United Nations A/AC.292/2022/CRP.1

General Assembly

28 July 2022

English only

Open-ended working group on security of and in the use of information and communications technologies 2021-2025
Third substantive session, New York
25-29 July 2022

Draft Annual Progress Report

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 targeting critical infrastructure and essential services. At these sessions, States 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.[1] In this regard, States further recalled the contributions of the first OEWG, established pursuant to General Assembly Resolution 73/27, which concluded its work in 2021, through its final report agreed by consensus, as well as noted the Chair's summary and list of non-exhaustive proposals annexed to the Chair's summary, and recalled the contributions of the sixth Group of Governmental Experts (GGE), established pursuant to General Assembly Resolution 73/266, which concluded its work in 2021, through its final report agreed by consensus.

2. Furthermore, States reaffirmed the consensus report of the 2021 OEWG on developments in the field of ICTs in the context of international security[2] and the consensus reports of the 2010, 2013, 2015, and 2021 GGEs.[3] States recalled and reaffirmed that the reports of these Groups "recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time", and that "specific confidence-building, capacity-building and cooperation measures were recommended". States also recalled and reaffirmed that "international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment".[4] These elements consolidate a

[1] GA resolutions 70/237 and 76/19.
[2] A/75/816.
[3] A/65/201, A/68/98, A/70/174 and A/76/135.
[4] Report of the 2021 OEWG, A/75/816, Annex I, para 7.

cumulative and evolving framework[5] for responsible State behaviour in the use of ICTs providing a foundation upon which the current OEWG builds its work.

3. The OEWG recalled its mandate contained in General Assembly resolution 75/240 as follows: "Acting on a consensus basis, to continue, as a priority, to further develop the rules, norms and principles of responsible behaviour of States and the ways for their implementation and, if necessary, to introduce changes to them or elaborate additional rules of behaviour; to consider initiatives of States aimed at ensuring security in the use of information and communications technologies; to establish, under the auspices of the United Nations, regular institutional dialogue with the broad participation of States; to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, *inter alia*, data security, and possible cooperative measures to prevent and counter such threats, and how international law applies to the use of information and communications technologies by States, as well as confidence-building measures and capacity-building; and to submit, for adoption by consensus, annual progress reports and a final report on the results of its work to the General Assembly at its eightieth session." In this regard, the OEWG acknowledged the importance of addressing its mandate in a balanced manner and the need to give due attention to both further develop common understandings between States on security in the use of ICTs, as well as to further the implementation of existing commitments.

4. The OEWG is committed to engaging stakeholders in a systematic, sustained and substantive manner, in accordance with the modalities agreed by silence procedure on 22 April 2022 and formally adopted at the first meeting of the third session of the OEWG on 25 July 2022, and in line with its mandate contained in General Assembly Resolution 75/240 to interact, as appropriate, with other interested parties, including businesses, non-governmental organizations and academia.

5. The OEWG recognized that regional and sub-regional organizations could continue to play an important role in implementing the framework for responsible State behaviour in the use of ICTs. In addition, regional, cross-regional and inter-organizational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. As not all States are members of a regional organization and not all regional organizations focus on the issue of security in the use of ICTs, the OEWG noted that regional efforts are complementary to its work.

6. The OEWG welcomed the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions.[6] The OEWG underscored the importance of narrowing the "gender digital divide" and of promoting the full, equal and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security.

7. In recognition that the OEWG is in the early stages of its deliberations and that substantive discussions under the OEWG will continue until the completion of its mandate in 2025, 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 proposals by States and next steps of the OEWG, as well as set out a roadmap for focused discussions on specific topics within the OEWG's mandate. This progress report will be submitted to the General Assembly pursuant to the OEWG mandate in resolution 75/240.

B. Existing and Potential Threats

8. States, recalling the threats identified in the 2021 OEWG and GGE reports, reiterated increasing concern that threats in the use of ICTs in the context of international security have continued to intensify and have evolved significantly in the current challenging geopolitical environment.

[5] Report of the 2021 GGE, A/76/135, para 2, consensus GA resolution 76/19
[6] Report of the 2021 OEWG, A/75/816, Annex I, para 12.

9. States recalled that a number of States are developing ICT capabilities for military purposes. They also recalled that the use of ICTs in future conflicts between States is becoming more likely. The continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including terrorists and criminal groups, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States.[7]

10. Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, has become increasingly serious. Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities. The COVID-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain.[8]

11. New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity.[9]

12. States recalled that any use of ICTs by States in a manner inconsistent with their obligations under the framework, which includes voluntary norms, international law, and CBMs, undermines international peace and security, trust and stability between States.[10]

13. States also recalled the OEWG's mandate on existing and potential threats: "To continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security, inter alia, data security, and possible cooperative measures to prevent and counter such threats".[11]

Recommended next steps

1. **States continue exchanging views at the OEWG on existing and potential threats to security in the use of ICTs with the potential to impact international peace and security, and possible cooperative measures to address these threats, in this regard committing to and reaffirming their observation and implementation of the framework for responsible State behaviour in the use of ICTs, which is essential to addressing the existing and potential ICT-related threats to international security.**

2. **States engage in focused discussions on the existing and potential threats identified in paragraphs 8 to 13 at the fourth and fifth sessions of the OEWG.**

C. Rules, Norms and Principles of Responsible State Behaviour

14. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on rules, norms and principles of responsible state behaviour. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) States consider developing additional guidance or checklists on norms implementation, elaborating and building upon the conclusions and recommendations agreed to in previous OEWG and GGE

[7] Report of the 2021 OEWG, A/75/816, Annex I, para 16.
[8] Report of the 2021 GGE, A/76/135, para 10, consensus GA resolution 76/19
[9] Report of the 2021 GGE, A/76/135, para 11, consensus GA resolution 76/19
[10] Report of the 2021 OEWG, A/75/816, Annex I, para 17.
[11] GA resolutions 75/240, operative paragraph 1

reports, as well as consider sharing national definitions on technical ICT terms to promote mutual understanding.

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.[12]

c) Cooperation and assistance could be strengthened to ensure the integrity of the supply chain, and prevent the use of harmful hidden functions. Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include[13]:

   i) "Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice."[14]

   ii) "Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels 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." [15]

d) States could consider voluntarily surveying or reporting on their national implementation of rules, norms and principles of responsible State behaviour utilizing, on a voluntary basis, existing avenues and tools such as the report of the Secretary-General on developments in the field of ICTs in the context of international security[16] as well as the National Survey of Implementation, as contained in the recommendations of the 2021 OEWG report.[17]

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 State behaviour (annexed to the Chair's Summary in the 2021 OEWG Report[18]) in future discussions on security in the use of ICTs within the United Nations.[19]

Recommended next steps

1. **States continue exchanging views at the OEWG with the aim of developing common understandings on, as well as facilitating the implementation of, 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 14(e) above, at the fourth and fifth sessions of the OEWG.**

2. **Interested States or groups of States are invited to submit, on a voluntary basis, working papers to contribute to the development of guidance, checklists and to share national views on technical ICT terms along with other tools to assist States in developing common understandings on as well as facilitating the implementation of rules, norms and principles of responsible State behaviour in the use of ICTs. Such working papers could facilitate a**

[12] Report of the 2021 OEWG, A/75/816, Annex I, para 29.
[13] Report of the 2021 GGE, A/76/135, para 57, consensus GA resolution 76/19
[14] Report of the 2021 GGE, A/76/135, para 57(b), consensus GA resolution 76/19
[15] Report of the 2021 GGE, A/76/135, para 57(d), consensus GA resolution 76/19
[16] General Assembly resolution 76/19 operative paragraph 6.
[17] Report of the 2021 OEWG, A/75/816, Annex I, para 65.
[18] Report of the 2021 OEWG, A/75/816, Annex II.
[19] Report of the 2021 OEWG, A/75/816, Annex I, para 33.

focused exchange of views at the OEWG.

3. **States are encouraged to, on voluntary basis, survey and/or report on their national efforts to implement rules, norms and principles, including through the report of the Secretary-General on developments in the field of ICTs in the context of international security as well as the National Survey of Implementation.**

D. International Law

15. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on international law. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could convene discussions on specific topics related to international law. Such discussions should focus on identifying areas of convergence and consensus. A non-exhaustive, open list of topics proposed by States for further discussion under international law includes: How international law, in particular the Charter of the United Nations, applies in the use of ICTs; sovereignty; sovereign equality; non-intervention in the internal affairs of other States; peaceful settlement of disputes; State responsibility and due diligence; respect for human rights and fundamental freedoms; whether gaps in common understandings exist on how international law applies; and proposals contained in the 2021 OEWG report and Chair's summary where relevant.

b) The OEWG noted the recommendations in the 2021 OEWG report and 2021 GGE report respectively as follows:

(i) "Throughout the OEWG process, States participated consistently and actively, resulting in an extremely rich exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States, including the possibility of additional legally binding obligations. The diverse perspectives are reflected in the attached Chair's Summary of the discussions and specific language proposals under agenda item "Rules, norms and principles". These perspectives should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240.";[20]

(ii) "The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict."[21]

c) Recalling the recommendation of the previous OEWG,[22] States could continue sharing national views, on a voluntary basis, on how international law applies in the use of ICTs, utilizing, on a voluntary basis, existing avenues and tools.

d) 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

[20] Report of the 2021 OEWG, A/75/816, Annex I, para 80.
[21] Report of the 2021 GGE, A/76/135, para 71(f), consensus GA resolution 76/19.
[22] Report of the 2021 OEWG, A/75/816, Annex I, para 38.

and sub-regional levels, as well as draw from the experience of relevant regional organizations, as appropriate.

Recommended next steps

1. **States continue exchanging views at the OEWG on how international law applies in the use of ICTs.**

2. **States engage in focused discussions on topics from the non-exhaustive list in paragraph 15(a)-(b) above as well as proposals contained in the 2021 OEWG report and Chair's summary, where relevant, at the fourth and fifth sessions of the OEWG.**

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

E. Confidence-Building Measures

16. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on confidence-building measures (CBMs). The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) Recalling the conclusions and recommendations of the 2021 OEWG report and the consensus GGE reports, recognizing the significant work done by regional organizations on CBMs as well as existing regional initiatives to develop points of contact (PoCs) directories on security in the use of ICTs, and further recognizing that not all States are members of regional organizations or of regional organizations undertaking such work, the OEWG could agree to establish a global, inter-governmental, points of contact directory on security in the use of ICTs at the United Nations for enhancing interaction and cooperation between States, by building on existing regional initiatives.

b) States may, on a voluntary basis, provide points of contact at the diplomatic 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. States may wish to nominate the same PoCs for inclusion in the global directory as for the regional directory as applicable, such that the global directory could build upon and serve a complementary function to existing regional initiatives.

c) Recalling the recommendation of the previous OEWG, States voluntarily engage in transparency measures by sharing relevant information and lessons in their chosen format and fora, as appropriate.[23]

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

e) States continued to emphasize that the OEWG itself served as a CBM.

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

Recommended next steps

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

2. **States agree to establish, building on work already done at the regional level, a global, inter-governmental, points of contact directory. At the fourth and fifth sessions of the OEWG, States to engage in further focused discussions on the development of such a directory, on a consensus basis, as well as engage in discussions on initiatives for related capacity-building, taking into account available best practices such as regional and sub-regional experiences where appropriate.**

3. **The UN Secretariat is requested to seek views from States on the global points of contact directory, which could include views on experiences at the regional and sub-regional levels, and produce a background information paper on these views by the end of January 2023 for consideration at the fourth session of the OEWG.**

4. **The OEWG Chair is requested to convene an inter-sessional meeting with States, regional and sub-regional organizations and interested stakeholders as appropriate, including businesses, non-governmental organizations and academia, no later than the beginning of the fourth session, to discuss topics which could support and foster confidence-building.**

5. **States are encouraged to continue, on a voluntary basis, to share concept papers, national strategies, policies and programmes, as well as information on ICT institutions and structures with relevance to international security, including through the report of the Secretary-General on developments in the field of information and communication technologies in the context of international security as well as the UNIDIR Cyber Policy Portal as appropriate.**

F. Capacity-Building

17. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on capacity-building efforts on ICTs in the context of international security. The following is a non-exhaustive list of proposals with varying levels of support from States that may be further elaborated upon and supplemented at forthcoming OEWG sessions:

a) The OEWG could encourage the mainstreaming of the principles of capacity-building in relation to State use of ICTs in the context of international security as adopted in the 2021 OEWG report[24] as well as better integrate capacity-building efforts on security in the use of ICTs into the 2030 Sustainable Development Agenda. States concluded that threats may be experienced differently by States according to their levels of digitalization, capacity, ICT security and resilience, infrastructure and development.

b) The value of South-South, South–North, triangular, and regionally focused cooperation was also recalled.[25]

c) The OEWG could promote better understanding of the needs of developing States with the aim of narrowing the digital divide through tailored capacity-building efforts, so as to work towards

[24] Report of the 2021 OEWG, A/75/816, Annex I, para 56.
[25] Report of the 2021 OEWG, A/75/816, Annex I, para 57.

ensuring that all States have the necessary capacity to observe and implement the initial framework for responsible State behaviour in the use of ICTs.

d) Acknowledging the wide range of existing programmes in this space, the OEWG itself could be a platform to continue exchanging views and ideas related to capacity-building efforts on security in the use of ICTs including how best to leverage existing initiatives in order to support States in developing institutional strength to implement the framework of responsible State behaviour in the use of ICTs.

e) Recognizing existing initiatives for funding capacity-building efforts on security in the use of ICTs, States could also consider additional avenues of funding specifically targeted at capacity-building on security in the use of ICTs through potential coordination and integration with existing development programmes and funds.

f) States could continue to raise awareness of the gender dimensions of security in the use of ICTs and promote gender-sensitive capacity-building at the policy level as well as in the selection and operationalization of projects.

g) States recalled the need for a concrete, action-oriented approach to capacity- building. States concluded that such concrete measures could include support at both the policy and technical levels such as the development of national cybersecurity strategies, providing access to relevant technologies, support to Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs) and establishing specialized training and tailored curricula including "training the trainer" programmes and professional certification. The benefits of establishing platforms for information exchange including legal and administrative good practices was recognized, as were the valuable contributions of other relevant stakeholders to capacity-building activities.[26]

h) 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, research, and facilitating access to internet and digital services.

Recommended next steps

1. **States continue exchanging views at the OEWG on capacity-building on security in the use of ICTs.**

2. **States engage in focused discussions at the fourth and fifth sessions of the OEWG on, *inter alia,* (a) funding specifically for capacity-building efforts on security in the use of ICTs through potential coordination and integration with existing development programmes and funds, (b) exchanging views and ideas on capacity-building efforts on security in the use of ICTs, leveraging on existing initiatives, and (c) best practices and lessons learnt on the topic of public-private partnerships on security in the use of ICTs, and (d) the gender dimensions of security in the use of ICTs. Experts could be invited to make presentations on these topics to facilitate further discussion.**

3. **States are encouraged, on a voluntary basis, to survey their capacity needs including through the National Survey of Implementation or other tools.**

[26] Report of the 2021 OEWG, A/75/816, Annex I, para 61.

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

G. Regular Institutional Dialogue

18. States, reaffirming the cumulative and evolving framework for responsible State behaviour in the use of ICTs, made concrete, action-oriented proposals on regular institutional dialogue. This non-exhaustive list of proposals with varying levels of support from States 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 should build incrementally on the previous one. States recognized the centrality of the OEWG as the mechanism within the United Nations for dialogue on security in the use of ICTs.

b) States noted a variety of proposals for advancing responsible State behaviour in the use of ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action (PoA). In considering these proposals, the concerns and interests of all States should be taken into account through equal State participation at the United Nations. In this regard, it was recalled that the PoA should be further elaborated including at the 2021-2025 Open-Ended Working Group process.[27]

Recommended next steps

1. **States continue exchanging views at the OEWG on regular institutional dialogue and on proposals by States to facilitate regular institutional dialogue on the security in the use of ICTs.**

2. **States, at the fourth and fifth sessions of the OEWG, to continue to engage in focused discussions within the framework of the OEWG to further elaborate the PoA with a view towards its possible establishment as a mechanism to advance responsible State behaviour in the use of ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs. 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.**

3. **States in a position to do so to continue to consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the relevant UN processes.[28]**

. . . . .

[27] Report of the 2021 OEWG, A/75/816, Annex I, para 77.
[28] Report of the 2021 OEWG, A/75/816, Annex I, para 79.