



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

20 February 2024

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.

Further to my letter dated 29 January 2024 on the arrangements for the seventh substantive session of the OEWG which will be held from 4 to 8 March 2024 at United Nations Headquarters (UNHQ) in New York, I am pleased to circulate a revised **non-exhaustive list of guiding questions** to assist delegations in their preparations for the seventh substantive session. These guiding questions build on the previous guiding questions issued on 22 November 2023 ahead of the sixth substantive session, with new questions added to reflect the development of our discussions since then. I wish to emphasize that the guiding questions are not exhaustive and prepared under my own responsibility as a tool to facilitate our discussions. As always, I encourage delegations to come prepared to address these questions, and also raise other relevant questions and views that you deem important in advancing the work of the OEWG.

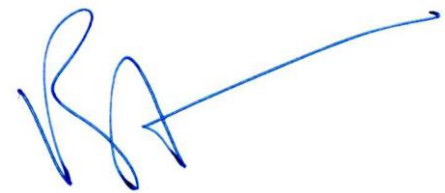
In accordance with the decision in the second Annual Progress Report (APR) for the Chair to produce an “initial draft” of a checklist on the implementation of norms “for consideration by States”, I have prepared, under my own responsibility, a **Chair’s discussion paper on a checklist of practical actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs**. This paper is attached for discussion and consideration by member States. I have structured the checklist as a non-exhaustive **compilation of voluntary, practical and actionable measures** gathered from various relevant sources, with the aim of creating a useful reference tool for States in their efforts to implement the voluntary, non-binding norms of responsible State

behavior. In this regard, I **welcome suggestions for additional measures** which could be included in this checklist, while encouraging delegations to **refrain from re-opening previous agreements**. Given the technical nature of the checklist, **interested States in a position to do so may wish to consider working together in cross-regional group(s)** to put forward suggestions on further developing and refining part or all of the initial draft checklist.

I am also pleased to enclose a **Chair's discussion paper on draft elements for the permanent mechanism on ICT security in the context of international security**. The discussion paper draws on delegations' proposals for the permanent mechanism and the discussions at the sixth substantive session and aims to serve as a tool to facilitate further focused discussion on the issue of regular institutional dialogue. It is my hope that the discussion paper will help to facilitate focused discussions and support our efforts to **build on and expand the common elements agreed in paragraph 55 of the second APR**, and in this way help us find a path forward towards consensus on this issue.

I look forward to the continued active and constructive participation of your delegations in the forthcoming seventh substantive session with the aim of advancing our work in accordance with the mandate contained 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

Enclosures:

- Annex A – Revised Non-exhaustive List of Guiding Questions
- Annex B – Chair’s discussion paper on a checklist of practical actions for the implementation of voluntary, non-binding norms of responsible State behaviour in the use of ICTs
- Annex C – Chair’s discussion paper on draft elements for the permanent mechanism on ICT security in the context of international security

**REVISED NON-EXHAUSTIVE LIST OF GUIDING QUESTIONS:
OEWG SEVENTH SUBSTANTIVE SESSION
4 TO 8 MARCH 2024**

Note: This set of guiding questions builds on the guiding questions issued on 22 November 2023 ahead of the sixth substantive session of the OEWG. New guiding questions are indicated in *italics*.

Existing and Potential Threats

- Are there any new developments or trends in existing and potential ICT threats which the OEWG should discuss in-depth?
 - *At recent sessions of the OEWG, some delegations highlighted that recent developments in artificial intelligence and other emerging technologies could possibly have implications for ICT security. What potential threats, if any, should the OEWG study further in this area?*
 - *At recent sessions of the OEWG, some delegations highlighted that the proliferation and ready availability of sophisticated commercial and/or open-source ICT capabilities to non-State and private actors could possibly have implications for ICT security. What potential threats, if any, should the OEWG study further in this area?*
- In the Second APR, States underscored the urgency of raising awareness and deepening understanding of existing and potential threats, and of further developing and implementing cooperative measures to tackle these threats. What are some potential initiatives that can be undertaken at the global level toward this objective?

Rules, Norms and Principles

- Taking into account discussions that have taken place within the OEWG so far as well as the non-exhaustive list of proposals annexed to the Chair's Summary in the 2021 OEWG Final Report, and given some national views that additional norms could continue to be developed over time, what are some possible examples of such additional norms that could potentially complement existing norms?
- What are some measures or best practices that member states can undertake to protect CI and CII from ICT threats? How can developing countries and small states who are in the process of identifying national CI and CII be better supported in this area?
- What are specific ways in which states can further strengthen cooperation to ensure the integrity of the supply chain and prevent the use of harmful hidden functions? Are there existing programmes/policies that help promote the adoption of good practices by suppliers and vendors of ICT equipment and systems?
- The Second APR calls on "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". What would such additional guidance, including a checklist, look like?
 - *Delegations are invited to share views on the Chair's Discussion Paper on a Checklist of Practical Actions for the Implementation of Voluntary, Non-binding Norms of Responsible State Behaviour in the use of ICTs dated 20 February 2024.*
- Are there any specific areas in which the implementation of the agreed norms is currently lacking, or where existing implementation efforts can be improved? If so, how can these be addressed?
 - *How can additional guidance, including a checklist, on the implementation of norms be leveraged to accelerate implementation efforts?*

International Law

- Based on discussions thus far, can we identify any further convergences in terms of States' perspectives of how international law applies in the use of ICTs with regard to the topics contained in the non-exhaustive list in subparagraphs 29(a) and (b) in the Second APR, as well as proposals contained in the 2021 OEWG report and Chair's summary, where relevant?
- Are there unique features relating to the use of ICTs that require a distinction in terms of how international law applies as compared to other domains?
- Do gaps exist in how international law applies to the use of ICTs, and if so, what can be done to bridge those gaps?
- Para 36 of the Second APR calls on "States in a position to do so to support, in a neutral and objective manner, additional efforts, including within the United Nations, to build capacity in the areas of international law". What specific capacities are most urgently required in this area and are there existing initiatives or capacity building programmes targeted at addressing these specific capacities?
- *At recent sessions of the OEWG, some delegations suggested that scenario-based discussions could provide a productive means of facilitating deeper discussions on international law.*
 - *How could scenario-based discussions possibly be carried out within the framework of the OEWG?*
 - *How could the OEWG work with and build upon existing initiatives in this regard (e.g. the UNIDIR workshop "Application of International Law to the Behaviour of States in the Use of ICTs – Challenges and Opportunities")?*
 - *What are some examples of scenarios that could be used as part of such discussions?*

Confidence-Building Measures

- How can we accelerate the universal implementation of the CBMs listed in the Initial List of Voluntary Global CBMs? How can these CBMs be further operationalized, including, inter alia, through (a) related capacity-building, and (b) the global POC directory?
- Are there additional CBMs that can be added to the Initial List of Voluntary Global CBMs?
 - *Drawing on discussions at recent session of the OEWG, could some examples of such additional CBMs potentially include:*
 - *CERT to CERT cooperation;*
 - *Cooperation between States on capacity building to close the digital divide;*
 - *Protection of critical infrastructure;*
 - *Public-private sector cooperation; and*
 - *Coordinated vulnerability disclosure?*
- Paras 14(a) to (d) of Annex A of the Second APR suggests topics of discussion for further work by States on the POC directory. What proposals, suggestions and ideas do States have in relation to these possible areas of future work?

Capacity-building

- What are some of the foundational capacities required for States to detect, defend against or respond to malicious ICT activities, and also for them to utilize effectively existing mechanisms such as CERT-CERT channels for this purpose?
 - *Are there existing studies of foundational capacities that the OEWG could study and build upon?*

- *How could the identification of foundational capacities be used to support “demand-driven”¹ capacity building?*
- The Second APR calls on States to continue to discuss the proposal for a Global Cyber Security Cooperation Portal (GCSCP) as a “one-stop shop” tool for States, developed under the auspices of the UN, and that further discussions could take place on how to synergize this portal with other existing portals as appropriate. What would such a portal look like in practice?
 - *At recent sessions of the OEWG, some delegations highlighted possible modules that could be incorporated over time into such a portal. What views do delegations have on these suggested modules? Are there any other possible modules that delegations wish to highlight?*
- The Second APR encourages States to develop and share voluntary checklists and other tools to assist States in mainstreaming the capacity-building principles contained in Annex C of the Second APR. What would such checklists and tools look like?
- The Second APR encourages States to develop and share tools that would assist States in incorporating a gender perspective into capacity-building efforts. What would such tools look like?
- What additional role, can the United Nations perform in the provision, coordination, or facilitation of capacity-building efforts, in a manner that complements existing initiatives?

Regular Institutional Dialogue

- Recalling the list of common elements for a future mechanism for regular institutional dialogue agreed in the Second APR, what additional consensus elements can be added to this list?
- Taking into account latest developments on the Programme of Action as well as ongoing discussions on other proposals made related to regular

¹ Second Annual Progress Report of the OEWG 2021-2025, Annex C, Agreed principles of capacity-building, Partnerships: “Capacity-building should be based on mutual trust, demand driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.”

institutional dialogue, how can we align different synergies and best develop a future mechanism for ICT security?

- *Delegations are invited to share views on the Chair's Discussion Paper on Draft Elements for the Permanent Mechanism on ICT Security in the context of international security dated 20 February 2024.*

.

**Chair's Discussion Paper on a Checklist of Practical Actions
for the implementation of voluntary, non-binding norms of
responsible State behaviour in the use of ICTs
[Initial Draft]**

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."¹

2 This checklist is a compilation of voluntary, practical and actionable measures gathered from various relevant sources. It is intended as a voluntary 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. In this regard, this checklist could (a) serve as a starting point to support States' implementation efforts, (b) provide a useful means of identifying priorities in tailored capacity-building efforts, and (c) function as a common reference to support the exchange of best practice in specific areas of ICT security.

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 would include the establishment of Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) and other national coordination structures and mechanisms, as well as 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 would include participation in international and regional ICT processes, engaging in the exchange of information and best practice on different aspects of ICT security, and offering and requesting assistance where relevant. 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.

4 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.²

¹ Second annual progress report (APR) of the current OEWG, A/78/265, paragraph 26.

² 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.³
- ☐ 2. Put in place or strengthen mechanisms⁴ to detect, defend against or respond to, and recover from ICT incidents, which may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).⁵
- ☐ 3. Put in place or strengthen whole-of-government cooperative and partnership arrangements and policies to support or facilitate international cooperation.⁶
- ☐ 4. Put in place or strengthen cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community.⁷
- ☐ 5. Voluntarily survey national efforts and share national experiences on the implementation of norms.⁸
- ☐ 6. Engage 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.⁹

³ 2021 GGE report, A/76/135, para 21, consensus GA resolution 76/19.

⁴ A/76/135, para 21.

⁵ UNIDIR Report on “Unpacking Cyber Capacity-Building Needs: Part 1. Mapping the Foundational Cyber Capabilities”, Page 16.

⁶ A/76/135, para 21.

⁷ A/76/135, para 21.

⁸ A/76/135, para 21.

⁹ UNIDIR Report, Page 17.

Actions requiring international cooperation

- ☐ 7. Participate at the multilateral, regional and bilateral levels¹⁰ 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.
- ☐ 8. Participate in inclusive and transparent mechanisms such as the Global Points of Contact Directory to foster cooperation and information sharing.
- ☐ 9. 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.¹¹
- ☐ 10. Share best practice between States on measures to increase stability and security in the use of ICTs.

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *How can inclusive, active and sustainable participation in international processes such as the OEWG continue to be further strengthened and expanded (e.g. through fellowship programmes)?*
- *What other steps can States take to further cooperate in developing and applying measures to increase stability and security in the use of ICTs?*
- *What are examples of the relevant national policies, legislation and mechanisms that would support the implementation of this norm?*

^^*^*^*^*^*^*^*^*^*

¹⁰ UNIDIR Report, Page 17.

¹¹ Acknowledging that not all States are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to its work. (First and Second APR of the OEWG (A/77/275, para 5 and A/78/265 para 7 respectively)

Norm b

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

Voluntary, practical actions for implementing this norm

Actions at the national level

- ☐ 1. Put in place or strengthen mechanisms to detect, defend against or respond to, and recover from ICT incidents, which may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).

- ☐ 2. 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.¹²

- ☐ 3. In case of ICT incidents, consider all aspects in the assessment of the incident.¹³ 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.¹⁴

- ☐ 4. 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.¹⁵

¹² A/76/135, para 26.

¹³ 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).

¹⁴ A/76/135, para 24.

¹⁵ A/76/135, para 25.

Actions requiring international cooperation

- ☐ 5. Put in place cooperation between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, to strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.¹⁶
- ☐ 6. 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.¹⁷
- ☐ 7. All parties involved in an ICT are encouraged to consult among each other through relevant competent authorities.¹⁸
- ☐ 8. Put in place processes for the peaceful settlement of disputes¹⁹ 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.²⁰

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What would considering “all relevant information” entail in the context of this norm?*
- *What legal capacities would be required for the implementation of this norm?*
- *What would the requisite skills to detect, defend against or respond to, and recover from malicious ICT activities entail?*

^^*^*^*^*^*^*^*^*^*

¹⁶ A/76/135, para 27.

¹⁷ A/76/135, para 28.

¹⁸ A/76/135, para 23.

¹⁹ A/76/135, para 25.

²⁰ 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. Put in place or strengthen mechanisms to detect, defend against or respond to, and recover from ICT incidents, which may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
- ☐ 2. Elaborate national interpretations of this norm in accordance with international law.²¹
- ☐ 3. 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.²²
- ☐ 4. Establish and make use of structures and mechanisms to formulate and respond to requests for assistance in the case of an ICT incident.²³

Actions requiring international cooperation

- ☐ 5. Utilize, where appropriate, multilateral communications channels at the diplomatic and technical levels for information sharing and to seek or respond to requests for assistance in the case of an ICT incident.
- ☐ 6. In the case of an ICT incident, the following steps could be undertaken:

²¹ UNIDIR Report, Page 21.

²² A/76/135, para 30(a).

²³ 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)).

- An affected State should notify the State from which the activity is emanating.²⁴
- 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.²⁵
- The notified State should make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed.²⁶

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What mechanisms or processes are required for a State to detect if its territory is being used for an internationally wrongful act using ICTs and to respond to such an act in accordance with international law?*
- *How can the Global POC directory play a role in supporting States in the implementation of this norm?*

^^*^*^*^*^*^*^*^*

²⁴ A/76/135, para 30(c).

²⁵ A/76/135, para 30(c).

²⁶ A/76/135, para 30(c). An ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State for the incident. Additionally, notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself. (2021 GGE report, A/76/135, para 30(d) and Second APR, A/78/265, Annex A, para 10).

Norm d

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

Voluntary, practical actions for implementing this norm

Actions at the national level

- ☐ 1. Develop and strengthen 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.²⁷
- ☐ 2. 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.²⁸
- ☐ 3. 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.²⁹

Actions requiring international cooperation

- ☐ 4. 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.³⁰
- ☐ 5. Use existing processes, initiatives and legal instruments and consider additional procedures or communication channels to facilitate the exchange of information and assistance (such as mutual legal assistance agreements) for addressing criminal and terrorist use of ICTs.³¹

²⁷ UNIDIR Report, Page 23.

²⁸ A/76/135, para 33.

²⁹ A/76/135, para 32.

³⁰ A/76/135, para 33.

³¹ A/76/135, para 35; UNIDIR report, page 23.



6. Participate in international operational, and technical networks for law enforcement (for example, INTERPOL I-24/7) and for ICT incident response teams (for example, FIRST).³²

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What mechanisms, expertise or skills are required for handling the chain of custody in the ICT context at the domestic level?*
- *What multilateral mechanisms are already in place to facilitate international cooperation to address terrorist and criminal use of ICTs?*
- *As foreseen in the norm itself, are new measures required for States to cooperate to exchange information, assist each other and prosecute terrorist and criminal use of ICTs?*
- *What technologies are available to States to support the implementation of this norm?*

^^*^*^*^*^*^*^*^*^*

³² UNIDIR Report, Page 24.

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.³³
- ☐ 2. Develop 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.³⁴
- ☐ 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.³⁵
- ☐ 4. Engage with stakeholders which contribute in different ways to the protection and promotion of human rights and fundamental freedoms to support efforts for the promotion, protection and enjoyment of human rights online and to help clarify and minimize potential negative impacts of policies on people, including those in vulnerable situations.³⁶

³³ A/76/135, para 36; UNIDIR report, page 25.

³⁴ UNIDIR report, page 25.

³⁵ A/76/135, para 40.

³⁶ A/76/135, para 41; UNIDIR report, page 25.

Actions 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 open, secure, stable, accessible and peaceful ICT environment and to contribute to the achievement of the Sustainable Development Goals (SDGs).³⁷

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What are examples of national legislation encompassing respect for human rights in the use of ICTs?*
- *What other national mechanisms or processes would support the implementation of this norm?*
- *What global or regional processes already exist to address human rights, including the right to freedom of expression in the use of ICTs?*

^^*^*^*^*^*^*^*^*

³⁷ A/76/135, para 39.

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. Put in place or strengthen mechanisms to detect, defend against or respond to, and recover from ICT incidents, which may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
- ☐ 2. 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.³⁸
- ☐ 3. Put in place relevant policy³⁹ 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.⁴⁰

Actions requiring international cooperation

- ☐ 4. Participate in bilateral, regional, and multilateral frameworks for cooperation⁴¹ to enhance measures and strengthen cooperation on the protection of Critical Infrastructure.

³⁸ A/76/135, para 44.

³⁹ UNIDIR Report, Page 27.

⁴⁰ A/76/135, para 46.

⁴¹ UNIDIR Report, Page 27.

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What tools are available to assist States in assessing which national infrastructures or sectors they should deem as critical?*
- *What may relevant national policy and legislative measures to prevent ICT activity against Critical Infrastructure include?*

^^*^*^*^*^*^*^*^*^*

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. Put in place or strengthen mechanisms to detect, defend against or respond to, and recover from ICT incidents, which may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
- ☐ 2. Determine the structural, technical, organizational, legislative and regulatory measures and contingency plans necessary to protect national critical infrastructure and restore functionality if an incident occurs.⁴²
- ☐ 3. Ensure the safety and security of ICT products throughout their lifecycle.⁴³
- ☐ 4. Classify ICT incidents in terms of their scale and seriousness.⁴⁴

Actions requiring international cooperation

- ☐ 5. Participate 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.
- ☐ 6. 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.⁴⁵

⁴² UNIDIR Report, Page 28.

⁴³ A/76/135, para 50.

⁴⁴ A/76/135, para 50.

⁴⁵ A/76/135, para 49.

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

- ☐ 1. Have emergency warning networks regarding ICT vulnerabilities, threats and incidents.
- ☐ 2. Raise awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.
- ☐ 3. Examine infrastructures and identify interdependencies among them, thereby enhancing the protection of such infrastructures.
- ☐ 4. Promote partnerships among stakeholders, both public and private, to share and analyse critical infrastructure information in order to prevent, investigate and respond to damage to or attacks on such infrastructures.
- ☐ 5. Create and maintain crisis communication networks and test them to ensure that they will remain secure and stable in emergency situations.
- ☐ 6. Ensure that data availability policies take into account the need to protect critical information infrastructures.
- ☐ 7. Facilitate the tracing of attacks on critical information infrastructures and, where appropriate, the disclosure of tracing information to other States.
- ☐ 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.⁴⁶



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

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What methodologies are available that could assist States in classifying the scale and severity of an ICT incident?*
- *What steps would be needed to implement the “Elements for protecting Critical Information Infrastructure” as set out in the annex to General Assembly resolution 58/199?*

^^*^*^*^*^*^*^*^*^*^*^*

⁴⁶ 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.

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.⁴⁷ Structures may include:
 - A national centre or responsible agency or entity that leads on ICT security matters; and
 - Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).
- ☐ 2. Establish 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.⁴⁸

Actions requiring international cooperation

- ☐ 3. 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.⁴⁹
- ☐ 4. Seek the services of the private sector to assist in responding to requests for assistance where appropriate.⁵⁰
- ☐ 5. 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.⁵¹

⁴⁷ A/76/135, para 53.

⁴⁸ UNIDIR Report, Page 30.

⁴⁹ A/76/135, paras 51 and 52.

⁵⁰ A/76/135, para 52.

⁵¹ A/76/135, paras 54 and 55.

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *As with norm c, how could the Global POC directory support States in the implementation this norm?*
- *What further relevant policy and legislative measures at the national level may be required to facilitate requests for assistance and responses to such requests for mitigating malicious ICT activity aimed at critical infrastructure?*

^^*^*^*^*^*^*^*^*

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.⁵²
- ☐ 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.⁵³
- ☐ 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.⁵⁴
- ☐ 4. Put in place legislative and other safeguards that enhance the protection of data and privacy.⁵⁵
- ☐ 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.⁵⁶
- ☐ 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,

⁵² A/76/135, para 57(a).

⁵³ Second APR (A/78/265), para 23d).

⁵⁴ A/76/135, para 58(a).

⁵⁵ A/76/135, para 58(b).

⁵⁶ 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.⁵⁷

- ☐ 7. Put in place supply chain risk management mechanisms to identify, monitor, and reviews risks to the supply chain.⁵⁸

Actions requiring international cooperation

- ☐ 8. 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.⁵⁹
- ☐ 9. 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.⁶⁰

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What are the specific processes and partnerships involved in setting up a national framework or mechanism for supply chain management?*
- *What technologies are available that States could use to support the implementation of this norm?*
- *How can emerging technologies be addressed in accordance with this norm?*

^^*^*^*^*^*^*^*^*

⁵⁷ Second APR (A/78/265), para 23(e).

⁵⁸ UNIDIR Report, Page 32.

⁵⁹ A/76/135, para 57(c).

⁶⁰ Second APR (A/78/265), para 23(d).

Norm j

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

Voluntary, practical actions for implementing this norm

Actions at the national level

- ☐ 1. Put in place vulnerability disclosure policies and programmes including a coordinated vulnerability disclosure process to minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities.⁶¹
- ☐ 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.⁶²
- ☐ 3. Put 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).⁶³
- ☐ 4. Provide legal protections for researchers and penetration testers including decriminalizing and protecting ICT security researchers and ethical hackers wishing to signal vulnerabilities.⁶⁴
- ☐ 5. Put in place measures which facilitate international cooperation on the responsible reporting of ICT vulnerabilities including requests for assistance

⁶¹ A/76/135, para 61.

⁶² A/76/135, para 63.

⁶³ UNIDIR Report, Pages 34-35.

⁶⁴ A/76/135, para 62; UNIDIR report, page 34.

between countries and emergency response teams, consistent with domestic legislation.⁶⁵

- ☐ 6. Set up systematic awareness campaigns (both for the general public and for the workforce of specific sectors) on the importance of patching.⁶⁶

Actions requiring international cooperation

- ☐ 7. 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 that may pose a risk to international peace and security or human rights and fundamental freedoms.⁶⁷
- ☐ 8. 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.⁶⁸

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What are the specific processes and partnerships involved in setting up a national coordinated vulnerability disclosure programme?*
- *What further practical steps could States take to cooperate regarding the responsible reporting of ICT vulnerabilities and share associated information on available remedies?*
- *What technologies are available to States to support the implementation of this norm?*

^^*^*^*^*^*^*^*^*^*^*^*

⁶⁵ A/76/135, para 61.

⁶⁶ UNIDIR Report, Page 35.

⁶⁷ A/76/135, para 62.

⁶⁸ A/76/135, para 64.

Norm k

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

Voluntary, practical actions for implementing this norm

Actions at the national level

- ☐ 1. Consider categorizing CERTs/CSIRTs as part of national critical infrastructure.⁶⁹
- ☐ 2. Issue a list of all declared CSIRT/CERTs within your State's territory.⁷⁰
- ☐ 3. 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.⁷¹
- ☐ 4. 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.⁷²
- ☐ 5. 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.⁷³

Action requiring international cooperation

- ☐ 6. Facilitate cooperation and coordination among CERTs/CSIRTs and other relevant security and technical bodies at the national, regional and

⁶⁹ A/76/135, para 66.

⁷⁰ UNIDIR Report, Page 36.

⁷¹ A/76/135, para 68.

⁷² A/76/135, para 68.

⁷³ A/76/135, para 67.

international levels including through national ICT security incident management frameworks.⁷⁴

Guiding questions (to assist in the preparation of the next draft)

- *What other voluntary practical actions would the implementation of this norm entail?*
- *What are the specific processes and partnerships involved in setting up a national management framework for CERTS/CSIRTs?*
- *What expertise, skills and processes would a management framework for a CERT/CSIRT require?*
- *What capacities would be required to undertake the practical actions for implementing this norm?*

^^*^*^*^*^*^*^*^*^*^*^*

⁷⁴ A/76/135, para 68.

**Chair's Discussion Paper on Draft Elements
for the Permanent Mechanism on ICT Security
in the context of international security**

Introduction

1 In the second Annual Progress Report (APR) of the OEWG, States agreed by consensus to the following recommended next step: "States, at the sixth, seventh and eighth sessions of the OEWG, as well as in two dedicated intersessional meetings, to continue to engage in focused discussions within the framework of the OEWG to further discuss proposals on regular institutional dialogue, including the PoA. At these sessions, States will also engage in focused discussions, on the relationship between the PoA and the OEWG, and on the scope, content and structure of a PoA. The United Nations Secretariat is also requested to brief the OEWG at its sixth session on the report of the Secretary-General submitted to the General Assembly at its seventy-eighth session."⁴⁰¹

Guiding Principles

2 In the second APR of the OEWG, States also agreed by consensus to the following elements contained below in paragraphs 3 to 5.

3 The permanent mechanism should be based on the following common elements:

- (a) It would be a single-track, State-led, permanent mechanism under the auspices of the United Nations, reporting to the First Committee of the United Nations General Assembly;
- (b) The aim of the future mechanism would be to continue to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment;
- (c) The future mechanism would take as the foundation of its work the consensus agreements on the framework of responsible State behaviour in the use of ICTs from previous OEWG and GGE reports;
- (d) It would be an open, inclusive, transparent, sustainable and flexible process which would be able to evolve in accordance with States' needs and as well as in accordance with developments in the ICT environment.

⁴⁰ A/78/76.

¹ Second APR, A/78/265, para 58.

4 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.

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

Focused Discussions

6 As part of the OEWG Chair's efforts to facilitate focused discussions within the framework of the OEWG in accordance with the recommended next step agreed in the second APR, States will recall that the Chair had asked the following guiding questions in the non-exhaustive list of guiding questions issued on 22 November 2023 ahead of the sixth substantive session of the OEWG:

- (a) Recalling the list of common elements for a future mechanism for regular institutional dialogue agreed in the Second APR, what additional consensus elements can be added to this list?
- (b) Taking into account latest developments on the Programme of Action as well as ongoing discussions on other proposals made related to regular institutional dialogue, how can we align different synergies and best develop a future mechanism for ICT security?

7 Building on delegations' proposals and the constructive discussions at the sixth substantive session of the OEWG, the following elements are intended to serve as a tool to facilitate further focused discussion on the issue of regular institutional dialogue and complement the guiding questions above:

- (a) The permanent mechanism could fulfil the following **functions**:
 - i. To further develop the framework for responsible State behaviour;
 - ii. To advance implementation of the framework for responsible State behaviour;
 - iii. To strengthen the capacity of all States to develop and implement the framework for responsible State behaviour.
- (b) The **scope** of the permanent mechanism could cover the following topics of discussion:
 - i. [What topics should be discussed under the permanent mechanism?]

- ii. [Are there new topics that could be specifically identified for discussion in the permanent mechanism to reflect recent developments within or outside the OEWG, e.g. operationalization and further improvement of the Global Points of Contact Directory?]
- iii. [How would the scope of the future mechanism build on the work already done and on the concrete outcomes achieved under current and previous processes?]

(c) The **structure** of the permanent mechanism could take the following form:

- i. **Number of meetings:** Two substantive sessions of the permanent mechanism could be convened per year.
- ii. **Progress Reports:** The permanent mechanism could submit Progress Reports on a biennial basis (i.e. once every two years) to the First Committee.
- iii. **Dedicated Thematic Groups:** The permanent mechanism could possibly establish dedicated thematic groups focused on specific issues. [If so, what topics could the Dedicated Thematic Groups focus on, e.g. capacity-building, specific issues under international law, the Global POC Directory?]

(d) The permanent mechanism could operate in accordance with the following **modalities**:

- i. The permanent mechanism could be established as a subsidiary body of the First Committee.
- ii. The United Nations Office for Disarmament Affairs could serve as the Secretariat of the permanent mechanism.
- iii. The Chair of the permanent mechanism could be appointed for a period of [one year] [two years] on the basis of equitable geographical representation.
- iv. [The Chair could be assisted by a bureau, comprising additional officers, taking into account the principle of equitable geographical distribution?]
- v. Formal meetings of the permanent mechanism could be convened at [UNHQ in New York?]

- vi. Inter-sessional meetings of the permanent mechanism could be convened at [UNHQ in New York? UN Office in Geneva? Other appropriate locations?]
- vii. An e-portal/website could be established to facilitate the work of the permanent mechanism (e.g. storing and making available official documents, working papers and statements).

(e) The permanent mechanism could conduct **decision making** in accordance with the following procedures:

- i. Decisions could be put forward by the Chair for adoption by States on a consensus basis at any time during a substantive session, with decisions to be formalized as soon as they are agreed upon by the OEWG.

(f) The permanent mechanism could be subject to **review** in accordance with the following procedures:

- i. The operations of the permanent mechanism, in particular the arrangements contained above, could be reviewed every [X] years.
- ii. Any modifications to these arrangements could be decided by States on the basis of consensus.

8 Delegations are invited to share views on the proposed elements set out in paragraph 7 during the focused discussions at the seventh substantive session of the OEWG on the issue of regular institutional dialogue, in accordance with the recommended next step agreed in the second APR.

.