework for responsible State behaviour in the use of ICTs.

Recommendations

54. States to continue discussions on capacity-building efforts at the future permanent mechanism.

55. States to convene regular Global Roundtables, including at a high-level as appropriate, 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 Global Roundtables could include technical-level discussions between 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.

56. States to establish a dedicated Global ICT Security Cooperation and Capacity Building Portal via a step-by-step modular approach. In this regard, the Portal should first be developed to function as an online platform to support the future permanent mechanism. States also request the UN Secretariat to provide an update on the establishment and operationalization of the Portal prior to the first substantive plenary session of the future permanent mechanism.

57. States are encouraged to continue supporting programs to facilitate the participation of delegates in the work of the future permanent mechanism, including the existing delegates sponsorship program, and the Women in International Security and Cyberspace Fellowship, in the work of the future permanent mechanism.

58. States to continue discussions at the future permanent mechanism on the initial report prepared by the UN Secretariat outlining a proposal for the development and operationalization of a UN voluntary fund to support the capacity-building of States on security of and in the use of ICTs.[81]

59. States in a position to do so are encouraged 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. States are encouraged to ensure that these capacity-building programmes address the specific needs and priorities of developing countries in line with the ICT security capacity-building principles as adopted in the 2021 OEWG report and contained in the second APR.

G. Regular Institutional Dialogue

60. During the ninth, tenth and eleventh sessions as well as the dedicated intersessional meetings of the OEWG, States continued discussions on regular institutional dialogue and reaffirmed their commitment to making a seamless transition from the OEWG to the future permanent mechanism to ensure continuity in States' discussions on the important issue of ICT security in the context of international security.

[81] A/AC.292/2025/2.

61. The future permanent mechanism will be operationalized in accordance with Annex C of the third APR, as endorsed by General Assembly Resolution 79/237, laying out its guiding principles; functions and scope; structure; modalities; and decision making approach.

62. States continued discussions on additional elements, in accordance with paragraph 59 of the third APR. In this regard, States considered and proposed the adoption of the paper entitled "Additional Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security" as contained in Annex I of this report.

Recommendations

63. Further to General Assembly Resolution 79/237, States agree to the additional elements outlined in Annex I of this Report in order to ensure a smooth and seamless transition from the OEWG to the single-track future permanent mechanism.

. . . . .

Annex I: Additional Elements for the Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs

1. This paper sets out additional elements for the establishment of the United Nations Global Mechanism that is inclusive and universal in nature, on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs, following the conclusion of the work of the Open-Ended Working Group on security of and in the use of ICTs 2021-2025 (OEWG). These additional elements complement the "Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security" agreed in Annex C of the OEWG's third Annual Progress Report (A/79/214) and endorsed by the UN General Assembly in resolution A/RES/79/237.

2. The additional elements in this paper are set out in accordance with paragraph 59 of the OEWG's third APR for States "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 Global Mechanism; b) dedicated thematic groups of the Global Mechanism; and c) other elements as required".

3. The Global Mechanism would be established in accordance with Annex C of the third APR, namely the elements relating to Guiding Principles; Functions and Scope; Structure; Modalities; and Decision Making in conjunction with the additional elements set out in this Annex. These elements will collectively constitute the basis for the operationalization of the Global Mechanism and for a smooth and seamless transition.

Additional Elements on Structure, including Dedicated Thematic Groups

4. The work of the Global Mechanism will be carried out in a coherent and coordinated way. In this regard, the work of substantive plenary sessions, dedicated thematic groups, dedicated intersessional meetings, review conferences, or any other meetings convened in any format, will be mutually reinforcing and avoid duplicative discussions.

5. The work of the substantive plenary sessions will be organized in accordance with the five pillars of the framework for responsible State behaviour in the use of ICTs.

6. The work of dedicated thematic groups will aim to build on and complement the discussions in the substantive plenary sessions by providing the opportunity for more detailed and action-oriented discussions, drawing on the five pillars of the framework, in line with the agreed functions and scope of the Global Mechanism.

7. The Global Mechanism would comprise the following dedicated thematic groups:

- An **integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to address specific challenges in the sphere of ICT security in the context of international security in order to promote an open, secure, stable, accessible, peaceful, and interoperable ICT environment,** with the participation of, *inter alia*, technical experts and other stakeholders. (DTG 1)

- An **integrated, policy-oriented and cross-cutting dedicated thematic group drawing on the five pillars of the framework to accelerate ICT security capacity-building,** with the participation of, *inter alia*, capacity-building experts, practitioners, and other stakeholders. (DTG 2)

8. Meetings of each dedicated thematic group could proceed in the following manner: (a) briefings from relevant experts drawing from a pool of experts nominated by States; (b) dedicated time for focused discussions on a rotating agenda of specific issues including lessons learned and best practice, identifying capacity-building needs and facilitating partnerships in this regard; and (c) updates and draft recommendations on possible action-oriented measures. To ensure focused discussions, the Chair of the Global Mechanism would prepare guiding questions prior to each dedicated thematic group meeting, which delegations are encouraged to address.

9. The dedicated thematic groups specified above will continue their work until the first Review Conference, after which the Review Conference will take a decision on the number and scope of the dedicated thematic groups that are to be convened over the subsequent four years.

10. In order to facilitate inclusive participation, all dedicated thematic group meetings will take place in hybrid format, with in-person participation strongly encouraged. Dedicated thematic group meetings will also be broadcast on UN WebTV. In accordance with UN practice, hybrid meetings are considered informal.

11. In addition to the dedicated thematic groups specified above, the Global Mechanism could also establish additional ad-hoc dedicated thematic groups with a fixed duration to engage in focused discussions, and also convene roundtable discussions on specific topics, as necessary, in accordance with its decision making modalities as adopted in Annex C of the third APR.

12. In accordance with the agreement by States that "The dedicated thematic groups would report to the substantive plenary sessions with updates and recommendations", facilitators of the dedicated thematic group will provide updates to the Global Mechanism at its substantive plenary sessions on the work of their respective dedicated thematic group. The facilitators of the dedicated thematic groups, in consultation with States, could also transmit action-oriented draft recommendations, if any, to the Global Mechanism at its substantive plenary sessions for consideration by States, in accordance with its decision making modalities as adopted in Annex C of the third APR.

13. To ensure a seamless transition to the Global Mechanism and in line with paragraph 16 of Annex C of the third APR, the organisational session will be convened no later than March 2026.

14. The Global Mechanism would meet twice per year, with one week of dedicated thematic group meetings and one week of substantive plenary session meetings.

Additional Elements on Modalities on the Participation of Other Interested Parties and Stakeholders, including Businesses, Non-Governmental Organizations and Academia

15. The Global Mechanism would adopt the following modalities on the participation of other interested parties and stakeholders, including businesses, non-governmental organizations and academia:

a) Member States of the Global Mechanism are committed to engaging with other interested parties and stakeholders, including businesses, non-governmental organizations, and academia (henceforth "stakeholders") in a systematic, sustained, and substantive manner.

b) Relevant non-governmental organizations in consultative status with the Economic and Social Council in accordance with resolution 1996/31 would inform the Secretariat of the Global Mechanism of their interest to be accredited to participate in the substantive plenary sessions and review conferences of the Global Mechanism.

c) In accordance with UN practice, stakeholders relevant and competent to the scope and purpose of the Global Mechanism should also inform the Secretariat of their interest in participating by submitting information on the organization's purpose, programmes and activities in areas relevant to the scope of the Global Mechanism. These organizations would accordingly be accredited, on a non-objection basis, to participate in the substantive plenary sessions and review conferences of the Global Mechanism. Once received, accreditation would remain valid for the duration of each

five-year cycle of the Global Mechanism. Applications for accreditation may be submitted to the Secretariat during an annual window to be determined by the Secretariat. The annual window would be well in advance of each substantive plenary session or review conference in order to allow sufficient time for States to consider applications and to ensure timely accreditation.

d) Accredited stakeholders will be able to attend substantive plenary sessions and review conferences of the Global Mechanism, and make oral statements during dedicated stakeholder sessions. They may also be allowed to make oral statements after States, subject to the availability of time and at the discretion of the Chair, at substantive plenary sessions and review conferences.

e) Member States are encouraged to utilize the non-objection mechanism judiciously, bearing in mind the spirit of inclusivity.

f) Where there is an objection to a stakeholder, the objecting Member State will make known its objection to the Chair of the Global Mechanism and, on a voluntary basis, make known to the Chair the general basis of its objections. Guided by the principles of inclusivity and transparency, the Chair will disseminate any information received to all Member States, and engage in informal consultations, as appropriate, for a period not exceeding three months, regarding the objection expressed with a view to addressing concerns and facilitating accreditation wherever possible. Following the conclusion of the period of informal consultations, the Chair will provide an update to all Member States at the next substantive plenary session and allow for an exchange of views, if necessary.

g) On the basis of informal consultations, if there is consensus to do so, the Chair may put forward a decision to the Global Mechanism to confirm the accreditation of some or all stakeholders that had initially received objections. Where consensus is not yet attainable, the Chair will continue to engage in further informal consultations, as appropriate.

h) Stakeholders may submit written inputs to be posted on the webpage of the Global Mechanism.

i) Stakeholders are reminded that their participation in the work of the Global Mechanism, would be of a strictly consultative nature with the aim of constructively assisting and informing the work of States in view of their domain and/or technical expertise. Stakeholders would engage in a technical and objective manner, and shall provide contributions that directly relate to the specific matters at issue in the meeting where they contribute. Stakeholders shall refrain from politicizing issues and their contributions shall remain apolitical in nature. The Chair of the Global Mechanism will endeavour to ensure adherence to these guidelines.

j) Member States emphasize the importance of facilitating inclusive participation by ensuring diverse stakeholder participation, with due consideration given to equitable geographical representation, and encourage Member States and stakeholders in a position to do so to establish and support sponsorship programmes to facilitate stakeholder participation from developing countries.

k) The Chair of the Global Mechanism will organize informal and/or virtual consultative meetings with all interested stakeholders during the inter-sessional period, building on the practice of the previous OEWG.

l) The Global Mechanism is an inter-governmental process in which negotiation and decision making are exclusive prerogatives of Member States.

m) The modalities for this Global Mechanism shall in no way create a precedent for any other UN process.

. . . . .