*Russian amendments*
*to the draft OEWG report*
*of 22 June 2022*

# 2022 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 77TH SESSION OF THE GENERAL ASSEMBLY PURSUANT TO GENERAL ASSEMBLY RESOLUTION 75/240

## A. Introduction

1. The first, second and third substantive sessions of the Open-ended Working Group (OEWG) on the security of and in the use of Information and Communications Technologies (ICTs) 2021-2025 took place in a challenging geopolitical environment with rising concern over the malicious use of ICTs by State and non-state actors. At these sessions, States reaffirmed the consensus report of the 2021 OEWG on developments in the field of ~~ICTs~~ information and telecommunications in the context of international security[1] and the consensus reports of the 2010, 2013, 2015, and 2021 groups of governmental experts (GGEs).[2] States recalled consensus resolutions of the UN General Assembly in which States agreed that in their use of ICTs they should be guided by the reports of the OEWG and the GGEs.[3]

States recalled and reaffirmed that the reports of these Groups "recommended 11 voluntary, non-binding rules, norms and principles of responsible ~~State~~ behaviour of States and recognized that additional norms could be developed over time", and that "specific confidence-building, capacity-building and cooperation measures were recommended". States also referred to the initial set of 13 rules, norms and principles of responsible behaviour of States recommended in the UN General Assembly resolution[4] and proposals made by States on the elaboration of rules, norms and principles of responsible behaviour of States within the OEWG on developments in the field of information and telecommunications in the context of international security[5].

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] and reaffirmed, considering unique features of ICTs, the possibility of elaboration of additional legally binding obligations[7]. ~~States~~

[1] Report of the 2021 OEWG, A/75/816.
[2] Reports of the GGEs, A/65/201, A/68/98, A/70/174 and A/76/135.
[3] UNGA resolutions No.70/237 and No.76/19.
[4] UNGA resolution No.73/27.
[5] Report of the 2021 OEWG, A/75/816, Annex I, para 33 and Annex to the Chair's Summary.
[6] Report of the 2021 OEWG, A/75/816, Annex I, para 7.
[7] UNGA resolution No.76/19.

~~also recalled the consensus resolutions of the General Assembly in which States agreed they should be guided in their use of ICTs by the OEWG and GGE reports.[8]~~

2. In recognition that substantive discussions under the OEWG will continue until the completion of its mandate in 2025, States agreed that this first annual progress report of the Group is not intended to be a comprehensive summary of discussions by States which are ongoing, but aims to capture concrete progress made at the OEWG to date, with a focus on the proposals by States as well as next steps of the OEWG. This progress report will be submitted to the General Assembly pursuant to the OEWG mandate in resolution 75/240.

**B. Existing and Potential Threats**

3bis. States indicated the following challenges and threats in the field of ensuring security in the use of ICTs:
– the use of ICTs in military, political and other spheres to undermine (infringe upon) sovereignty, violate the territorial integrity of states, and commit other acts in the global information space impeding the maintenance of international peace, security and stability;
– the use of ICTs for terrorist purposes, including for advocacy of terrorism and recruitment of new supporters;
– the use of ICTs for extremist purposes and interference in internal affairs of sovereign states;
– the use of ICTs for disseminating information harmful to socio-political and socio-economic systems, as well as spiritual, moral, and cultural environment of other States;
– the use of ICTs for criminal purposes, including to commit computer information crimes and various frauds;
– the use of ICTs for computer attacks on state information resources, including critical information infrastructure;
– the use of ICTs for disseminating, under the guise of reliable messages, information known to be false leading to threat to the life and safety of citizens or to severe consequences;
– the use of ICTs for making unfounded accusations by some States against other States of organizing and (or) committing crimes and computer attacks;
– the use by certain states of technological dominance in the global information space to monopolize the ICTs market, limit access of other states to advanced information and communications technologies, and to increase their technological dependence from states dominating the sphere of informatization, and information inequality;
– deploying in the national information space of States, in free access, tools for conducting computer attacks, instructions on methods of their organization and

~~[8] GA resolutions 70/237 and 76/19.~~

elaboration of practical skills of using such instruments, coordination of respective actions on carrying out computer attacks.

3. States made concrete, action-oriented proposals to address existing and potential threats. The following is a non-exhaustive list of proposals that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) Technical and cooperative measures to address existing and potential threats, including:

(i) bis Measures to prevent manipulation of information flows in information space of States, dissemination of disinformation, falsified messages and hateful rhetoric in order to undermine global strategic stability, public order in particular States, and to incite interethnic, interracial and interreligious hatred, propaganda of racist and xenophobic ideas and theories, as well as to destabilize the internal political and socio-economic situation, to undermine State governance;

(i) Cooperation and assistance to establish and strengthen Computer Emergency Response Teams (CERTs);

(ii) Cooperation and assistance for developing ~~ICT security~~ baseline studies on ensuring security in the use of ICTs and designing security as a critical requirement;

(iii) Sharing of risk assessments and technical information between States including threat intelligence and compendiums;

(iv) Developing and disseminating comprehensive best practices on the classification and protection of ~~Critical Infrastructure (CI) and Critical~~ national ~~I~~information ~~I~~infrastructure ~~(CII)~~, including critical infrastructure~~.~~;

(iv) bis Measures to prevent the deployment in the national information space of States, in free access, tools for conducting computer attacks, instructions on methods of their organization and elaboration of practical skills of using such instruments;

(v) Undertaking international exercises for exchanging experience – upon agreement of States on the topic, format and other parameters – and technical training including of law enforcement officials understanding that this activity should not be directed against any UN Member State;

(vi) Prioritizing mutual legal assistance;

~~(vii) Enhancing tailored capacity building efforts;~~

(viii) Cooperation and assistance to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions;

(ix) Measures and initiatives to strengthen data security, including elaboration of basic requirements for personal data processing with a view to improving its safety and decreasing falsified information flow;

(ix) bis Prevention of unlawful restrictive measures against particular States, including those directed against freedom of dissemination of information in mass media, and pursuing discriminatory policy against private companies;

(x) Measures to safeguard the general availability ~~and integrity~~, secure and stable functioning of the internet taking into account States' sovereignty in their

information space, as well as to ensure equal participation of States in the governance of this network.

(x) bis ***(based on the Chair's summary of the OEWG 2019-2021)***

– Possibility of using mechanisms to settle disputes related to the use of ICTs by peaceful means instead of imposing unlawful unilateral sanctions and other restrictions that lead to escalation of tensions.

– Measures to counter cross-border information-psychological attacks aimed at undermining existing political system.

– Measures to counter the use of artificial intelligence for creating bots and deepfakes with a view to interfering in internal affairs of other States;

– Measures to ensure freedom of mass media and to limit unlawful unilateral measures aimed at blocking their activities;

– Elaboration of norms, which define international legal status (rights, obligations, responsibilities) of IT-companies from private sector in terms of ensuring the right of users of their services for freedom of information;

– Implementation of rules, norms and principles of responsible behaviour of States in information space aimed at assessing activities of members of the international community should not lead to escalation of tension.

– If an ICT activity is launched or otherwise originates from the territory or the ICT infrastructure of a UN Member State for purposes contradicting the UN Charter, attribution of this activity to that State, as well as accusations of organizing and implementing wrongful acts should be substantiated and grounded on genuine, reliable and adequate proof in this context.

– Inadmissibility of eroding the concepts of peacetime and wartime through recognition of the applicability of international humanitarian law during peacetime.

– Inadmissibility of using the rules, norms and principles of responsible behaviour of States in information space for purposes inconsistent with the objectives of maintaining international peace, stability and security, as well as for undue restrictions on international cooperation, nor for hindering innovation for peaceful purposes and economic development of States in a fair and non-discriminatory environment.

b) The OEWG could be a platform to foster global, inter-regional cooperative approaches on the security ~~of and~~ in the use of ICTs. There is value in regional and sub-regional organizations sharing relevant experiences at the OEWG.

c) States could consider strengthening interactions with responsible interested stakeholders~~, including businesses, non-governmental organizations and academia,~~ through the exchange of knowledge and best practices, including on the protection of ~~CI~~ critical infrastructure (CI) and ~~CII~~ critical information infrastructure (CII), primarily with subjects of such infrastructure.

**Recommended next steps**

**1. States continue exchanging views at the OEWG on emerging and existing threats to security in the use of ICTs with the potential to impact international peace and security, and cooperative measures to address them.**

**2. States consider utilizing the framework of the OEWG to further exchange technical information relating to existing and potential threats to security in the use of ICTs, including the sharing of risk assessments, relevant threat intelligence, best practices, and incident mitigation measures, on a voluntary basis. Experts could be invited to make presentations on these topics to facilitate further discussion.**

**3. States engage in focused discussions on, *inter alia*, the protection of CI and CII, as well as ensuring security of personal and other data ~~with representatives from the different regions and subregions as well as representatives from interested stakeholders, including businesses, non-governmental organizations and academia,~~ at the fourth and fifth sessions of the OEWG. If States have no objections, representatives of different regions and subregions, as well as businesses, non-governmental organizations and academia could also be involved in such discussions.**

**C. Rules, Norms and Principles of Responsible State Behaviour**

4. States made concrete, action-oriented proposals on rules, norms and principles of responsible state behaviour. The following is a non-exhaustive list of proposals that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) States consider developing additional guidance ~~or checklists~~ with recommendations on implementation of rules, norms and principles of responsible behaviour ~~implementation~~, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE reports, as well as consider developing common understandings on technical ~~ICT~~ terms related to security in the use of ICTs.

b) States proposed that additional norms could continue to be developed over time, noting that the further development of norms and the implementation of existing norms were not mutually exclusive but could take place in parallel.[9]

[9] Report of the 2021 OEWG, A/75/816, Annex I, para 29.

c) Information exchange on best practices and cooperation could be enhanced~~, potentially drawing from models of information sharing in other fields,~~ and could include topics such as innovation, vulnerability disclosure, normative legal regulation in the field of ensuring security in use of ICTs, the protection of critical infrastructure and cooperation between CERTs, as well as Internet governance.

d) States could ~~consider surveying or voluntarily reporting on their national~~ exchange information on development and implementation of rules, norms and principles of responsible State behaviour utilizing, on a voluntary basis, existing avenues and tools such as ~~the National Survey of Implementation, as contained in the recommendations of the 2021 OEWG report,[10] and~~ the report of the Secretary-General on developments in the field of ~~ICTs~~ information and telecommunications in the context of international security. In this regard, States also recalled the National Survey of Implementation, elaborated by Australia and Mexico and referred to in the 2021 OEWG report.

e) Regarding the consideration of proposals under this topic, States recalled the recommendation in the 2021 OEWG report that States take note of the list of non-exhaustive proposals made on the elaboration of rules, norms and principles of responsible behaviour of States (annexed to the Chair's Summary in the 2021 OEWG Report[11]) in future discussions on ensuring security in the use of ICTs within the United Nations~~.~~[12], in particular:

– States will refrain from any action that might result in attempted disruption of the integrity of CI and government activities, and offer through agreed channels timely clarifications to prevent further possible escalation.

– States should reaffirm their commitment to the principle of abandonment of militarization of existing ICTs and the creation of new ICTs specifically designed to harm information resources, infrastructure and critical facilities of other countries.

– States have the rights and responsibilities regarding legal protection of their CII against damage resulting from materialized threats in the use of ICTs, interference, attacks and sabotage.

– States should not exploit political and technical advantages to undermine the security and integrity of CI of other states.

– States should increase exchanges on standards and best practices with regard to CI protection and encourage enterprises to embark on such exchanges.

e) bis States noted the proposal for an international code of conduct for information security tabled in 2015.

e) bis bis States, expressing concern over the creation of harmful hidden functions in ICT products, also proposed further ensuring the integrity of the ICT supply chain and introducing responsibility to notify users when significant vulnerabilities are identified. States, furthermore, expressed concern regarding the stockpiling of vulnerabilities. Some States proposed to formulate objective international rules and standards on supply chain security.

---

~~[10] Report of the 2021 OEWG, A/75/816, Annex I, para 65.~~

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

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

**Recommended next steps**

**1. States continue exchanging views at the OEWG on rules, norms and principles of responsible State behaviour in the use of ICTs, including on best practices in this regard, and discuss the proposals from the non-exhaustive list in paragraph 4e) above, at the fourth and fifth sessions of the OEWG. The OEWG participants agreed to take practical steps on elaborating additional rules, norms and principles of reaponsible behaviuor of States, including those of a legally binding nature[13].**

**2. Interested States or groups of States are invited to submit working papers to contribute to the development of ~~guidance, checklists~~ rules, norms and principles of responsible behaviour and measures to implement them and common understandings on technical ~~ICT~~ terms related to security in the use of ICTs along with other tools to assist States in the implementation of abovementioned rules, norms and principles ~~of responsible State behaviour in the use of ICTs~~. Such working papers could facilitate a focused exchange of views at the OEWG.**

**3. States ~~are encouraged to~~ can exchange views, on voluntary basis, ~~survey and/or report~~ on their national efforts to develop and implement rules, norms and principles of responsible behaviour, including through ~~the National Survey of Implementation and~~ the report of the Secretary-General on developments in the field of ~~ICTs~~ information and telecommunications in the context of international security. States can study prospects of elaborating additional forms for such exchange under the UN auspices.**

**D. International Law**

5. States made concrete, action-oriented proposals on international law. The following is a non-exhaustive list of proposals that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could convene discussions on specific topics related to international law. ~~This may include expert briefings, such as from the International Committee of the Red Cross, to consolidate~~ Holding intersessional consultative meetings and expert briefings could help States elaborate common understandings on this subject, including through additional expert information. A non-exhaustive list of topics proposed by States for further discussion under applicability of international law includes: State sovereignty in information space, ~~; sovereign equality; non-intervention in the internal affairs of other States; peaceful settlement of disputes;~~ how international law, in particular the Charter of the United Nations and such of its principles, as sovereign equality, settlement of disputes by peaceful

[13] UNGA resolution No.76/19.

means, non-intervention in internal affairs of States, applies ~~in~~ to the use of ICTs, whether gaps in common understandings exist on how international law applies, as well as the possibility of additional legally binding obligations; State responsibility and due diligence; respect for human rights and fundamental freedoms, as well as special duties and responsibilities that their exercise carries; ~~and principles of proportionality, distinction, humanity, necessity~~.

b) Recalling the recommendation of the previous OEWG,[14] States could continue sharing national views on how international law applies in the use of ICTs, utilizing, on a voluntary basis, existing avenues and tools ~~such as the UNIDIR Cyber Policy Portal and the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security~~.
b) bis States could also continue exchanging views on prospects for negotiating at the international level legally binding normative framework for regulating the use of ICTs. Such legally binding normative framework could contribute to more effective fulfillment of obligations at the global level and could become a more reliable basis for bringing subjects to responsibility for committed acts.

c) Capacity-building efforts on international law could be strengthened and could include workshops and training courses as well exchanges on best practice at the international, inter-regional, regional and sub-regional levels, as well as draw from the experience of relevant regional organizations. It was proposed that capacities could be developed on issues such as, *inter alia*, common understanding of criteria for unlawful ~~ICT~~ activities with the use ICTs by different States and improving mechanisms of mutual legal assistance for investigating malicious use of ICTs.

**Recommended next steps**

**1. States continue exchanging views at the OEWG on how international law applies ~~in~~ to the use of ICTs and on prospects of its adaptation taking into consideration the specificities of these technologies.**

**2. States engage in focused discussions on topics from the non-exhaustive list in paragraph 5a) above at the fourth and fifth sessions of the OEWG. Holding consultative meetings and expert briefings in the intersessional period is to contribute to S~~s~~uch discussions ~~should include briefings from experts~~.**

**3. States are invited to continue to voluntarily share their national views on international law, including through existing mechanisms ~~such as the National Survey of Implementation and the report of the Secretary-General on developments in the field of ICTs in the context of international security~~.**

**4. States are, on a voluntary basis, invited to submit to the ~~Secretariat~~ Chair of the OEWG information on their positions on international legal regulation of**

[14] Report of the 2021 OEWG, A/75/816, Annex I, para 38.

**the use of ICTs, as well as on potential needs and gaps in capacity-building in the area of international law, ~~as well as on~~ existing ~~capacity-building~~ initiatives and opportunities in this area. The ~~Secretariat~~ Chair of the OEWG is requested to collate this information submitted by States, to prepare a background paper on ~~needs, opportunities and gaps in the area of capacities relating to international law,~~ the abovementioned issues and to make a presentation on this topic at ~~the fourth~~ one of the future OEWG sessions.**

**E. Confidence-Building Measures**

6. States made concrete, action-oriented proposals on confidence-building measures (CBMs). The following is a non-exhaustive list of proposals that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could agree to establish a global points of contact directory on ICTs at the United Nations. States may, on a voluntary basis, provide points of contact (PoCs) at the diplomatic, policy and technical levels with due competence at the national level in ensuring security in the use of ICTs that could be reached in times of urgency, for example through hotlines. Such a directory would respect State sovereignty and be politically neutral. It would be updated regularly, and be ~~secure~~ pragmatic, operational and complemented by capacity-building such as table-top exercises where requested. Taking into account the voluntary nature of CBMs, Member States recognize the importance of interstate interaction in ensuring security in the use of ICTs and will seek to raise the status of such cooperation. The ~~UN Secretariat~~ Chair of the OEWG could be requested to collect and disseminate ~~to the OEWG~~ among States best practices on operationalizing such a directory which would include experiences at the regional level.

b) Recalling the recommendation of the previous OEWG,[15] States could continue to voluntarily share white papers, national strategies and policies including ~~ICT~~ capabilities in the use of ICTs, as well as share information on national ~~ICT~~ institutions and structures in the field of ensuring security in the use of ICTs, and national lists of CI areas. ~~The UNIDIR Cyber Policy Portal could be an avenue for sharing such information.~~

c) It was proposed that aspects of confidence-building could include stakeholder engagement such as cooperation with interested stakeholders, including businesses, non-governmental organizations and academia, on *inter alia* ensuring the integrity of the supply chain, preventing malicious uses of ICTs tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat

[15] Report of the 2021 OEWG, A/75/816, Annex I, para 50.

information. Points of Contact in the private sector could be established as appropriate.

d) Cooperation between CERTs could be strengthened and include the sharing and dissemination of good practices on incident management. Cooperation to mitigate attacks on CI and other malicious ICT-related activity could also be enhanced.

e) States also made a variety of proposals for new CBMs on issues such as public-private partnerships; the coordinated disclosure of vulnerabilities; the development of common understanding on a glossary of basic terms with the aim of reducing mistrust by building common understanding; and on the use of ICTs for the economic development of States in a fair and non-discriminatory environment.

**Recommended next steps**

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

**2. States engage in focused discussions on *inter alia*: (a) the development and operationalization of the global points of contact directory as well as related initiatives for capacity-building and the sharing of best practices, and (b) the sharing of regional and sub-regional experiences on the development and operationalization of CBMs, including briefings by regional and sub-regional organizations as appropriate, at the fourth and fifth sessions of the OEWG.**

**3. The ~~UN Secretariat~~ Chair of the OEWG is requested to collate best practices on the operationalization of a global points of contact directory, which could include experiences at the regional level, and produce a report with options for the development of such a global directory for consideration at the fourth session of the OEWG.**

**4. States are encouraged to submit, on a voluntary basis, information on their national P~~O~~oCs to the Chair of the OEWG, as well as part of their responses to ~~either (a) the National Survey of Implementation, and/or (b)~~ the report of the Secretary-General on developments in the field of ~~ICTs~~ information and telecommunications in the context of international security.**

**5. States are invited to submit to the ~~UN Secretariat~~Chair of the OEWG, on a voluntary basis, their views, suggestions and recommendations on the development of voluntary protocols, procedures, and standardised templates for exchange of information between points of contact at the technical and political levels. The ~~UN Secretariat~~Chair of the OEWG is requested to collate**

**and circulate all submitted information to delegations for discussion at the fourth session.**

**6. The OEWG Chair is requested to convene an inter-sessional meeting with States and interested stakeholders, including businesses, non-governmental organisations and academia, ~~no later than the beginning of the fourth session, to explore the development and implementation of CBMs, including *inter alia*~~ in particular, to discuss such topics as ensuring the integrity of the supply chain, preventing malicious uses of ICT~~s~~ tools and techniques, preventing the use of harmful hidden functions and the sharing of current threat information.**

**7. States are encouraged to continue, on a voluntary basis, to share white papers, national legislation, strategies and policies including ~~ICT~~ capabilities in the use of ICTs, as well as information on ~~ICT~~ institutions and structures in the field of ensuring security in the use of ICTs, ~~including through the UNIDIR Cyber Policy Portal~~.**

**F. Capacity-Building**

7. States made concrete, action-oriented proposals on capacity-building. This non-exhaustive list of proposals may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could promote better understanding of the needs of developing States, for instance through ~~encouraging participation in questionnaires; the National Survey of Implementation; the Cybersecurity Capacity Maturity Model; technical studies; and needs~~ assessment ~~models~~ of existing needs, as well as studying the necessity to elaborate under the UN auspices a template format and/or questionnaire for conducting such an assessment. Such efforts could also assist in matching needs with resources and lead to more effective coordination in capacity-building. At the same time, the abovementioned efforts of UN Member States should not result in unlawful acts in information space of developing countries.

b) The OEWG could play a role in furthering capacity-building coordination by encouraging coordination between online portals, consolidating and compiling a calendar of capacity-building programmes and developing a list of regional and sub-regional centres of excellence in ensuring security in the use of ICTs.

c) States could ~~consider~~ assess whether it is appropriate to establish~~ing~~ a permanent mechanism for exchanging views and ideas related to capacity-building in ensuring security in the use of ICTs while taking into account existing initiatives. It was ~~proposed that such a mechanism could be established within the UN~~ highlighted that concrete modalities of such a mechanism should be developed within the OEWG to

ensure that views of all States are taken into account on a fair basis. Its activities should not duplicate the efforts of the OEWG.

d) States could consider further funding for ~~ICT~~ capacity-building for ensuring security in the use of ICTs through potential coordination and integration with larger development programmes and multi-donor trust funds. In this regard, States also highlighted the possibility of a dedicated trust fund for ~~ICT~~ capacity-building projects for ensuring security in the use of ICTs.

e) States could strengthen coordination and cooperation between States and interested stakeholders, including businesses, non-governmental organizations and academia. States noted that stakeholders are already playing an important role through partnerships with States for the purposes of training public officials, research, and facilitating access to internet and digital services.

**Recommended next steps**

**1. States continue exchanging views at the OEWG on capacity-building.**

**2. States engage in focused discussions on, *inter alia*: (a) funding for ~~ICT~~ capacity-building for ensuring security in the use of ICTs through potential coordination and integration with larger development programmes and multi-donor trust funds, (b) whether it is appropriate to establish a permanent mechanism~~, potentially~~ within the UN, for exchanging views and ideas related to capacity-building for ensuring security in the use of ICTs while taking into account existing initiatives~~, at the fourth and fifth sessions of the OEWG,~~ and (c) best practices and lessons learnt on the topic of public-private partnerships in ~~the use of ICTs~~ this area.**

**3. States are invited, on a voluntary basis, to provide the ~~UN Secretariat~~Chair of the OEWG with information on forthcoming capacity-building programmes as well as information on regional and sub-regional ~~ICT~~ centres of excellence in the field of ensuring security in the use of ICTs. The UN Secretariat is requested to make this information available on the OEWG website.**

**4. The ~~UN Secretariat~~ Chair of the OEWG is requested to designate a~~n~~ ~~ICT capacity-building~~ focal point on capacity-building for ensuring security in the use of ICTs with the responsibility of coordinating offers and requests for capacity-building, taking into account the proposals in paragraphs 7(a)-(e). The focal point could also coordinate capacity-building efforts by working with interested stakeholders, including businesses, non-governmental organizations and academia.**

**5. States are encouraged, on a voluntary basis, to survey their capacity needs ~~including through the National Survey of Implementation and/or the~~**

**~~Cybersecurity Capacity Maturity Model~~, as well as to study the need for elaborating under the UN auspices a template format and/or questionnaire for conducting such an assessment.**

**6. States in a position to do so are invited to continue to support capacity-building programmes, including in collaboration with interested stakeholders, including businesses, non-governmental organizations and academia.**

**7. The ~~UN Secretariat~~ Chair of the OEWG is requested to invite interested stakeholders, including businesses, non-governmental organizations and academia, to submit offers to share resources in support of international capacity-building efforts, such as, *inter alia* expertise, information, data, experience and training, and to collate information on these offers and share the information on the OEWG website.**

**G. Regular Institutional Dialogue**

8. States made concrete, action-oriented proposals on regular institutional dialogue. This non-exhaustive list of proposals may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could play a role in raising awareness, building trust and deepening understanding in areas where no common understanding has yet emerged. Furthermore, each OEWG session should build incrementally on the previous one. States underlined the centrality of the OEWG as the negotiation mechanism within the United Nations on the security of and in the use of ICTs.

a) bis States reaffirmed their preference to continue the negotiation process on security in the use of ICTs under the UN auspices within a single consensus-based mechanism.

b) In considering proposals under this topic, States recalled the recommendation in the 2021 OEWG report that the Programme of Action (PoA) for advancing responsible State behaviour in ICTs should be further elaborated including at the current OEWG.11 It was proposed that the PoA could be a mechanism to support capacity-building for

~~c)~~ implementing the framework of responsible ~~State~~ behaviour of States~~in the use of ICTs~~.

b) bis States suggested fostering interaction and exchange of views on ensuring security in the use of ICTs between the UN and regional organizations.

**Recommended next steps**

**1. States continue exchanging views at the OEWG on regular institutional dialogue.**

**2. States engage in focused discussions on the ~~elaboration~~ development of various proposals of States, including a PoA within the framework of the**

**OEWG with a view towards its possible establishment as a mechanism to advance capacity-building with the understanding that the OEWG should remain a single negotiation mechanism on security in the use of ICTs under the UN auspices and its mandate and efforts should not be duplicated in other structures. States will also engage in focused discussions, at the fourth and fifth sessions of the OEWG, on the relationship between ~~the PoA~~ such proposals and the OEWG, and on the scope, content and timeframe for the establishment of a PoA.**