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.

As stated in my letter dated 29 May 2024, the eighth substantive session of the OEWG will be held at United Nations Headquarters in New York from 8 to 12 July 2024. The provisional programme of work for the eighth substantive session, structured in line with the agenda adopted at our organizational session (A/AC.292/2021/1) and the mandate contained in General Assembly resolution 75/240, is enclosed. I have allocated time for two readings of the draft of the third Annual Progress Report (APR) of the OEWG in the meeting time available to us. I also anticipate that additional informal meetings and informal-informal meetings may also be required in order to find consensus, and I will convene such meetings if and when necessary in the course of our discussions.

In this regard, I would like to take this opportunity to once again thank delegations for their constructive participation in the virtual open-ended informal “town-hall” meeting on 10 June 2024 to discuss the Zero Draft of the third APR, and for the various comments and inputs submitted to me.

Having carefully reviewed and considered the points raised by delegations at the “town-hall” meeting, I am pleased to enclose a revised (Rev. 1) draft of the third APR for delegations’ consideration ahead of the eighth substantive session. In preparing the Rev. 1 draft, I have endeavoured to reflect as far as possible the various suggestions, ideas and proposals put forward by delegations, while continuing to keep in mind our imperative to work towards the formulation
of a balanced text acceptable to all delegations and capable of commanding consensus.

I would like to remind delegations that it is an inherent characteristic of a consensus process at the UN that we will not be able to fully satisfy and reflect the preferences held by each and every delegation. I call on delegations to continue building on the same spirit of moderation, compromise, and constructive cooperation that characterised our discussions leading up to the successful consensus adoption of the first and second APRs. In this regard, I hope delegations will approach our discussions at the eighth substantive session not only from the perspective of your delegation’s preferences, but also from the perspective of how we can formulate proposals that could ultimately command consensus amongst all delegations, and in this regard exercise restraint in proposing changes to the Rev. 1 draft.

Finally, I would like to invite all Heads of Delegations plus accompanying experts to an in-person cocktail reception on Monday, 8 July 2024 at 6.30pm at the Permanent Mission of Singapore. The cocktail reception invitation is enclosed.

I look forward to working closely with all delegations to reach consensus at the eighth substantive session on a meaningful and substantive third APR, in accordance with our mandate as established in General Assembly resolution 75/240.

Please accept, Excellency, the assurances of my highest consideration.
Burhan Gafoor
Chair
Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025

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

Enclosure:

- Annex A – Provisional programme of work for the eighth substantive session of the OEWG
- Annex B – Invitation to an in-person cocktail reception at the Singapore Mission on Monday 8 July 2024 at 6.30pm
- Annex C – Rev. 1 draft of the third Annual Progress Report of the OEWG
Open-ended working group on security of and in the use of information and communications technologies 2021–2025
Eighth substantive session
New York, 8-12 July 2024

Provisional programme of work

Note by the Secretariat

1. The eighth substantive session of the open-ended working group on security of and in the use of information and communications technologies 2021–2025, established pursuant to General Assembly resolution 75/240, will be held at Headquarters from 8 to 12 July 2024.

2. The provisional programme of work is contained in the annex to the present note. The annotated agenda for the session, as adopted at the organizational meeting, on 1 June 2022, is contained in document A/AC.292/2021/1.

3. Additional information can be found at https://meetings.unoda.org/open-ended-working-group-on-information-and-communication-technologies-2021.
Annex

Provisional programme of work

Monday, 8 July

10 a.m.–1 p.m.  Opening of the session

Opening statements

– Under-Secretary-General and High Representative for Disarmament Affairs, Ms. Izumi Nakamitsu (pre-recorded)

– H.E. Ambassador Burhan Gafoor, Chair of the Open-ended working group on security of and in the use of information and communications technologies 2021–2025

Agenda item 3: organization of work

Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240

Chair’s presentation of draft third annual progress report

3–6 p.m.  Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)

First reading of, and negotiations on, draft third annual progress report

Tuesday, 9 July

10 a.m.–1 p.m.  Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)

First reading of, and negotiations on, draft third annual progress report (continued)

3–6 p.m.  Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)

First reading of, and negotiations on, draft third annual progress report (continued)

Wednesday, 10 July

10 a.m.–1 p.m.  Dedicated stakeholder session (in accordance with agreed modalities for the participation of stakeholders of 22 April 2022)

Interactive session with States and stakeholders

3–6 p.m.  Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)

Second reading of, and negotiations on, draft third annual progress report
Thursday, 11 July

10 a.m.–1 p.m.  
Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)  
Second reading of, and negotiations on, draft third annual progress report (continued)

3–6 p.m.  
Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)  
Second reading of, and negotiations on, draft third annual progress report (continued)

Friday, 12 July

10 a.m.–1 p.m.  
Agenda item 5: discussions on substantive issues contained in paragraph 1 of General Assembly resolution 75/240 (continued)  
Second reading of, and negotiations on, draft third annual progress report (continued)

3–6 p.m.  
Agenda item 7: adoption of annual progress reports  
Adoption of third annual progress report

Agenda item 6: other matters

Closure of the session

Concluding remarks by the Chair of the open-ended working group
INVIATION

On the occasion of the eighth substantive session of the Open-Ended Working Group (OEWG) on security of and in the use of information and communications technologies 2021-2025

H.E. Ambassador Burhan Gafoor,
Chair of the OEWG and
Permanent Representative of Singapore to the United Nations,

has the honour to invite the

Head of Delegation
plus one accompanying expert

to a Reception on

Monday, 8 July 2024, at 6.30 pm
at the
Permanent Mission of Singapore to the United Nations
318 East 48th Street
New York, NY 10017
(between 1st and 2nd Avenues)

To confirm your participation, please RSVP at https://forms.gle/MKiDUNqPbUNiiQJ97
THIRD ANNUAL PROGRESS REPORT OF THE OPEN-ENDED WORKING GROUP ON SECURITY OF AND IN THE USE OF INFORMATION AND COMMUNICATIONS TECHNOLOGIES 2021–2025, SUBMITTED TO THE 79TH SESSION OF THE GENERAL ASSEMBLY PURSUANT TO GENERAL ASSEMBLY RESOLUTION 75/240

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

---

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.
cumulative and evolving framework\textsuperscript{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, \textit{inter alia}, data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the General Assembly at its eightieth session.” In this regard, the OEWG acknowledged the importance of addressing its mandate in a balanced manner and the need to give due attention to both further develop common understandings between States on security in the use of ICTs, as well as to further the implementation of existing commitments.

5. As discussions at the OEWG continue to deepen, States increasingly recognized the integrated, connected and cross-cutting nature of all the issues addressed under the OEWG. For example, in order to address existing and potential ICT-related threats to international security, it was emphasized that it was fundamental for all States to observe and actively implement the framework for responsible State behaviour in the use of ICTs. It was further emphasized that international law and voluntary, non-binding norms of responsible State behaviour are complementary and mutually-reinforcing, and that the adherence of States to international law, their observation and implementation of voluntary, non-binding norms and their cooperation in ICT security capacity-building act as important confidence-building measures, enhancing trust between States and strengthening dialogue between them. In this regard, States emphasized that an integrated, cross-cutting and mutually-reinforcing approach was crucial for strengthening the framework for responsible State behaviour in the use of ICTs and advancing the work of the OEWG.

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

\textsuperscript{7} Report of the 2021 GGE, A/76/135, para 2, consensus GA resolution 76/19.
accelerating the digital transformation of States and their implementation of the sustainable development goals. 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 and peaceful ICT environment. Given the rapid pace of developments in the digital landscape, capacity-building efforts need to be accelerated to ensure that all States can safely and securely seize the benefits of digital technologies.

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.

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.

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 of the Group is not intended to be a comprehensive summary of discussions by States, but aims to capture concrete progress made at the OEWG to date, building also on the roadmap for discussion contained within the first and second APRs. This third APR will be submitted to the General Assembly pursuant to the OEWG’s mandate contained in resolution 75/240.

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.8

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 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.9

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.10 At the same time, States highlighted the need to secure ICT-related CI such as 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.

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

17. States noted a worrying increase in States’ malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.11 States expressed particular concern regarding malicious ICT activities that are aimed at interfering in the internal affairs of States.12

---
9 Second APR, para 12.
11 Second APR, para 14.
12 Second APR, para 13.
18. 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.  

19. 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 undertaken 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. States further highlighted with concern that the increasing frequency, scale and severity of ransomware attacks can have a disruptive impact on individuals, economies and societies at large, and may have an impact on international peace and security. Such attacks should be tackled by their source, means of dissemination and methods of monetization. States also highlighted with concern rising cryptocurrency theft and financing of malicious ICT activity using cryptocurrency which could potentially impact international peace and security.

20. States noted that the growing market for commercially-available ICT intrusion capabilities and their ready availability to State and non-State actors could have implications for ICT security. States also noted that the growth of this market was increasing the opportunity for the irresponsible and potentially malicious use of ICT intrusion capabilities, and making it more difficult to mitigate and defend against the threats they pose. There were concerns that the irresponsible or potentially malicious use and proliferation of ICT intrusion capabilities by State and non-State actors could contribute to unintentional escalation and threaten international peace and security.

21. States noted that new and emerging technologies are expanding development opportunities. However, 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. Risks could also be exacerbated through the combinatory use of new technologies.

22. States expressed particular concern regarding the security of artificial intelligence systems as well as the data used for training machine learning and artificial intelligence models as used in the context of ICT security. Furthermore, States also highlighted that artificial intelligence could be harnessed to enhance the speed and accuracy of ICT operations and to enable autonomous ICT attacks over which the initiators may not have full control. Such operations increase the risk of cascading effects that may cause unintended harm, including to individuals and critical infrastructure. They could also lead to misperceptions and unintended escalation between States. In this regard, States underscored that there was a need to better understand the risks associated with new and emerging ICT systems, including artificial intelligence, and to implement and strengthen security-by-design approaches throughout the life cycle of these technologies, so as to

---

13 Second APR, para 15.
fully seize the opportunities presented by such systems. States also stressed that it is in the interest of all States to promote the use of new and emerging technologies for peaceful purposes.

23. 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.\(^\text{15}\)

24. 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.

25. 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 sustainable development goals, while respecting the national needs and priorities of States.\(^\text{16}\)

26. 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.\(^\text{17}\)

27. 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 or respond to malicious ICT activities may make them more vulnerable.\(^\text{18}\) 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\(^\text{19}\) and capacity-building initiatives under the cumulative and evolving framework for responsible State behaviour.\(^\text{20}\)

Recommended next steps

28. States 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 27 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

\(^{15}\) Second APR, para 17.
\(^{16}\) Second APR, para 18.
\(^{17}\) Second APR, para 19.
\(^{20}\) Second APR, para 20.
remains fundamental to addressing existing and potential ICT-related threats to international security.

29. 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 malicious ICT activities. 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

30. 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) States recalled that the mandate of the OEWG contained in General Assembly resolution 75/240, inter alia, “to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour;”21 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.22

b) Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. States stressed that such norms reflect the expectations and standards of the international community regarding the behaviour of States in their use of ICTs and allow the international community to assess the activities of States.23

c) States welcomed the 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 proposed that the checklist could be a voluntary capacity-building tool which States may wish to use as part of their efforts to implement the voluntary, non-binding norms of

---

21 General Assembly resolution 75/240, operative paragraph 1, Second APR, para 23a).
responsible State behaviour in the use of ICTs, as well as for developing a baseline of capacities needed by States to build resilience in terms of ICT security. At the same time, States recognized that there is no one-size-fits all solution to implementation. In this regard, 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. States suggested that the checklist may be viewed as a living document which could be updated periodically per the agreement of States. States also noted that there were other available resources which could assist States in the implementation of agreed rules, norms and principles.

d) States underlined the importance of the protection of Critical Infrastructure (CI) and Critical Information Infrastructure (CII). States highlighted that ICT activity that intentionally damages CI or CII or otherwise impairs the use and operation of CI or CII to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population and can be escalatory.24

e) 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 classification of CI and CII, comprehensive risk assessments, ICT awareness and training, as well as adherence to relevant national regulatory requirements and guidelines. 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 CI and CII operators need to be provided with support in this regard.

f) 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.25

g) In the context of taking steps to ensure the integrity of the supply chain, States also emphasized that security-by-design should be embedded in the development and manufacture of ICT products and that prioritizing the integration of product security over speed to market should be encouraged. It was also suggested that fostering transparency in the development of each of

24 Report of the 2021 GGE, A/76/135, para 42, consensus GA resolution 76/19; Second APR para 23c).
25 Second APR, para 23d).
the components of ICT products could enhance the trust of end users and facilitate the swift identification of any vulnerabilities.

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.26

i) In the report of the 2021 OEWG, States concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.27 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 Report28) further to the recommendation contained in the 2021 OEWG report.29 States further proposed that the current OEWG could continue its discussion on the need to develop additional norms and proposed that States, as well as interested stakeholders, could, on a voluntary basis, submit working papers on potential additional norms.

j) In the context of the evolving nature of ICTs, States had an in-depth discussion on the need to further develop the rules, norms and principles of responsible behavior of states in the use of ICTs. In this regard, several proposals were put forward for potential new norms which are still being discussed by States.

Recommended next steps

31. States continue exchanging views at the OEWG on rules, norms and principles of responsible State behaviour in the use of ICTs, taking into account sub-paragraphs 30a) to 30j) above, at the forthcoming substantive sessions of the OEWG.

32. States agree that the Checklist of Practical Actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs (Annex A) is 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 and which

---

26 Second APR, para 23e).
interested States may also use as a tool for strengthening the capacity of developing and small States. Interested States and regional organizations are invited to submit to the UN Secretariat any additional materials which States could use along with the Checklist to assist their implementation of rules, norms and principles. The UN Secretariat is requested to make these additional materials available on the OEWG website.

33. States, as well as interested stakeholders, could, on a voluntary basis, submit working papers on proposals for the development of additional norms of responsible State behaviour in the use of ICTs or update proposals appended to the annex to the Chair’s Summary in the 2021 OEWG Report.30

D. International Law

34. 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.31

35. 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 paragraphs32:

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-interference 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:

30 Report of the 2021 OEWG, A/75/816, Annex II.
31 Second APR, para 28.
32 Second APR, para 29a) and 29b).
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.”;  

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.”

36. 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. Additionally, State sovereignty applies 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.

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” 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”. Additionally, States highlighted that the Global Points of Contact Directory could be useful as a potential avenue to facilitate dialogue between States for the settlement of disputes by peaceful means.

---

35 Second APR, para 30a.
37 Article 2(3) of the Charter of the United Nations.
38 Article 33(1) of the Charter of the United Nations.
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.\(^{39}\)

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, especially the principle of State sovereignty or the prohibition on intervention in the internal or external affairs of States.

f) Highlighted the obligations of States regarding the protection of civilians under international law.

g) Highlighted the obligations of States regarding the protection of critical infrastructure and critical information infrastructure under international law.

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

a) States welcomed 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 an additional intersessional meeting could be convened to build on this momentum. States also proposed that these discussions could continue to benefit from briefings from experts, including experts from the International Law Commission, with due consideration given to equitable geographical representation and national contexts.

b) States, reaffirming that international law applies in the use of ICTs, additionally 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. Discussions may include issues such as, \textit{inter alia}, on how the transborder nature and anonymity of some ICT operations can be addressed under international law.

c) States further noted that sharing national as well as regional 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

\(^{39}\) Report of the 2021 GGE, A/76/135, para 71(c), consensus GA resolution 76/19.
of international legal experts may also assist States in developing such common understandings.40

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 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 should be undertaken in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.41

e) States welcomed the scenario-based exercises undertaken by academic and research institutions as a useful avenue for capacity-building in the area of international law and for the development of common understandings on how international law applies in the use of ICTs. In this regard, States proposed that interested States could continue to support such further efforts.

f) 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.42

Recommended next steps

38. States continue to engage in focused discussions at the OEWG on how international law applies in the use of ICTs drawing from topics from the non-exhaustive list in paragraphs 35 to 37 above as well as proposals on the topic of international law contained in the 2021 OEWG report and Chair’s summary, where relevant.

39. Building on discussions at the sixth, seventh and eighth sessions of the OEWG, States are invited to continue to voluntarily share their national as well as regional 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. States in a position to do so, together with relevant UN entities and stakeholder partners, are encouraged to, where requested, continue supporting States in preparing their national positions on how international law applies in the use of ICTs.

40 Second APR, para 31b).
41 Second APR, para 31c).
42 Second APR, para 32.
40. 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. Such capacity-building efforts should be undertaken in accordance with the capacity-building principles contained in paragraph 56 of the 2021 OEWG report.

41. Interested States are encouraged to support the organization of scenario-based exercises by academic and research institutions, including in New York, as a useful additional avenue of capacity-building and for developing common understandings in the area of international law that can implement and support the role of the United Nations in this regard.

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 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 highlighted that the POC directory could facilitate secure and direct communications between the competent authorities of States including in the event of an urgent or significant ICT incident, to help prevent and address serious ICT incidents, help reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents. The POC directory would also be a valuable tool for taking forward CBMs in general. States proposed in particular that the POC directory could be an inclusive platform to accelerate CBM implementation through information sharing, the conducting of simulation exercises at the global level and facilitating consultations between States. It was emphasized that regular information sharing through the POC directory should be established as soon as possible.

c) States highlighted that a step-by-step approach could be taken to improve and enhance the functioning of the POC directory. 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 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 POC directory, standardized templates could be developed. In particular, standardized templates could be developed to ensure 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 POC directory particularly in urgent situations.

e) In addition to the already agreed 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 for further consideration within the OEWG.

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

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. Furthermore, States also highlighted that OEWG could be a platform for the innovative exercising of CBMs.

Recommended next steps

43. States 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 further discuss and engage in the operationalization and utilization of the global POC directory at the forthcoming substantive sessions of the OEWG. As a priority, all UN Member States who have not already done so are encouraged to nominate national POCs to the 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 to optimize communication through the POC directory including through the development of standardized templates. In this regard, the UN Secretariat, drawing from

---

43 Second APR, para 37f).
44 Second APR, para 37g).
examples from regional organizations where appropriate, is requested to develop an example of such a template no later than the end of March 2025 for use by States at their discretion.

46. Recalling the list of global CBMs contained in Annex B of the second APR,45 States agree that the CBMs as contained in Annex B of this report are additional voluntary global CBMs. 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.

47. States are encouraged, on a voluntary basis, to continue to submit national views on technical ICT terms and terminologies to enhance transparency and understanding between States. The UN Secretariat is requested to make these views available on the OEWG website for the reference of all States.

F. Capacity-Building

48. 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 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.46

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, could be enhanced by a State’s evaluation of its own current status of ICT security at the national level including through voluntary national assessments. 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

45 A/78/265.
46 Second APR, para 43a).
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, in complement with 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” tool for States, developed under the auspices of the UN. It was envisaged that the portal could be a platform for cooperation and 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. Furthermore, the portal could be harmonized with existing and related online portals.

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 agreed by States.

e) A proposal was also made for the list of voluntary, non-binding norms of responsible State behaviour in the use of ICTs to be integrated into the portal and for a tool to be developed to assist States in self-tracking the implementation of these norms.

f) 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.

g) States acknowledged the mapping exercise47 to survey the landscape of capacity-building programmes and initiatives within and outside the United Nations and at the global and regional levels as undertaken 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 including through taking stock of States’ capacity-building needs and identifying capacity-building gaps through tools and surveys and by facilitating access by States to capacity-building programmes. 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 to support the future permanent mechanism on ICT security in the context of international

---

47 A/AC.292/2024/2.
security, including through coordination with existing development programmes and relevant funding mechanisms.

h) 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 capacity-building, as well as for continuing work to develop cooperative mechanisms to address threats in the use of ICTs.

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

j) 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**

49. **States continue exchanging views at the OEWG on ICT capacity-building in the context of international security, including on sub-paragraphs 48a) to 48j) above.**

50. **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.** The portal would: a) be a practical and neutral, member State-driven and modular “one-stop shop” tool 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 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 Secretariat is requested to submit the report in March 2025.

51. **In order to ensure sustained attention to the urgent issue of ICT security capacity-building, States agree to convene future High-level Global Roundtables on ICT Security Capacity-building during the UN General Assembly High-level week 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 interested 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 Roundtable.

52. States agree in principle to establish a United Nations voluntary trust fund on security in the use of ICTs, maximally leveraging on existing initiatives, in order to, inter alia, support the participation of national representatives and experts, particularly from developing countries, at relevant meetings under the OEWG and 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 trust fund for consideration by States, with a view towards reaching agreement on these details by July 2025. In preparing this proposal, the Secretariat will 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.

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

G. Regular Institutional Dialogue

54. During the sixth, seventh and eighth sessions as well as the dedicated intersessional meetings of the OEWG, States continued discussions on regular institutional dialogue. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on regular institutional dialogue:

a) Building on the recommendations in the 2021 OEWG Report48 and in the first49 and second APRs50 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 future permanent mechanism. In this regard, States considered the paper

---

49 First APR, regular institutional dialogue section, recommended next steps, para. 2.
50 Second APR, paras 54-59.
prepared by the Chair entitled “Elements for the Open-Ended Action-Oriented Permanent Mechanism on ICT Security in the context of international security”.

Recommended next steps

55. States agree to adopt 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.

56. States agree to continue focused discussions on further elements needed to operationalize the future permanent mechanism.
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 agreed to 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.”

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 can be updated periodically per the agreement of States.

3. In general, the implementation of the voluntary, non-binding norms as a whole may require States to undertake 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.

---

51 Second annual progress report (APR) of the current OEWG, A/78/265, paragraph 26.
4. Capacity-building is key for all States to be able to undertake 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.52

52 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.53

☐ 2. Put in place or strengthen national structures and mechanisms54 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.55

☐ 4. Put in place or strengthen cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.56

☐ 5. Voluntarily survey national efforts and share national experiences on the implementation of norms.57 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.58

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.59

---

53 2021 GGE report, A/76/135, para 21, consensus GA resolution 76/19.
54 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).
55 A/76/135, para 21.
56 A/76/135, para 21.
57 A/76/135, para 21.
58 First APR of the OEWG, A/77/275, Recommended Next Steps section on Rules, Norms and Principles of Responsible State Behaviour, para 3.
59 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)
**Suggestions for additional actions**

- Consider engaging with instruments foreseen in multilateral agreements to which your State is a party that relate to cooperation in the context of ICTs, including law enforcement cooperation.\(^{60}\)

- Consider participating at the multilateral, regional and bilateral levels\(^{61}\) in inclusive and transparent processes which foster cooperation between States on the use of ICTs in the context of international security, including the OEWG on security of and in the use of information and communications technologies.

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

- Consider sharing best practices between States on measures to increase stability and security in the use of ICTs.


\(^{61}\) UNIDIR Report, Page 17.
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.62

☐ 2. In case of ICT incidents, consider all aspects in the assessment of the incident.63 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.64

☐ 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.65

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

63 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).
64 A/76/135, para 24.
65 A/76/135, para 25.
of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.\textsuperscript{66}

☐

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.\textsuperscript{67}

☐

6. All parties involved in an ICT are encouraged to consult among each other through relevant competent authorities.\textsuperscript{68}

☐

7. Put in place processes for the peaceful settlement of disputes\textsuperscript{69} 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.\textsuperscript{70}

\textit{Suggestions for additional actions}

- Consider developing policies outlining the methodology and the chain of responsibility related to the process of identifying the source of an ICT incident.\textsuperscript{71}

- 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.

\textsuperscript{65} A/76/135, para 27.
\textsuperscript{66} A/76/135, para 28.
\textsuperscript{67} A/76/135, para 23.
\textsuperscript{68} A/76/135, para 25.
\textsuperscript{69} A/76/135, para 25.
\textsuperscript{70} 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.\(^72\)

☐ 2. Establish and make use of structures and mechanisms to formulate and respond to requests for assistance in the case of an ICT incident.\(^73\)

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.\(^74\)
   - 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.\(^75\)
   - The notified State should make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed.\(^76\)

---
\(^72\) A/76/135, para 30(a).
\(^73\) 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)).
\(^74\) A/76/135, para 30(c).
\(^75\) A/76/135, para 30(c).
\(^76\) 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).
Suggestions for additional actions

- Consider elaborating national interpretations of this norm in accordance with international law.\textsuperscript{77}

- 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.

\textsuperscript{77} UNIDIR Report, Page 21.
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.\(^78\)

☐ 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.\(^79\)

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.\(^80\)

☐ 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.\(^81\)

☐ 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.\(^82\)

\(^{78}\) A/76/135, para 33.
\(^{79}\) A/76/135, para 32.
\(^{80}\) A/76/135, para 33.
\(^{81}\) A/76/135, para 35.
\(^{82}\) A/76/135, para 33.
Suggestions for additional actions

- Consider developing and strengthening ICT law enforcement capacity (for example, ICT police units) to be able to effectively address criminal and terrorist use of ICTs at the operational level.\(^{83}\)

- Consider participating in international operational, and technical networks for law enforcement (for example, INTERPOL I-24/7) and for ICT incident response teams (for example, FIRST).\(^{84}\)

- Consider entering into mutual legal assistance (MLA) agreements with other States in order to cooperate regarding the prosecution of terrorist and criminal use of ICTs.\(^{85}\)

\(^{83}\) UNIDIR Report, Page 23.
\(^{84}\) UNIDIR Report, Page 24.
\(^{85}\) The UN Office on Drugs and Crime (UNODC) has developed tools to assist States in the facilitation of mutual legal assistance agreements. See https://www.unodc.org/e4j/zh/organized-crime/module-11/key-issues/mutual-legal-assistance.html
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. Develop a national position on how international law, including international human rights law, applies to the ICT domain, taking into account relevant provisions in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and as set out in the Universal Declaration of Human Rights.\(^86\)

☐ 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.\(^87\)

☐ 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.\(^88\)

☐ 4. Engage with stakeholders which contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline.\(^89\)

Action requiring international cooperation

☐ 5. Participate in global, regional and sub-regional processes to develop and strengthen measures for ensuring the full respect for human rights, including the right to freedom of expression in the use of ICTs, in order to promote an

---

\(^{86}\) A/76/135, para 36.
\(^{87}\) A/76/135, paras 37 and 38.
\(^{88}\) A/76/135, para 40.
\(^{89}\) A/76/135, para 41.
open, secure, stable, accessible and peaceful ICT environment and to contribute to the achievement of the Sustainable Development Goals (SDGs).\textsuperscript{90}

Suggestions for additional actions

- Consider developing ICT security legislation, policies and strategies consistent with international human rights law and taking into account resolutions cited in this norm as well as other relevant General Assembly resolutions (this may include putting in place human rights regulations related to ICTs for businesses).\textsuperscript{91}

- Consider, where appropriate, engaging with relevant stakeholders with different areas of expertise regarding the respect for human rights in the use of ICTs within multilateral fora.

\textsuperscript{90} A/76/135, para 39.
\textsuperscript{91} UNIDIR report, page 25.
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.\(^92\)

☐ 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.\(^93\)

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.\(^94\)

Suggestion for additional actions

- Consider, where appropriate, cooperating with other States to determine which cross-jurisdiction infrastructures or sectors to deem critical and how to cooperate to better protect them.

---

\(^92\) A/76/135, para 44.
\(^93\) A/76/135, para 46.
\(^94\) 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.95

☐ 2. Classify ICT incidents in terms of their scale and seriousness.96

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.97

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.

95 A/76/135, para 50.
96 A/76/135, para 50.
97 A/76/135, para 49.
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.

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.

**Suggestions 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.98
• Given that CIs and CIIIs are often not owned or controlled by the government, consider the appointment of an overall coordinator for CI and CII, such as an interagency committee.99

• Consider participating in global, regional and sub-regional exchanges on best practices with regard to Critical Infrastructure (CI) and Critical Information Infrastructure (CII) protection, including the sharing of national policies, and on the recovery from ICT incidents involving CI and CII.

*^^^^^^^^^^^^^^^^^^
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.\(^{100}\)

**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.\(^{101}\)

☐ 3. Seek the services of the private sector to assist in responding to requests for assistance where appropriate.\(^{102}\)

☐ 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.\(^{103}\)

**Suggestions for additional actions**

- Consider establishing relevant policy and legislative measures at the national level to receive, process, evaluate requests for assistance and responses to such requests for mitigating malicious ICT activity aimed at CI and CII.\(^{104}\)

---

\(^{100}\) 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).

\(^{101}\) A/76/135, paras 51 and 52.

\(^{102}\) A/76/135, para 52.

\(^{103}\) A/76/135, paras 54 and 55.

\(^{104}\) UNIDIR Report, Page 30.
• 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.
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.105

☐ 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.106

☐ 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.107

☐ 4. Put in place legislative and other safeguards that enhance the protection of data and privacy.108

☐ 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.109

☐ 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,

105 A/76/135, para 57(a).
106 Second APR (A/78/265), para 23d).
107 A/76/135, para 58(a).
108 A/76/135, para 58(b).
109 A/76/135, para 58(c).
including supply chain security for ICT products, in accordance with the national laws and regulations of the countries within which they operate.\textsuperscript{110}

**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.\textsuperscript{111}

☐ 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.\textsuperscript{112}

**Suggestion for additional actions**

- Consider putting in place supply chain risk management mechanisms to identify, monitor, and reviews risks to the supply chain.\textsuperscript{113}

\textsuperscript{110} Second APR (A/78/265), para 23(e).
\textsuperscript{111} A/76/135, para 57(c).
\textsuperscript{112} Second APR (A/78/265), para 23(d).
\textsuperscript{113} UNIDIR Report, Page 32.
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. \(^{117}\)

\(^{114}\) A/76/135, para 61.
\(^{115}\) A/76/135, para 63.
\(^{116}\) A/76/135, para 61.
\(^{117}\) A/76/135, para 62.
**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.\textsuperscript{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.\textsuperscript{119}

**Suggestions for additional actions**

• Consider putting in place legal frameworks and protocols that allow for cooperation and information exchange on new vulnerabilities and available remedies between relevant stakeholders (such as governments, suppliers/vendors, security researchers, and incident response teams).\textsuperscript{120}

• Consider setting up systematic awareness campaigns (both for the general public and for the workforce of specific sectors) on the importance of patching.\textsuperscript{121}

\textsuperscript{118} A/76/135, para 62.
\textsuperscript{119} A/76/135, para 64.
\textsuperscript{120} UNIDIR Report, Pages 34-35.
\textsuperscript{121} UNIDIR Report, Page 35.
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.\(^\text{122}\)

☐ 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.\(^\text{123}\)

☐ 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.\(^\text{124}\)

☐ 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.\(^\text{125}\)

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.

\(^\text{122}\) A/76/135, para 66.
\(^\text{123}\) A/76/135, para 68.
\(^\text{124}\) A/76/135, para 68.
\(^\text{125}\) A/76/135, para 67.
international levels including through national ICT security incident management frameworks.\textsuperscript{126}

\textbf{Suggestions for additional actions}

- Consider testing crisis-management procedures and communication mechanisms, verifying the operational ability of CERTs/CSIRTs to respond under pressure, and understanding any cross-sector dependencies.\textsuperscript{127}

- Consider issuing a list of all declared CSIRT/CERTs within your State’s territory.\textsuperscript{128}

- Consider participating in multilateral CERT/CSIRT exercises to build institutional capacity to perform incident response effectively.\textsuperscript{129}

\textsuperscript{126} A/76/135, para 68.
\textsuperscript{127} ITU publication entitled “Guide to Developing a National Cybersecurity Strategy”, page 42.
\textsuperscript{128} UNIDIR Report, Page 36.
\textsuperscript{129} ITU publication entitled “Guide to Developing a National Cybersecurity Strategy”, page 42.
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, intergovernmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and sub-regional experiences where appropriate.

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

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

[2021 OEWG report, paragraph 51]

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

i) Communication checks in the form of “Ping” tests;

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

iii) Tabletop exercises to simulate practical aspects of participating in a POC directory; and

iv) Regular in-person or virtual meetings of POCs to share practical information and experiences on the operationalization and utilization of the POC directory on a voluntary basis.

v) Utilize the POC directory to establish communication between POCs, in accordance with the modalities of the POC directory.
CBM 2. Continue exchanging views and undertaking bilateral, sub-regional, regional, cross-regional and multilateral dialogue and consultations between States

a) States concluded that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs.
[2021 OEWG report, A/75/816, paragraph 43]

b) States explore mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations.
[2021 OEWG report, A/75/816, paragraph 52]

c) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.
[2021 OEWG report, paragraph 53]

d) States continued to emphasize that the OEWG itself served as a CBM.
[First APR of the OEWG, paragraph 16(e)]

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

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

b) States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate, including through the Cyber Policy Portal of the United Nations Institute for Disarmament Research.
[2021 OEWG report, paragraph 50]

c) States are encouraged to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.
[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 5]
CBM 4. **Encourage opportunities for the cooperative development and exercise of CBMs**

   a) States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.  
   **[2021 OEWG report, paragraph 49]**

   b) States continue to consider CBMs at the bilateral, regional and multilateral levels and encourage opportunities for the cooperative exercise of CBMs.  
   **[2021 OEWG report, paragraph 53]**

   c) States continue exchanging views at the OEWG on the development and implementation of CBMs, including on the potential development of additional CBMs.  
   **[First APR of the OEWG, CBM section, Recommended Next Steps, paragraph 1]**

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

**CBM 5. Cooperation and partnership between States to strengthen capacity in ICT security**
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. 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 of information and best practice on the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building.**
Exchange of information and best practice on the protection of critical infrastructure (CI) and critical information infrastructure (CII), including through related capacity-building could build trust and enhance confidence between States.
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.

1 This paper sets out elements for the establishment at the United Nations of an open-ended action-oriented 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 will build on previous consensus reports, and will further develop and operationalize an action-oriented programme to advance the cumulative and evolving framework for responsible State behaviour in the use of ICTs.

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 agree to finalize the elements of the open-ended action-oriented permanent mechanism, including as contained in this paper, by consensus within the framework of the OEWG, so as to ensure a seamless transition to the new mechanism.

Guiding Principles

3 The establishment of the open-ended action-oriented permanent mechanism will be guided by the elements agreed by consensus in the OEWG, including the common elements agreed by consensus in paragraphs 55 to 57 of the second Annual Progress Report (APR) of the OEWG and reproduced below.

4 The open-ended action-oriented 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;
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;

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.

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.

Other interested parties, including businesses, non-governmental organizations and academia could contribute to any future regular institutional dialogue, as appropriate. Their contribution would take place in accordance with modalities to be agreed by consensus within the OEWG; these modalities could be further reviewed and developed within the future mechanism.

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 open-ended action-oriented permanent mechanism.

**Functions and Scope**

The main functions of the open-ended action-oriented permanent mechanism are:

a) To further develop the cumulative and evolving framework for responsible State behaviour in the use of ICTs;

b) To advance implementation of the cumulative and evolving framework for responsible State behaviour in the use of ICTs;

c) To strengthen the capacity of all States to develop and implement the cumulative and evolving framework for responsible State behaviour in the use of ICTs.

Guided by the functions listed above, the open-ended action-oriented permanent mechanism will address, with a view to facilitating an integrated, policy-oriented and cross-cutting approach to discussions, the following issues, *inter alia*, existing and potential threats; rules, norms and principles of responsible State behaviour and the ways for their
implementation, and if necessary, to introduce changes to them or elaborate additional rules of behaviour; how international law applies in the use of ICTs, including the development of additional legally binding obligations as appropriate; confidence-building measures; and capacity-building.

10 The open-ended action-oriented permanent mechanism would work towards the advancement of mutually-beneficial cross-cutting objectives, including *inter alia*, enhancing cooperation on ICT security, increasing stability in the ICT security sphere, and fostering resilience in the context of existing and potential ICT security threats.

11 The open-ended action-oriented permanent mechanism would promote engagement and cooperation with relevant stakeholders, including business, non-governmental organizations and academia, and other international and regional organizations, within the framework of an inter-governmental process in which negotiation and decision-making are exclusive prerogatives of States.

**Structure**

12 The structure of the open-ended action-oriented permanent mechanism is as follows:

a) **Substantive Plenary Sessions:** One substantive plenary session to be convened per year, with each session lasting for one week. Substantive plenary sessions would carry out discussions in accordance with the scope and functions set out above, as well as consider the work and recommendations of the dedicated thematic groups. The substantive plenary sessions will consider and adopt Progress Reports to be submitted to the First Committee on a biennial basis.

b) **Dedicated Thematic Groups:** Dedicated thematic groups to be convened to conduct focused discussions. The dedicated thematic groups would report to the substantive plenary sessions with updates and recommendations.

c) **Dedicated Intersessional Meetings:** The Chair of the open-ended action-oriented permanent mechanism could also convene dedicated intersessional meetings to engage in additional discussions on specific issues as necessary.

d) **Dedicated Stakeholder Consultations:** A dedicated stakeholder consultation of at least one day in length to be convened prior to each substantive plenary session, open to all interested parties, including States, regional organizations, businesses, non-governmental organizations and academia.

e) **Review Conference:** A Review Conference to be convened every four years to review the effective functioning of the open-ended action-oriented 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 for the open-ended action-oriented permanent mechanism contained in this document could also be decided by States on the basis of consensus.

13 The open-ended action-oriented permanent mechanism will be led by a Chair elected to serve for a period of two years on the basis of equitable geographical rotation. The dedicated thematic groups will be led by Vice-Chairs elected to serve for a period of two-years on the basis of equitable geographic representation.

14 The open-ended action-oriented permanent mechanism will establish the following dedicated thematic groups with a view to facilitating an integrated, policy-oriented and cross-cutting approach to discussions:

a) A dedicated thematic group on international law, with the participation of legal advisors and experts, in order to advance an in-depth study and understanding of how international law applies to the use of ICTs, including the development of additional legally binding obligations, as appropriate.

b) A dedicated thematic group on Confidence-Building Measures (CBMs) to support the further development and operationalization of the voluntary Global CBMs, as well as the Global POC Directory, and to ensure the active participation of technical experts and national POCs.

c) A dedicated thematic group on capacity-building to facilitate the active participation of capacity-building practitioners and to provide a platform for States and stakeholders to work together on capacity-building initiatives, including, inter alia, by convening the Global Roundtable on ICT security capacity-building on a regular basis, and exploring “additional avenues of funding specifically targeted at capacity-building related to ICT security including through potential coordination and integration with existing development programmes and funds”.¹

d) A dedicated thematic group to facilitate a cross-cutting approach to ICT security, including developing recommendations, policy guidance and best practices on priority challenges such as the protection of critical infrastructure; facilitating cooperation between States following a serious cyber incident; and improving States’ ability to deter and mitigate ICT threats and identifying capacity-building measures that would best support the recommended actions. Through a cross-cutting approach to ICT security, this group would address the implementation and development of the voluntary non-binding norms of responsible State behaviour, application of international law, and the use of confidence building measures and appropriate capacity-building measures to support the policy goal

¹ Second Annual Progress Report of the OEWG, A/78/265, para 43e).
of achieving an open, secure, stable, accessible, peaceful and interoperable ICT environment.

15 In addition to the dedicated thematic groups specified above, the Chair of the open-ended action-oriented permanent mechanism could also convene additional dedicated thematic groups with a fixed duration, to be led by facilitators appointed by the Chair, to engage in focused discussions on specific issues as necessary.

16 Recommendations and updates by the dedicated thematic groups would be provided to the open-ended action-oriented permanent mechanism at its substantive plenary sessions for consideration by States.

17 To facilitate inclusive participation, meetings of the open-ended action-oriented permanent mechanism, including the substantive plenary sessions, dedicated intersessional meetings, and meetings of any dedicated thematic groups, should not be held in parallel.

**Modalities**

18 The open-ended action-oriented 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, including its dedicated thematic groups.

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

19 To ensure a seamless transition from the work of the OEWG to the open-ended action-oriented permanent mechanism, the first substantive plenary session of the new mechanism will be convened no later than June 2026. In this regard, States agree to the following arrangements:

a) An organizational session to be convened in December 2025 to carry out, *inter alia*, (a) the election of officers, and (b) the adoption of the agenda.

b) The first substantive plenary session to be convened in March 2026.
Decision Making

20 The open-ended action-oriented permanent mechanism will take all decisions on the basis of consensus. 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 agreed upon by the open-ended action-oriented permanent mechanism.