United Nations A/AC.290/2021/CRP.2

General Assembly

Conference room paper
10 March 2021

English only

Open-ended working group on developments in the field of information and telecommunications in the context of international security

Final Substantive Report

A. Introduction

1. Despite the radical transformations the world has experienced since the United Nations was founded 75 years ago, its purpose and timeless ideals retain foundational relevance. Alongside the reaffirmation of their faith in fundamental human rights, and their commitment to promote the economic and social advancement of all peoples and to establish conditions for justice and respect of international law, States resolved to unite their strength to maintain international peace and security.[1]

2. Developments in information and communications technologies (ICTs) have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development. ICTs and global connectivity have been a catalyst for human progress and development, transforming societies and economies, and expanding opportunities for cooperation.

3. The imperative of building and maintaining international peace, security, cooperation and trust in the ICT environment has never been so clear. Negative trends in the digital domain could undermine international security and stability, place strains on economic growth and sustainable development, and hinder the full enjoyment of human rights and fundamental freedoms. These trends include the growing use of ICTs for malicious purposes.

4. The current global health crisis has underscored the fundamental benefits of ICTs and our reliance upon them, including for provision of vital government services, communicating essential public safety messages, developing innovative solutions to ensure business continuity, accelerating research, and helping to ensure continuity in education and social cohesion through virtual means. In this time of uncertainty, States, as well as the private sector, scientists and other actors, have leveraged digital technology to keep individuals and societies connected and healthy. At the same time, the COVID-19 pandemic has demonstrated the risks and consequences of malicious activities that seek to exploit vulnerabilities in times when societies are under

[1] Preamble of the Charter of the United Nations.

enormous strain. It has also highlighted the necessity of bridging digital divides, building resilience in every society and sector, and maintaining a human-centric approach.

5. As ICTs can be used for purposes that are inconsistent with the objectives of maintaining international peace, stability and security, the General Assembly has recognized[2] that the dissemination and use of ICTs affect the interests of the entire global community and that broad international cooperation would lead to the most effective responses.

6. In light of the above, the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG), established pursuant to General Assembly resolution 73/27, was an opportunity to advance consideration of this critical issue. It provided a democratic, transparent and inclusive platform for all States to participate, express their views and extend cooperation on the international security dimension of ICTs. The active participation of the UN membership and the engagement of a variety of other relevant stakeholders demonstrates the international community's shared aspiration and collective interest in a peaceful and secure ICT environment for all and their resolve to cooperate to achieve it.

7. The OEWG represents a significant milestone in international cooperation towards an open, secure, stable, accessible and peaceful ICT environment. On six occasions since 2003, groups of governmental experts (GGEs) have been established to study existing and potential threats in the sphere of information security and possible cooperative measures to address them.[3] Through their three consensus reports (2010, 2013 and 2015[4]), which are cumulative in nature, these Groups recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time. Furthermore, specific confidence-building, capacity-building and cooperation measures were recommended. They also 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. In General Assembly resolution 70/237, Member States agreed by consensus to be guided in their use of ICTs by the 2015 GGE report, thereby consolidating an initial framework for responsible State behaviour in the use of ICTs. In this regard, the OEWG also noted General Assembly resolutions 73/27 and 73/266.

8. Building on this foundation and reaffirming this framework, the OEWG has sought common ground and mutual understanding among all Member States of the United Nations on a subject of global consequence. In accordance with its mandate the OEWG discussed existing and potential threats in the sphere of information security and possible cooperative measures to address them; further development of rules, norms and principles of responsible behaviour of States; how international law applies to the use of ICTs by States; confidence-building measures; capacity-building; and the possibility of establishing regular institutional dialogue with broad participation under the auspices of the United Nations. In its effort to build consensus and promote international peace, security, cooperation, and trust, the OEWG's discussions were guided by the principles of inclusivity and transparency.

9. The United Nations should continue to play a leading role in promoting dialogue on the use of ICTs by States. The OEWG recognizes the importance and complementarity of specialized discussions on aspects of digital technologies addressed by other UN bodies and fora.

10. While States bear primary responsibility for the maintenance of international peace and security, all stakeholders have a responsibility to use ICTs in a manner that does not endanger peace and security. As the international security dimension of ICTs cuts across multiple domains and disciplines, the OEWG has benefited from the expertise, knowledge and experience shared by representatives from inter-governmental organizations, regional organizations, civil society,

[2] See, for example A/RES/53/70, pp 6.
[3] A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237, A/RES/73/266.
[4] A/65/201, A/68/98* and A/70/174.

the private sector, academia and the technical community. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich discussion between States and a wide variety of other stakeholders.[5] In addition, these stakeholders have provided concrete proposals and examples of good practice through written contributions and informal exchanges with the OEWG. Some delegations have also conducted multi-stakeholder consultations at their own initiative to inform their contributions to the OEWG.

11. Mindful of the different situations, capacities and priorities of States and regions, the OEWG acknowledges that the benefits of digital technologies are not evenly distributed and that narrowing digital divides, including through universal, inclusive and non-discriminatory access to ICTs and connectivity, remains an urgent priority for the international community.

12. The OEWG welcomes the high level of participation of women delegates in its sessions and the prominence of gender perspectives in its discussions. The OEWG underscores the importance of narrowing the "gender digital divide" and of promoting the effective and meaningful participation and leadership of women in decision-making processes related to the use of ICTs in the context of international security.

13. The OEWG underscores that the individual elements comprising its mandate are interrelated and mutually reinforcing, and together promote an open, secure, stable, accessible and peaceful ICT environment.

B. Conclusions and recommendations

14. Having considered the substantive aspects of the OEWG's mandate, and recalling that General Assembly resolution 73/27 welcomed the effective work of the 2010, 2013 and 2015 Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security and the relevant outcome reports transmitted by the Secretary-General, [6] States reached the following conclusions and recommendations, which include concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment.

Existing and Potential Threats

15. States concluded that they are increasingly concerned about the implications of the malicious use of ICTs for the maintenance of international peace and security, and subsequently for human rights and development. In particular, concern was expressed regarding the development of ICT capabilities for purposes that undermine international peace and security. Harmful ICT incidents are increasing in frequency and sophistication, and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs without accompanying measures to ensure ICT security can bring unintended risks, making societies more vulnerable to malicious ICT activities. Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts.

16. 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.

[5] See "Chair's Summary of the Informal intersessional consultative meeting of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security" available at https://www.un.org/disarmament/open-ended-working-group/

[6] A/65/201, A/68/98 and A/70/174.

17. States also concluded 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, and may increase the likelihood of future conflicts between States.

18. States concluded that there are potentially devastating security, economic, social and humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public. While it is each State's prerogative to determine which infrastructures it designates as critical, such infrastructure may include medical facilities, financial services, energy, water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the general availability or integrity of the Internet, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.

19. States also concluded that ICT activity contrary to 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, could pose a threat not only to security but also to State sovereignty, as well as economic development and livelihoods, and ultimately the safety and wellbeing of individuals.

20. As all States are increasingly reliant on digital technologies, States concluded that a lack of awareness and adequate capacities to detect, defend against or respond to malicious ICT activities may make them more vulnerable. As witnessed during the current global health emergency, existing vulnerabilities may be amplified in times of crisis.

21. States concluded that threats may be experienced differently by States according to their levels of digitalization, capacity, ICT security and resilience, infrastructure and development. Threats may also have a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others.

22. In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, States underscored the urgency of implementing and further developing cooperative measures to address such threats. It was affirmed that acting together and inclusively whenever feasible would produce more effective and far-reaching results. The value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community, was also emphasized in this regard.

23. States emphasized the positive economic and social opportunities that can be derived from ICTs and concluded that it is the misuse of such technologies, not the technologies themselves, that is of concern.

Rules, Norms and Principles for Responsible State Behaviour

24. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. States stressed that such norms reflect the expectations and standards of the international community regarding the behaviour of States in their use of ICTs and allow the international community to assess the activities of States. In accordance with General Assembly resolution 70/237, and acknowledging General Assembly resolution 73/27 States were called upon to avoid and refrain from use of ICTs not in line with the norms for responsible State behaviour.

25. States reaffirmed that norms do not replace or alter States' obligations or rights under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs. Norms do not seek to limit or prohibit action that is otherwise consistent with international law.

26. While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID-19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237.

27. States affirmed the importance of supporting and furthering efforts to implement norms by which States have committed to be guided at the global, regional and national levels.

28. States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.

29. Given the unique attributes of ICTs, States reaffirmed that, taking into account the proposals on norms made at the OEWG, additional norms could continue to be developed over time. States also concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.

The OEWG recommends that

30. States, on a voluntary basis, survey their national efforts to implement norms, develop and share experience and good practice on norms implementation, and continue to inform the Secretary-General of their national views and assessments in this regard.

31. States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection.

32. States, in partnership with relevant organizations including the United Nations, further support the implementation and development of norms of responsible State behaviour by all States. States in a position to contribute expertise or resources be encouraged to do so.

33. States, recalling General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27 take note of proposals made by States on the elaboration of rules, norms and principles of responsible behaviour of States in future discussions on ICTs within the United Nations, noting that resolution 75/240 established an Open-ended Working Group on security of and in the use of information and communications technologies 2021-2025.

International Law

34. Recognizing General Assembly Resolution 70/237, and also acknowledging General Assembly resolution 73/27, which established the OEWG, States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT

environment. In this regard, States were called upon to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations. States also concluded that further common understandings need to be developed on how international law applies to State use of ICTs.

35. States also reaffirmed that States shall seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.

36. States concluded that, given the unique attributes of the ICT environment, deepening common understandings on how international law applies to State use of ICTs, can be developed by exchanging views on the issue among States and by identifying specific topics of international law for further in-depth discussion within the United Nations.

37. In order for all States to deepen their understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus and common understandings within the international community, States concluded that there was a need for additional neutral and objective efforts to build capacity in the areas of international law, national legislation and policy.

The OEWG recommends that

38. States, on a voluntary basis, continue to inform the Secretary-General of their national views and assessments on how international law applies to their use of ICTs in the context of international security, and continue to voluntarily share such national views and practices through other avenues as appropriate.

39. States in a position to do so continue to support, in a neutral and objective manner, additional efforts to build capacity, in accordance with the principles contained in paragraph 56 of this report, in the areas of international law, national legislation and policy, in order for all States to contribute to building common understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community.

40. States continue to study and undertake discussions within future UN processes on how international law applies to the use of ICTs by States as a key step to clarify and further develop common understandings on the issue.

Confidence-building Measures

41. Confidence-building measures (CBMs), which comprise transparency, cooperative and stability measures can contribute to preventing conflicts, avoiding misperception and misunderstandings, and the reduction of tensions. They are a concrete expression of international cooperation. With the necessary resources, capacities and engagement, CBMs can strengthen the overall security, resilience and peaceful use of ICTs. CBMs can also support implementation of norms of responsible State behaviour, in that they foster trust and ensure greater clarity, predictability and stability in the use of ICTs by States. Together with the other pillars of the framework for responsible State behaviour, CBMs can also help build common understandings among States, thereby contributing to a more peaceful international environment.

42. As CBMs are voluntary engagements taken progressively, they can be a first step to addressing mistrust arising from misunderstandings between States by establishing communication, building bridges and initiating cooperation on a shared objective of mutual interest. As such, CBMs may lay the foundations for expanded, additional arrangements and agreements in the future.

43. States concluded that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and

vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs.

44. In addition, States concluded that the UN has a crucial role in the development and supporting implementation of global CBMs. Practical CBMs have been recommended in each of the consensus GGE reports. In addition to these ICT-specific recommendations, in consensus resolution 43/78(H) the General Assembly endorsed the Guidelines for Confidence-building Measures developed in the United Nations Disarmament Commission, which outlined valuable principles, objectives and characteristics for CBMs which may be considered when developing new ICT-specific measures.

45. Building on their essential assets of trust and established relationships, States concluded that regional and sub-regional organizations have made significant efforts in developing CBMs, adapting them to their specific contexts and priorities, raising awareness and sharing information among their members. 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 have CBMs in place, it was noted that such measures are complementary to the work of the UN and other organizations to promote CBMs.

46. Drawing from the lessons and practices shared at the OEWG, States concluded that the prior existence of national and regional mechanisms and structures, as well as the building of adequate resources and capacities, such as national Computer Emergency Response Teams (CERTs), are essential to ensuring that CBMs serve their intended purpose.

47. As a specific measure, States concluded that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a helpful measure for the implementation of many other CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response.

The OEWG recommends that

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

49. States voluntarily identify and consider CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.

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

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

52. States explore mechanisms for regular cross-regional exchanges of lessons and good practices on CBMs, taking into account differences in regional contexts and the structures of relevant organizations.

53. States continue to consider CBMs at the bilateral, regional and multilateral levels and encouraged opportunities for the cooperative exercise of CBMs.

Capacity-building

54. The international community's ability to prevent or mitigate the impact of malicious ICT activity depends on the capacity of each State to prepare and respond. It is of particular relevance to developing States, in order to facilitate their genuine participation in discussions on ICTs in the context of international security and their ability to address vulnerabilities in their critical infrastructure. Capacity-building helps to develop the skills, human resources, policies, and institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies. It plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour, as well as supporting the implementation of CBMs. In a digitally interdependent world, the benefits of capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all.

55. Ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is an important aspect of such cooperation and a voluntary act of both the donor and the recipient.

56. Taking into consideration and further elaborating upon widely accepted principles, States concluded that capacity-building in relation to State use of ICTs in the context of international security should be guided by the following principles:

Process and Purpose

- Capacity-building should be a sustainable process, comprising specific activities by and for different actors.
- Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.
- Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.
- Capacity-building should be undertaken with full respect for the principle of State sovereignty.
- Access to relevant technologies may need to be facilitated.

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.
- As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.
- The confidentiality of national policies and plans should be protected and respected by all partners.

People

- Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.
- The confidentiality of sensitive information should be ensured.

57. States concluded that capacity-building is a reciprocal endeavour, a so-called "two-way street", in which participants learn from each other and where all sides benefit from the general

improvement to global ICT security. The value of South–South, South–North, triangular, and regionally focused cooperation was also recalled.

58. States concluded that capacity-building should contribute to transforming the digital divide into digital opportunities. In particular, it should be aimed at facilitating genuine involvement of developing countries in relevant discussions and fora and strengthening the resilience of developing countries in the ICT environment.

59. States concluded that capacity-building can help to foster an understanding of and address the systemic and other risks arising from a lack of ICT security, insufficient coordination between technical and policy capacities at the national level, and the related challenges of inequalities and digital divides. Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure was deemed to be of particular importance. Capacity-building may also help States to deepen their understanding of how international law applies. Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

60. In addition to technical skills, institution-building and cooperative mechanisms, States concluded that there is a pressing need for building expertise across a range of diplomatic, legal, policy, legislative and regulatory areas. In this context, the importance of developing diplomatic capacities to engage in international and intergovernmental processes was highlighted.

61. 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 cyber security 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.

62. States concluded that taking stock of national efforts with regard to the conclusions and recommendations in this report, as well as the assessments and recommendations Member States agreed to be guided by consensus resolution 70/237, is a valuable exercise to identify progress and where further capacity-building is needed.

The OEWG recommends that

63. States be guided by the principles contained in paragraph 56 in their ICT-related capacity-building efforts in the field of international security, and other actors be encouraged to take these principles into consideration in their own capacity-building activities.

64. States, on a voluntary basis, continue to inform the Secretary-General of their views and assessments on Developments in the field of ICTs in the context of international security and to include additional information on lessons learned and good practice related to capacity-building programmes and initiatives.

65. States, on a voluntary basis, use the model "National Survey of Implementation of United Nations General Assembly Resolution 70/237" (to be made available online) to help them do so. Member States may also wish to use the model survey, on a voluntary basis, to structure their abovementioned submissions informing the Secretary-General of their views and assessments.

66. States and other actors in a position to offer financial, in-kind or technical assistance for capacity-building be encouraged to do so. Further promotion of coordination and resourcing of

capacity-building efforts, including between relevant organizations and the United Nations, should be further facilitated.

67. States continue to consider capacity-building at the multilateral level, including exchange of views, information and good practice.

Regular Institutional Dialogue

68. The OEWG established by General Assembly resolution 73/27 offered, for the first time under the auspices of the United Nations, a dedicated platform for dialogue among all States on developments in ICTs in the context of international security.

69. In addition to its objective to seek common understandings among all States, the OEWG has fostered diplomatic networks and encouraged trust among participants. The broad engagement of non-governmental stakeholders has demonstrated that a wider community of actors is ready to leverage its expertise to support States in their objective to ensure an open, secure, stable, accessible and peaceful ICT environment. The OEWG discussions were an affirmation of the importance of recurrent and structured discussions under UN auspices on the use of ICTs.

70. States concluded that regular dialogue under UN auspices supports the shared objectives of strengthening international peace, stability and prevention of conflicts in the ICT environment. They also concluded that in light of increasing dependency on ICTs and the scope of threats emanating from their malicious use, there was an urgent need to continue to enhance common understandings, build confidence and intensify international cooperation.

71. As States hold primary responsibility for national security, public safety and the rule of law, States affirmed the importance of regular intergovernmental dialogue and of identifying appropriate mechanisms for engagement with other stakeholder groups in future processes.

72. Consideration of developments in ICTs and international security at the United Nations focuses on its international peace, stability and conflict prevention dimensions. States concluded that future regular institutional dialogue should not duplicate existing UN mandates, efforts and activities focusing on the digital dimensions of other issues.[7] States concluded that greater exchange between these forums and First Committee-established processes could help to reinforce synergies and improve coherence, while respecting the expert nature or specialized mandate of each body.

73. States concluded that future dialogue on international cooperation on ICTs in the context of international security should, inter alia, raise awareness, build trust and confidence, and encourage further study and discussion on areas where no common understanding has yet emerged. States recognized the utility of exploring mechanisms dedicated to following-up on the implementation of the agreed norms and rules as well as the development of further ones.

74. States concluded that any future mechanism for regular institutional dialogue under the auspices of the United Nations should be an action-oriented process with specific objectives, building on previous outcomes, and be inclusive, transparent, consensus driven, and results-based.

The OEWG recommends that

75. States continue to actively participate in regular institutional dialogue under the auspices of the United Nations.

[7] See background paper issued by the Chair of the OEWG, "An Initial Overview of UN System Actors, Processes and Activities on ICT-related issues of Interest to the OEWG, By Theme", December 2019, https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-existing-un-bodies-processes-related-to-mandate.pdf.

76. States ensure the continuation of the inclusive and transparent negotiation process on ICTs in the context of international security under the auspices of the United Nations, including and acknowledging the Open-Ended Working Group on security of and in the use of information and communications technologies 2021-2025, established pursuant to General Assembly resolution 75/240.

77. States note a variety of proposals for advancing responsible State behaviour in ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action. 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, the Programme of Action should be further elaborated including at the Open-Ended Working Group process established pursuant to General Assembly resolution 75/240.

78. States consider the conclusions and recommendations of this report in any future processes for regular institutional dialogue under the auspices of the United Nations.

79. States in a position to do so consider establishing or supporting sponsorship programmes and other mechanisms to ensure broad participation in the above UN processes.

C. Final Observations

80. 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.