United Nations A/AC.290/[DATE]

General Assembly

Distr.: Limited

[DATE]

Original: English

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

Draft Substantive Report [Zero Draft]

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 commitment to promote respect for human rights and fundamental freedoms, promote the economic and social advancement of all peoples, and establish conditions for the maintenance of respect for international law, States resolved to unite their strength to ensure international peace and security.

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 for the common good of humankind.

3. The imperative of building and maintaining trust and security in the digital 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 exploitation 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 maintain 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 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[1] 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 an 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 the latest 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.[2] Through their three consensus reports (2010, 2013 and 2015[3]), which are cumulative in nature, these Groups have reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability in the ICT environment. They also 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. 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.

8. Building on this foundation, the OEWG has sought common ground and mutual understanding among all Member States of the United Nations on a subject of global consequence. Its discussions were guided by the principles of inclusivity and transparency, with the aim of building consensus in order to promote and sustain trust. 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.

9. While States are responsible 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, 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

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

wide variety of other stakeholders.[4] *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.*

10. Mindful of the different situations, capacities and priorities of States and regions, the OEWG recognizes that States have both individual and shared responsibilities in the digital domain. The OEWG acknowledges that the benefits of digital technologies are not evenly distributed and that narrowing digital divides, including through wider access to ICTs and connectivity, remains an urgent priority for the international community.

11. 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.

12. The OEWG recognizes the importance and complementarity of specialized discussions on aspects of digital technologies addressed by other UN bodies and fora. These topics include matters related to sustainable development, human rights (including on data protection and privacy, freedom of expression, and freedom of information), digital cooperation, Internet governance, cybercrime and the use of the Internet for terrorist purposes.

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. International law provides a framework for State actions, and norms further define expectations of responsible State behaviour. Measures that build confidence and capacity reinforce adherence to international law, encourage the operationalization of norms, provide opportunities for enhanced cooperation between States, and empower each State to reap the benefits of ICTs for their societies and economies.

14. In light of these synergies, the following sections of the report are complementary and interdependent. Each of the following sections (B-G) starts with a reflection of the views expressed during the substantive discussions of the OEWG, followed by areas of agreement and specific recommendations.

B. Existing and Potential Threats

15. In their discussions at the OEWG, States raised a wide variety of existing and potential threats, which underscored that States may perceive threats emanating from the digital domain in different ways. The inclusive OEWG format offered an opportunity for States to deepen their understanding of how others perceive actions and behaviours in the ICT environment as well as to listen to what others consider as the most significant threats and risks.

[4] 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/

Discussions

16. Some States expressed concern over the development or use of ICT capabilities for military purposes in a manner inconsistent with the objectives of maintaining international peace and security. Some voiced concern that the characteristics of the ICT environment may encourage unilateral measures rather than the settlement of disputes by peaceful means. Concerns were also raised about stockpiling of vulnerabilities as well as a lack of transparency and defined processes for disclosing them, the exploitation of harmful hidden functions, the integrity of global ICT supply chains and ensuring data security. Concerns were raised by some States that ICTs could be used to interfere in their internal affairs, including by means of information operations and disinformation campaigns. Pursuit of increasing automation and autonomy in ICT operations was put forward as a specific concern, as were actions that could lead to the reduction or disruption of connectivity, unintended escalation or effects that negatively impact third parties. Some States also noted the lack of clarity regarding the responsibilities of the private sector as a concern in and of itself.

17. States emphasized that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of technologies, not the technologies themselves, that is of concern. States recognized that even as technological advances and new applications may offer development opportunities, they may also expand attack surfaces, amplify vulnerabilities in the ICT environment or be leveraged for novel malicious activities. Particular technological trends and developments were highlighted in this regard, including progress in machine learning and quantum computing; the ubiquity of connected devices (”Internet of Things“); new ways to store and access data through distributed ledgers and cloud computing; and the expansion of big data and digitized personal data.

Conclusions

18. States agreed 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. Harmful ICT incidents are increasing in frequency, precision and sophistication, and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs 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.

19. States agreed that the continuing increase in incidents involving the malicious use of ICTs by State and non-State actors, including proxies, is a disturbing trend. Some non-State actors have demonstrated ICT capabilities previously only available to States, and concern was expressed that these capabilities could be used for terrorist or criminal purposes.

20. States also agreed that any use of ICTs by States in a manner inconsistent with their Charter commitment to live together in peace with one another as good neighbours, as well as with their other obligations under international law, undermines trust and stability between States, which may increase the risk of misperception and the likelihood of future conflicts between States.

21. States agreed that there are potentially devastating humanitarian consequences of attacks on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public such as medical facilities, energy, water, transportation and sanitation. Attacks on CI and CII that undermine trust and confidence in political and electoral processes,

public institutions, or that impact the financial system, 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.

22. States also agreed that using ICTs to disrupt, damage, or destroy CI and CII poses a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals.

23. States agreed that a lack of awareness and adequate capacities to detect, defend against or respond to malicious ICT activities constitutes a challenge as all countries are increasingly reliant on digital technologies. As witnessed during the current global health emergency, existing vulnerabilities may be amplified in times of crisis.

24. States agreed that threats may be experienced differently by States according to their levels of 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, on vulnerable populations, particular professions, small and medium-sized enterprises, and others.

25. In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, States agreed on 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.

C. International Law

26. Guided by the Group's mandate, with a view to promoting common understandings of how international law applies to the use of ICTs by States, States had an exchange of views on how international law (general principles of law, treaties and customary international law) applies to the international security dimension of ICTs.

Discussions

27. In their discussions at the OEWG, States recalled that international law, and in particular the Charter of the United Nations in its entirety, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. At the same time, States highlighted that further understanding was required on how international law applies to States' use of ICTs.

28. Specific principles of the UN Charter highlighted in the discussion include among others State sovereignty; sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the

United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.[5]

29. It was recalled that international law is the foundation for stability and predictability in relations between States. In particular, international humanitarian law reduces risks and potential harm to both civilians and civilian objects as well as combatants in the context of an armed conflict. At the same time, States underscored that international humanitarian law neither encourages militarization nor legitimizes resort to conflict in any domain.

30. It was also noted that under customary international law, the responsibilities of States with regard to internationally wrongful acts extend to their use of ICTs. It was recalled that States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors acting on the instruction or under the control of a State to commit such acts. The responsibility of States was also noted regarding entities owned by or under the control of the State.

31. States recalled that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State and that accusations of organizing and implementing wrongful acts brought against States should be substantiated.

32. Some States expressed the view that existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of ICTs. It was also proposed that efforts should focus on reaching common understanding on how the already agreed normative framework applies through the development of additional guidance, and can be operationalized through enhancing implementation by all States. At the same time, some States expressed the view that due to the quickly evolving nature of the threat environment and the severity of the risk, an internationally agreed legally-binding framework on ICTs is needed. It was also suggested that such a binding framework may lead to more effective global implementation of commitments and a stronger basis for holding actors accountable for their actions.

33. It was highlighted that while existing bodies of international law do not include specific reference to the use of ICTs in the context of international security, international law can develop progressively, including through opinio juris and State practice. The possibility over time of developing complementary binding measures concurrently with the implementation of norms was raised. Furthermore, a political commitment was proposed as a way forward.

34. While recalling that international law, and in particular the Charter of the United Nations applies in the use of ICTs, it was highlighted that certain questions on how international law applies to the use of ICTs have yet to be fully clarified. Such questions include, inter alia, the kind of ICT-related activity that might be interpreted by other States as a threat or use of force (Art. 2(4) of the Charter) or that might give a State cause to invoke its inherent right to self-defence (Art. 51 of the Charter). They also include questions relevant to how the principles of international humanitarian law, such as principles of humanity, necessity, proportionality, distinction and precaution, apply to ICT operations. In this regard, some States noted that discussions on the applicability of international humanitarian law to the use of ICTs by States needed to be approached with prudence.

[5] A/RES/73/27, pp 16.

35. Also, in terms of ways forward, States proposed that a key first step to clarify and further develop common understandings could emanate from increased exchanges and in-depth discussions by States on how international law applies. It was noted that such exchanges in themselves could serve as an important confidence-building measure. States furthermore proposed several ways to voluntarily share their national views on the issue of international law, including utilizing the annual report of the Secretary-General on developments in the field of information and telecommunications in the context of international security or providing a survey of national practice in the application of international law. The progress made in regional and other arrangements to exchange views and develop common understandings on how international law applies was also highlighted.

36. From the perspective of maintaining peace and preventing conflict, it was noted that greater focus could also be placed on the settlement of disputes by peaceful means and refraining from the threat or use of force. In this context, States recalled existing bodies, mechanisms and tools for the prevention and peaceful settlement of disputes. Some States suggested that developing a universally-accepted, common approach and understanding of the source of ICT incidents at the technical level under the auspices of the United Nations, through the sharing of good practices, bearing in mind respect for the principle of State sovereignty, could lead to greater accountability and transparency, and could help support legal recourse for those harmed by malicious acts.

Conclusions and Recommendations

37. Pursuant to General Assembly Resolution 73/27, which established the OEWG, States affirmed 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. States also agreed that further common understandings need to be developed on how international law applies to State use of ICTs.

38. States also reaffirmed the importance of the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements.

39. States agreed that common understandings on how international law applies to State use of ICTs can be fostered by encouraging exchange of views on the issue among States and by identifying specific topics of international law for further in-depth discussion.

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

The OEWG recommends that

41. States, on a voluntary basis, continue to inform the Secretary-General of their national views and practices on how international law applies to their use of ICTs in the context of international security, to be made available in his annual report on developments in the field of ICTs in the context of international security.

42. States submit, on a voluntary basis, national views and practice on how international law applies to State use of ICTs to the Cyber Policy Portal of the United Nations Institute for Disarmament Research.

43. 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 85 of this report, in the areas of international law, national legislation and policy, in order for all States to develop their own understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community.

44. States continue to undertake discussions at the multilateral level, in order to foster common understandings of how international law applies in the use of ICTs by States in the context of international security, and to consider further initiatives in this regard.

D. Rules, Norms and Principles for Responsible State Behaviour

45. Voluntary, non-binding norms of responsible State behaviour 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 of the international community and set standards regarding the behaviour of States in their use of ICTs.

Discussions

46. In their discussions at the OEWG, States recalled that voluntary, non-binding norms of responsible State behaviour should be viewed as consistent with international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights. States also noted General Assembly resolution 2131 (XX), 1965 entitled “Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty”.

47. States recalled that resolution 70/237, adopted by consensus, calls upon States to be guided in their use of ICTs by the 2015 GGE report, which includes 11 voluntary non-binding norms of responsible State behaviour. Some States underscored that these 11 agreed norms formed the basis of the work of the OEWG, while some States also recalled that General Assembly resolution 73/27 includes a set of 13 rules, norms and principles of responsible behaviour of States. It was recognized that it was the prerogative of States to progressively implement voluntary norms according to their national priorities and capacities.

48. States stressed the need to promote awareness of the existing norms and to support their operationalization in parallel to the development of new norms over time. States underscored the need for guidance on how to operationalize norms. In this regard, States called for the sharing and dissemination of good practices and lessons on norm implementation. Different cooperative approaches were proposed, such as a roadmap developed by States, to assist in their implementation efforts, as well as voluntary surveys for the sharing of lessons and good practices.

49. States recognized that norms can help to prevent conflict in the ICT environment and contribute to ICTs peaceful use and full realization to increase global social and economic development. States highlighted that the implementation of norms should not result in undue

restrictions on international cooperation and technology transfer, nor hinder innovation for peaceful purposes and the economic development of States in a fair and non-discriminatory environment. States also stressed the interlinkages between norms, confidence-building and capacity-building, and underscored the need for gender perspectives to be mainstreamed into norm implementation.

50. During discussion, proposals were made for the further elaboration of existing norms. States reiterated the importance of the protection of critical infrastructure, which should include medical and healthcare facilities. They also drew attention to the importance of cooperating to protect critical infrastructure that crosses borders or jurisdictions, as well as the importance of ensuring the general availability and integrity of the Internet. States recalled General Assembly resolution 64/211 entitled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures".[6] In addition, States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products, and the responsibility to notify users when significant vulnerabilities are identified.

51. Further to the above paragraph, a list of written proposals made by States at the OEWG on the elaboration of existing norms, guidance on implementation as well as new norms were compiled in a non-paper and will be made available online.[7]

52. States also noted the proposal for an international code of conduct for information security tabled in 2015.[8]

53. States recognized the need to encourage and support further regional efforts as well as partnerships with other stakeholders such as the private sector and the technical community on the implementation of norms. Such partnerships could be built, for example, to ensure sustainable capacity-building efforts to address differences in implementation capacities. States could be called on to take the necessary outreach and cooperative steps to ensure that various stakeholders, including the public and private sectors and civil society, uphold their responsibilities in the use of ICTs.

Conclusions and Recommendations

54. States agreed that norms do not replace or alter States' obligations under international law, which are binding, but rather provide additional specific guidance on what constitutes responsible State behaviour in the use of ICTs.

55. States agreed that the COVID-19 pandemic accentuated the importance of protecting healthcare infrastructure including medical services and facilities as part of the norms addressing critical infrastructure.

56. States agreed on the importance of supporting and furthering efforts to implement norms at the global, regional and national levels.

57. 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

[6] Annexed to this resolution is a Voluntary self-assessment tool for national efforts to protect critical information infrastructures.
[7] https://www.un.org/disarmament/open-ended-working-group/
[8] A/69/723, referenced in A/70/174, para 12.

also agreed 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

58. States, on a voluntary basis, survey their national efforts to implement norms, and continue to inform the Secretary-General of these national surveys to be made available through his annual report on developments in the field of ICTs in the context of international security. States further requested the UN Secretariat to compile information from these surveys in support of capacity-building efforts.

59. States, in partnership with relevant organizations including the United Nations, develop further voluntary guidance on the implementation of norms of responsible State behaviour, and widely disseminate this voluntary guidance at national, regional, interregional and global levels. States in a position to contribute expertise or resources to the development and dissemination of such guidance be encouraged to do so.

60. States, taking into account resolution 70/237 and resolution 73/27 as well as, where appropriate, the non-paper of proposals made by States at this OEWG referred to in paragraph 51, continue to consider and undertake discussions at the multilateral level on international rules, norms and principles of responsible behaviour of States in the use of ICTs in the context of international security, including their implementation.

E. Confidence-building Measures

61. Confidence-building measures (CBMs), which comprise transparency, cooperative and stability measures can contribute to preventing conflicts, avoiding misperception and misunderstandings, and provide a "safety valve" for 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.

62. As CBMs are voluntary engagements taken progressively, they can be a first step to addressing mistrust 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 or more structured arrangements and agreements in the future.

Discussions

63. In their discussions at the OEWG, States noted the continuing relevance of the CBMs recommended in the consensus GGE reports. Several measures were highlighted as requiring

priority attention, such as regular dialogue and voluntary information exchanges on existing and emerging threats, national policy or doctrine, national views on how international law applies to State use of ICTs, and national approaches to defining critical infrastructure and categorizing ICT-related incidents. Sharing of good practices in approaches to digital forensics and investigation of malicious cyber incidents could both increase cooperation and build capacity. The value of developing shared understanding of concepts and terminology was also highlighted as a practical step for furthering international cooperation and building trust. Other such measures included developing guidance on the implementation of CBMs, training for diplomats, exchanging lessons on establishing and exercising secure crisis communication channels, personnel exchanges, scenario-based exercises at the policy level as well as operational exercises at the technical level between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs). National transparency measures, such as voluntarily sharing responses to an implementation survey or issuing national declarations of adherence to the framework for responsible State behaviour, are other avenues to build trust and confidence regarding the intentions and commitments of States.

64. Taking into account the experiences of regional bodies with establishing and maintaining Points of Contact (PoC) networks, and building on existing networks, the viability of establishing a central global directory of PoCs was discussed. At the same time, it was noted that the security of such a directory as well as its operational modalities would be crucial to its effectiveness, as would avoiding duplicative or overly detailed arrangements. The value of regularly conducting exercises among a network of PoCs was also emphasized, as it can help to maintain readiness and responsiveness and ensure that PoC directories remain updated.

65. As CBMs can be developed at the bilateral, regional or multilateral levels, States also discussed the desirability and viability of establishing a global repository of CBMs under the auspices of the United Nations, with the objective of sharing policy, good practice, experiences and assessments of CBM implementation, and encouraging peer learning and investment in capacity-building. Such a repository could also assist States to identify additional CBMs appropriate to their national and regional contexts and offer potential models for adaptation elsewhere. It was noted that any new global repository should not duplicate existing arrangements and that operational modalities would need to be further discussed.

66. States also drew attention to the roles and responsibilities of other actors, including civil society, the private sector, academia and the technical community, in contributing to building trust and confidence in the use of ICTs at the national, regional and global levels. States noted the variety of multi-stakeholder initiatives that, through the development of principles and commitments, have established new networks for exchange, collaboration and cooperation. In a similar vein, sector- or domain-specific initiatives have demonstrated the growing awareness of the roles and responsibilities of other actors and the unique contributions that they can make to ICT security through voluntary commitments, professional codes and standards.

Conclusions and Recommendations

67. States agreed 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.

68. In addition, States agreed 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.

69. Building on their essential assets of trust and established relationships, States agreed 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.

70. Drawing from the lessons and practices shared at the OEWG, States agreed 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.

71. As a specific measure, States agreed that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a prerequisite 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

72. States, on a voluntary basis, continue to inform the Secretary-General of their views and assessments to be made available in his annual report 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 relevant CBMs at the bilateral, regional or multilateral level.

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

74. As a CBM, States publicly re-affirm their commitment to be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts[9].

75. 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.

76. States, which have not yet done so, nominate 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.

[9] A/70/174, refer also to A/RES/70/237.

77. 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.

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

F. Capacity-building

79. 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. 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. Capacity-building is an important aspect of international cooperation and a voluntary act of both the donor and the recipient. 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.

Discussions

80. In their discussions at the OEWG, States emphasized the important function that capacity-building can play in empowering all States and other relevant actors to fully participate in the international discussions on the framework for responsible State behavior, while also contributing to shared commitments such as the 2030 Sustainable Development Agenda[10]. In this regard, States stressed the need for sufficient financial and human resources to be allocated to capacity-building programmes.

81. States highlighted the important work that has been undertaken in ICT-related capacity-building by other actors, including international organizations, regional and sub-regional bodies, civil society, the private sector, academia and specialized technical bodies, and they encouraged reflection on how to promote coordination, sustainability, effectiveness and reduction of duplication across these efforts.

82. The United Nations has an essential role to play in supporting States to raise the profile of capacity-building and by leveraging its convening power to support greater coordination of the variety of actors active in capacity-building. States suggested that existing platforms within the United Nations, its specialized agencies and in the wider international community could be used to strengthen already established coordination. These platforms could be used to share national views on capacity-building requirements, encourage the sharing of lessons and experiences from both recipients and providers of support, and facilitate access to information on capacity-building and technical assistance programmes. These platforms could also support the mobilization of

[10] Examples of relevant SDG goals and targets include, but are not limited to, the following: Significantly increase access to information and communications technology (9.C); Enhance North-South, South-South and triangular regional and international cooperation on and access to science, technology and innovation (17.6) and; Enhance international support for implementing effective and targeted capacity-building (17.9).

resources or assist with pairing available resources with requests for capacity-building support and technical assistance. It was suggested that the development of a global cyber capacity-building agenda under the auspices of the United Nations could help to ensure greater coherence in capacity-building efforts and that voluntary self-assessment surveys may help States to identify and prioritize their capacity-building needs or ability to provide support.

83. While recalling the primary responsibility of States for maintaining a secure, safe and trusted ICT environment, the importance of a multi-stakeholder approach to capacity-building that addresses technical and policy gaps in all relevant sectors of society was also emphasized. States noted in particular that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, the technical community, academic institutions and private sector actors and through the creation of expert rosters and hubs. In this regard, it was also emphasized that national approaches to ICT security could benefit from adopting a cross-sectoral, holistic and multi-disciplinary approach to capacity-building, including by enhancing national coordination bodies with the participation of relevant stakeholders to assess the effectiveness of programmes. Such an approach may also help address challenges posed by newly emerging technologies.

84. States called attention to the "gender digital divide" and urged that specific measures be taken at the national and international levels to address gender equality and the meaningful participation of women in international discussions and capacity-building programmes on ICTs and international security, including through the collection of gender-disaggregated data. States expressed appreciation for programmes that have facilitated the participation of women in multilateral ICT-security discussions. The need to strengthen linkages between this topic and the United Nations Women, Peace and Security agenda was also emphasized.

85. States noted that many obstacles hinder or reduce the effectiveness of capacity-building. Insufficient coordination and complementarity in the identification and delivery of capacity-building efforts were highlighted as significant concerns. States also raised practical concerns related to the identification of capacity-building needs, timeliness of response to requests for capacity-building assistance, as well as in the design, delivery, sustainability and accessibility of capacity-building activities, and the lack of specific metrics to measure their impact. In many contexts, insufficient human, financial and technical resources impedes capacity-building efforts and progress to narrow the digital divide. Once capacity has been built, some countries face the challenge of talent retention in a competitive market for ICT professionals. States mentioned that lack of access to ICT security-related technologies was also an issue.

Conclusions and Recommendations

86. Ensuring an open, secure, stable, accessible and peaceful ICT environment is a common but differentiated responsibility that requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is a crucial element of such cooperation. Taking into consideration and further elaborating upon widely accepted principles, States agreed 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.

87. States agreed that capacity-building is a shared responsibility as well as 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.

88. States agreed 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. Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

89. In addition to technical skills, institution-building and cooperative mechanisms, States agreed 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.

90. States recalled the need for a concrete, action-oriented approach to capacity-building. States agreed 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 centres of excellence and other mechanisms for information exchange including legal and administrative good practices was recognized.

The OEWG recommends that

91. States be guided by the principles contained in paragraph 86 in their ICT-related capacity-building efforts in the field of international security.

92. 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.

93. 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.

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

G. Regular Institutional Dialogue

95. 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 open to all States on developments in ICTs in the context of international security.

96. In addition to its objective to seek common understandings among all States through substantive exchanges as reflected in the previous sections of this report, 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, as also recognized by the consensus reports of the GGE.

Discussions

97. In their discussions at the OEWG, States recalled the OEWG's mandate in General Assembly resolution 73/27 to study the possibility of establishing regular institutional dialogue and confirmed that the OEWG's assessments and recommendations in this regard would be a central outcome of its work.

98. States expressed a range of views regarding the objectives that should be the priority for future regular institutional dialogue and which format of regular dialogue could best support these objectives. Some States expressed the desire for regular dialogue to prioritize implementation of existing commitments and recommendations, including developing guidance to support and monitor their implementation; coordinating and strengthening the effectiveness of capacity-building; and identifying and exchanging good practices. Other States expressed the desire for regular dialogue to prioritize the further development of existing commitments and elaboration of additional commitments, including the negotiation of a legally binding instrument and the institutional structures to support it.

99. Some States made a specific proposal on the establishment of a Programme of Action (PoA) for advancing responsible State behaviour in cyberspace with a view to establishing a permanent UN forum to consider the use of ICTs by States in the context of international security. It was proposed that the PoA would constitute a political commitment by States to agreed recommendations, norms and principles; convene regular meetings focused on implementation; enhance cooperation and capacity-building among States; and hold regular review conferences. Broad participation and consultations were also foreseen under the PoA proposal.

100. States also expressed the desire for the international community to ultimately return to a single process anchored in consensus and global support from the outset so as to ensure collective ownership of the process. In this regard, States noted that different proposed formats for dialogue are not necessarily mutually exclusive. It was suggested that different formats could be complementary or could be merged in order to capitalize on the unique features of each and reduce duplication of efforts. It was proposed that the OEWG could develop a roadmap that would identify priority themes and topics and a timeline for future regular institutional dialogue.

101. In addition, the need for further consideration of the duration and sustainability of future dialogue, whether it should be of a deliberative or action-oriented nature, its timing, potential locations, and budgetary considerations were also raised.

102. Consideration of developments in ICTs and international security at the United Nations focuses on its international peace, stability and conflict prevention dimensions and thus has been pursued under the First Committee of the General Assembly. Other UN bodies are mandated to consider the digital dimensions of other issues, including terrorism, crime, development and human rights, as well as Internet governance. It was suggested 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.

103. While recognizing the unique role and responsibility of States in relation to national and international security, States underscored the important contribution that responsible behaviour by other actors makes to an open, secure, accessible, and peaceful ICT environment. Building a more resilient and secure ICT environment may be facilitated by increased multi-stakeholder cooperation and partnerships.

Conclusions and recommendations

104. States agreed that in light of increasing dependency on ICTs and the scope of threats emanating from their misuse, there was an urgent need to enhance common understandings, build confidence and intensify international cooperation.

105. States agreed that regular dialogue supports the shared objectives of strengthening international peace, stability and prevention of conflicts in the ICT environment.

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

107. States agreed that regular institutional dialogue established through First Committee should remain focused on international peace and security so as not to duplicate existing UN mandates, efforts and activities focusing on the digital dimensions of other issues, including terrorism, crime, development, human rights and Internet governance.[11]

108. States agreed 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.

109. States agreed that 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.

110. Having considered the substantive aspects of its mandate as reflected in sections B to F of this report, States recommended under each section a list of concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment. States also agreed on the need for further dialogue including the sharing of national views or good practices on issues relating to how international law applies in the use of ICTs; the implementation of norms and their further development over time; as well as the development and implementation of confidence building and capacity building measures.

The OEWG recommends that

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

112. States establish a programme to continue to take forward existing agreements and commitments in their use of ICTs as set out in relevant General Assembly resolutions, in particular 70/237, as well as the conclusions and recommendations of this OEWG. Such discussions would take place under the First Committee of the United Nations General Assembly as a Programme of Action for advancing responsible State behaviour in cyberspace.

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

114. 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.

[11] 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.

H. Final Observations

115. The OEWG presented a historic opportunity for all States to engage in focused and sustained discussions, under the auspices of the United Nations, on matters related to ICTs and international security. In addition to the many areas of agreement reflected in this report, through its inclusive and transparent discussions, the OEWG has served as a valuable measure to build trust, confidence and understandings between States, as well as helped to establish a global diplomatic network of national experts. The active and broad engagement of all delegations has demonstrated the determination of States to continue to work together on this subject of fundamental importance to all.

116. The formal, informal and virtual sessions of the OEWG were characterized by substantive, interactive exchanges among States, as well as with civil society, the private sector, academia and the technical community. The commitment demonstrated by States and other stakeholders throughout the work of the OEWG, with growing engagement even as some of its meetings transitioned to a virtual format, is an undeniable indication of the increasingly universal relevance of the topics under its consideration as well as the growing recognition of the urgent need to collectively address the threats to international security posed by the malicious use of ICTs.

117. The OEWG has demonstrated the international community's collective resolve to continue to work together towards an open, secure, stable, accessible and peaceful ICT environment of benefit to all States and peoples. Throughout their deliberations at the OEWG, States underscored the linkages and synergies between each of the elements of its mandate: Voluntary, non-binding norms reinforce and complement existing obligations under international law. Both these elements define expectations of behaviour regarding State uses of ICTs in the context of international security. In this way, they also contribute to confidence-building by increasing transparency and cooperation between States and for reducing the risk of conflict. Capacity-building in turn is an enabler for all States to contribute to increased stability and security globally. Together, these elements constitute a global framework of cooperative measures to address existing and potential threats in the sphere of ICTs. Regular institutional dialogue will provide the opportunity for this framework to be further developed and operationalized through advancing common understandings, exchanging lessons learned and good practices in implementation, building confidence and increasing capacity amongst States.