Second "Pre-draft" of the report of the OEWG on developments in the field of information and telecommunications in the context of international security

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, transforming societies and economies, and expanding opportunities for cooperation for the common good of humankind.*

3. *The imperative of 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, which may inhibit securing the benefits of ICTs.*

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, innovative solutions to ensure business continuity, accelerating research, and the possibility 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 dual-use technologies, ICTs can be used for purposes that are inconsistent with the objectives of maintaining international stability and security. In recognition of the increasing relevance and potential impact of developments in the field of ICTs on international security, in 2003 the General Assembly requested the Secretary-General to study, with the assistance of a group of governmental experts, existing and potential threats in the sphere of information security and possible cooperative measures to address them.[1] Between 2004 and 2017, five Groups of Governmental Experts (GGEs) were convened, and a sixth GGE will report to the General Assembly at its 76th session.*

6. *The three consensus reports adopted by the GGEs (2010, 2013 and 2015[2]) are cumulative in nature and constitute important milestones in international cooperation towards an open, secure, stable, accessible and peaceful ICT environment. Over time, these Groups have generated a growing body of common understanding of the threats posed by the use of ICTs in matters related to international peace and security, and of States' commitments to address these threats through a*

[1] A/RES/58/32.
[2] A/65/201, A/68/98* and A/70/174.

framework of international law, voluntary norms and confidence-building measures, underpinned by capacity-building and cooperation.

7. *In resolution 70/237, Member States agreed by consensus to be guided in their use of ICTs by the 2015 report, thereby consolidating an initial framework for responsible State behaviour in the use of ICTs. Notably, the 2015 report 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. The 2015 report also recommended 11 norms of responsible State behaviour and recognized that additional norms could be developed over time.*

8. *From its very first resolution on this topic in 1998,[3] the General Assembly recognized 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. Building on the foundation of the consensus GGE reports and their recommendations, 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 ICTs in the context of international security. It provided an inclusive platform for all Member States to participate, express their views and extend cooperation on the international security dimension of ICTs.*

9. *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 promoting and sustaining 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.*

10. *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, a wide range of non-governmental stakeholders contribute to the shared objective of an open, secure, stable, accessible and peaceful ICT environment. Further development of a shared understanding of the roles, responsibilities and potential of other stakeholders to support and strengthen responsible behaviour in the use of ICTs is needed.*

11. *A wealth of expertise is held by other stakeholders on specific issues within the OEWG's mandate. Drawing upon this knowledge and experience, the OEWG has benefited from exchanges with representatives from inter-governmental organizations, regional organizations, non-governmental organizations, the private sector and academia. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich discussion between States and other stakeholders.[4] Views also have been collected through domestic multi-stakeholder consultations. In addition, stakeholders have provided concrete proposals and examples of good practice through written contributions and informal exchanges with the OEWG.*

[3] A/RES/53/70.

[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" in Annex.

12. *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.*

13. *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.*

14. *The OEWG recognizes the importance and complementarity of specialized discussions in other UN bodies and fora on aspects of digital technologies outside of the OEWG's mandate. These topics include matters related to digital cooperation, Internet governance, sustainable development, and human rights (including on data protection and privacy, freedom of expression, and freedom of information), as well as cybercrime and the use of the Internet for terrorist purposes.*

15. *The OEWG recognizes that the individual elements comprising its mandate are interrelated and mutually reinforcing. Together they form a global framework for promoting an open, secure, stable, accessible and peaceful ICT environment. International law and norms regulate and guide State behaviour; confidence-building measures help to create trust and stability in relations between States; and capacity-building helps States adhere to their international commitments and create a resilient, secure and peaceful ICT environment. 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.*

16. *In light of these synergies, the following sections of the report are complementary and interdependent. Sections B-G reflect the substantive discussions of the OEWG. Section H contains its recommendations.*

B. Existing and Potential Threats

Despite the invaluable benefits of ICTs for humanity, their malicious use can have significant and far-reaching negative impacts. There is growing concern about the implications of the malicious use of ICTs for the maintenance of international peace and security, the enjoyment of human rights, and economic and social 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.

17. In their discussions at the OEWG, States expressed concern at the malicious use of ICTs carried out by State actors, including the possible use of proxies. It was also noted that 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.

18. States highlighted as a central threat the possibility that ICTs could be used by States in a manner inconsistent with their Charter commitment to live together in peace with one another as good neighbours, as well as their obligations under international law. Such behaviour undermines trust and stability between States and could increase the risk of misperception. The concern was also raised that absent a culture of restraint, the use of ICTs in future conflicts between States may

become more likely. Additional concerns were conveyed regarding interference in the internal affairs of States through the use of ICTs, including by means of information operations and disinformation campaigns. A wide variety of other existing and potential threats were raised in discussions, underlining that States may perceive threats emanating from the digital domain in different ways. Concerns were expressed over the development or use of ICT capabilities, as well as stockpiling or non-disclosure of vulnerabilities, for military purposes inconsistent with the objectives of maintaining international stability and security. Concerns were also noted about the exploitation of harmful hidden functions and the integrity of global ICT supply chains. Pursuit of increasing automation and autonomy in ICT operations was put forward as a specific concern, as was reduction or disruption of connectivity, or the potential for unintended escalation or effects that negatively impact third parties.

19. States underscored that a lack of awareness and adequate capacities to detect, resist or respond to malicious activities constitutes a threat in and of itself 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.

20. It was noted that threats may 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 enterprises, and others. Threats may also be experienced differently by States according to their levels of capacity, ICT security and resilience, infrastructure and development.

21. States confirmed that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of such technologies, not the technologies themselves, that is of concern. Nonetheless, it was recognized that technological advances and new applications may expand attack surfaces, amplify vulnerabilities in the ICT environment or be leveraged for novel malicious activities. Particular technological trends 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.

22. States underscored that attacks on critical infrastructure (CI) and critical information infrastructure (CII) pose a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals. The potentially devastating human cost of attacks on CI and CII supporting essential services to the public such as medical facilities, energy, water and sanitation, were stressed. 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.

23. States observed that CI and CII are defined differently in accordance with national prerogatives and priorities. In many States such infrastructure is owned, managed or operated by the private sector. In addition, CI and CII may be shared or networked with another State or operated across different States and jurisdictions (sometimes categorized as transborder, transnational or supranational infrastructure). As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.

24. In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, the OEWG underscored the urgent need for States to further develop, through multilateral forums, 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 with the private sector, civil society and academia was also emphasized in this regard.

25. Sections C–G reflect the OEWG's discussions of how the international community might actively strengthen its collective resolve to address these threats.

C. International Law

Existing obligations under international law, in particular the Charter of the United Nations in its entirety, are applicable to State use of ICTs. Furthering shared understandings among States on how international law applies to the use of ICTs is fundamental for international security and stability. Such shared understandings can be fostered by encouraging exchange of views on the issue among States and by identifying specific topics of international law for more in-depth discussion.

26. In their discussions at 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.

27. Specific principles of the UN Charter highlighted include 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.

28. Guided by the Group's mandate to continue to study, 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 the relevance and applicability of international law (general principles of law, treaties and customary international law), to the international security dimension of ICTs, including international humanitarian law, international human rights law, international criminal law.

29. During the exchange, it was noted 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 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 reaffirmed 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 to commit such acts.

31. During discussions, various views were expressed on the application of international law in the use of ICTs. It was proposed 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, proposals were made for the development of a legally-binding instrument on the use of ICTs by

States as the quickly evolving nature of the threat environment and the severity of the risk may require a stronger, internationally agreed framework. It was also proposed 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.

32. It was highlighted that certain questions on how international law applies in the use of ICTs have yet to be fully clarified. Such questions include, *inter alia,* what kind of ICT-related activity might be interpreted by other States as a threat or use of force (Art. 2(4) of the Charter) or 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 the context of armed conflict. In this regard, it was noted that discussions on the applicability of international humanitarian law to the use of ICTs by States needed to be approached with prudence.

33. It was suggested 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 its practical application. The possibility of developing complementary binding measures concurrently with the implementation of norms was raised. A political commitment,[5] supported by regular meetings and voluntary State reporting, was also suggested as a possible middle ground approach.

34. Also in terms of ways forward, States proposed that a key first step to further develop and clarify common understandings could emanate from increased exchanges and in-depth discussions by States to generate consensus on the application of international law. It was noted that such exchanges in themselves could serve as an important confidence-building measure. States furthermore proposed several ways to 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 the creation of a global repository of State practice in the application of international law. During discussions, the progress made in regional and other arrangements to exchange views and develop common understandings on how international law applies was also highlighted.

35. In addition, it was proposed that guidance notes for use on a voluntary basis could be developed by States in the future to enhance common understanding on how existing international law applies to the use of ICTs by States, taking into consideration the specific characteristics of the ICT domain.

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 and mechanisms for the settlement of disputes, including the Security Council and the International Court of Justice. It was suggested that developing a common approach and understanding of the source of ICT incidents at the technical level 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.

[5] An example of such a politically-binding commitment is the 2001 UN Programme of Action to Prevent, Combat and Eradicate the Illicit Trade in Small Arms and Light Weapons (PoA) is a globally agreed framework for activities to counter the illicit trade in small arms and light weapons. See https://www.un.org/disarmament/convarms/salw/programme-of-action/.

37. 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, it was stressed that there was a strong need for additional efforts to build capacity in the areas of international law, national legislation and policy.

D. Rules, Norms and Principles for Responsible State Behaviour

Voluntary, non-binding norms reflect the expectations of the international community and set standards regarding the acceptable and unacceptable behaviour of States in their use of ICTs. They play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. 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. In 2015, the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which sets out 11 voluntary, non-binding norms of responsible State behaviour.

Alongside international law, voluntary non-binding norms complement confidence-building and capacity-building measures and related efforts to promote an open, secure, stable, accessible and peaceful ICT environment.

38. In their discussions at the OEWG, States reiterated that voluntary, non-binding norms of responsible State behaviour are 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 affirmed that norms play an important role in preventing conflict. States highlighted that norms should not place undue restrictions on international cooperation and technology transfer, nor hinder innovation for peaceful purposes and the economic development of States. States also stressed the interlinkages between norms, confidence-building and capacity-building, and urged that gender perspectives be mainstreamed into norm implementation. States noted that given the unique attributes of ICTs, additional norms could be developed over time.

39. States reaffirmed the 11 voluntary, non-binding norms of responsible State behaviour of the 2015 GGE report,[6] recalling that consensus resolution 70/237 calls upon States to be guided in their use of ICTs by the 2015 GGE report, which includes those norms. States at the same time recalled that in General Assembly resolution 73/27, States welcomed a set of 13 rules, norms and principles of responsible behaviour of States, which encompass therein the 11 norms of the 2015 GGE report.

40. Attention was drawn to the international code of conduct for information security tabled in 2015.[7] States also recalled General Assembly resolutions 2131 (XX), 1965 entitled "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty" and 58/199 entitled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures".

41. States stressed the need to promote awareness of the existing norms and support their operationalization. While these norms articulate what actions States should or should not take, States underscored the need for guidance on how to operationalize them. In this regard, States called for the sharing and dissemination of good practices and lessons on norm implementation.

[6] A/70/174, paragraph 13.
[7] A/69/723.

Different cooperative approaches were also proposed, such as developing a roadmap to assist States in their implementation efforts and surveys for the sharing of good practices.

42. States also made proposals for the enhancement as well as further elaboration of norms. Such proposals included, *inter alia*, that States affirm their commitment to a culture of restraint and to international peace and security in their use of ICTs; that States reaffirm their primary responsibility for maintaining a secure, safe and trustable ICT environment; that the general availability or integrity of the public core of the Internet should be protected; and that States should not conduct ICT operations intended to disrupt the infrastructure essential to political processes or to harm medical facilities. 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. States also highlighted that the protection of transborder critical information infrastructure, as a distinct category of critical infrastructure, is the shared responsibility of all States.

43. *[placeholder: additional proposals by Member States under agenda item "Rules, norms and principles" could be introduced here]*

44. The role of regional organizations was recognized in norms implementation. The need to encourage further partnerships and joint efforts with other stakeholders such as the private sector on the implementation of norms was also recognized. Such partnerships could, for example, be built to ensure sustainable capacity-building efforts to address differences in implementation capacities. States could be called on to take the necessary outreach, cooperation and, where necessary, regulatory steps to ensure that various stakeholders, including the public and private sectors and civil society, uphold their responsibilities.

E. Confidence-building Measures

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. CBMs, supported by adequate capacities, can strengthen the overall security, resilience and peaceful use of the ICT environment. CBMs can 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 normative framework, CBMs can also help build common understandings among States, thereby contributing to a more peaceful international environment in the longer term.

In addition to the recommendations on CBMs contained in the consensus GGE reports, the OEWG acknowledged the role of the UN in the development and implementation of global CBMs, and at the same time recognized that regional bodies have developed or adapted CBMs to address specific priorities of their members. The 1988 Guidelines for Confidence-building Measures developed by the UN Disarmament Commission and endorsed by the General Assembly in consensus resolution 43/78 (H) also contain principles, objectives and characteristics for CBMs that remain relevant today.

45. In their discussions at the OEWG, States reaffirmed the value of CBMs in increasing transparency, predictability and stability. They also highlighted the need to translate confidence-building measures into concrete actions that are implementable by all States.

46. States noted the continuing importance of the CBMs recommended in the consensus GGE reports. Several measures were highlighted for 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 or categorizing ICT-related incidents. Other such measures included developing guidance on the implementation of CBMs, training for diplomats, exchanging lessons on establishing and exercising secure crisis communication channels, 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).

47. States highlighted 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 normative framework that guides the use of ICTs by States. It was noted that national declarations of adherence to the normative framework of responsible State behaviour could build trust and confidence between States.

48. In particular, States stressed 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. It was suggested that a global directory of Points of Contact would be useful and could take into account the experiences from regional bodies in this area. 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. The value of regularly conducting exercises among a network of PoCs was also emphasized, as it can help to maintain readiness as well as responsiveness and ensure that PoC directories remain updated.

49. As CBMs can be developed at the bilateral, regional or global level, States proposed the establishment of a global repository of CBMs, with the objective of sharing policy, good practice, experiences and assessments with CBM implementation and encouraging peer learning. Such a repository could also assist States to identify additional CBMs appropriate to their national and regional contexts.

50. Drawing from the lessons and practices shared at the OEWG, States emphasized 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.

51. States underscored the significant efforts of regional and sub-regional bodies in developing CBMs, adapting them to their specific contexts, as well as the crucial awareness raising and information sharing role that regional, cross-regional or inter-organizational exchanges have served, which in themselves build confidence between States. It was noted that, as not all States are members of a regional organization and not all regional organizations have CBMs in place, it is important that other fora be used to promote CBMs as well. States also proposed that some CBMs developed at the regional level could serve as useful models for adaptation in wider contexts.

52. States drew attention to the roles and responsibilities of other actors, including the private sector, academia and civil society, in contributing to building trust and confidence in the use of ICTs at 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.

F. Capacity-building

Capacity-building helps to develop the skills, define the policies and build the institutions that increase the resilience and security of States so they can fully enjoy the benefits of digital technologies and sustainable development. 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 can also support adherence to binding or voluntary commitments. In a digitally interdependent world, the benefits of capacity-building "spill over" national borders and thereby contribute to a more secure and stable ICT environment for all.

53. In their discussions at the OEWG, States reiterated the recommendations on international cooperation and capacity-building in the consensus GGE reports. They emphasized the important function that capacity-building can play in empowering all States and other relevant actors to fully participate in the global normative framework and related intergovernmental processes, while also contributing to shared commitments such as the 2030 Sustainable Development Agenda. In addition, capacity-building plays an important enabling function for promoting adherence to international law and the implementation of norms of responsible State behaviour and the CBMs recommended by the previous GGEs, while also offering important opportunities for building understanding between and within States.

54. States noted that capacity-building can help to address the systemic and transnational 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 transborder critical information infrastructure was deemed to be of particular importance.

55. There was a general acknowledgement that in addition to technical skills, institution-building and cooperative mechanisms, 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.

56. States also highlighted the important work that has been undertaken in ICT-related capacity-building, including by States, international organizations, regional and sub-regional bodies, specialized technical bodies, the private sector and non-governmental organizations. At the same time, many challenges were identified that hinder or reduce the effectiveness of capacity-building. Insufficient coordination and complementarity in the identification and delivery of capacity-building efforts were highlighted as a significant concern. States also raised practical challenges related to the identification of capacity-building needs, as well as in the design, delivery, sustainability and accessibility of capacity-building activities, and the lack of specific metrics to measure their impact. 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.

57. 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 a crucial

element of such cooperation. In their discussions at the OEWG, States recognized the importance of the following principles:

Partnerships

- Capacity-building should be demand-driven, corresponding to nationally identified needs and priorities, and 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 a shared responsibility to collaborate in their design, execution and evaluation.

People

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

Process

- Building capacity is a sustained process comprising discrete 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 unconditional.
- Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

58. States stressed 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 and triangular cooperation was also recalled.

59. The importance of a multi-stakeholder approach to capacity-building that addresses technical and policy gaps in all relevant sectors of society was highlighted. States noted in particular that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, academic institutions and private sector actors. 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 establishing national coordination bodies with the participation of relevant stakeholders to assess the effectiveness of programs. Such an approach may also help address challenges posed by newly emerging technologies.

60. To address the need for greater coordination in capacity-building efforts, States suggested that existing platforms within the United Nations and in the wider global community could be used to strengthen coordination and avoid duplication. 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 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 capacity-building agenda would help to ensure greater coherence in capacity-building efforts.

61. 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.

G. Regular Institutional Dialogue

The growing interest of the international community in the issue of ICTs in the context of international security underlines its relevance to all States. The three consensus GGE reports have all called attention to the need for regular dialogue on the international security dimension of ICTs.[8] Through the OEWG, many States participated for the first time in inclusive discussions under United Nation auspices on this topic. The OEWG, as an open and transparent process, has enlarged appreciation of the different perceptions of threats and priorities, and initiated the process of finding common understandings among all States. It has been a valuable measure to build confidence between States as well as establish a global diplomatic network of national experts. The active and broad engagement of all delegations has demonstrated the commitment of Member States to continue to work together on this subject of fundamental importance to all.

62. Since 1998, consideration of developments in ICTs and international security at the United Nations has been pursued under the purview of the First Committee, and thus focused on its international peace, stability and conflict prevention dimensions. The importance of recurrent and structured discussions under UN auspices has been noted in the consensus GGE reports of 2010, 2013 and 2015. Each of these reports has called for regular dialogue on the international security dimension of ICTs, recognizing that the speed of ICT developments and the scope of the threat merited strengthening cooperation and finding common ground.

63. The OEWG has served as an initial response to these recommendations by offering, for the first time, a platform under United Nations auspices open to all States and focused solely on developments in ICTs in the context of international security. In addition to its objective to seek common understandings among all States through their substantive exchanges, the OEWG has permitted the strengthening of diplomatic networks and trust through its structured, in-person meetings. The broad participation 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.

64. In their discussions at the OEWG, States affirmed that given 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. They considered whether and how further regular dialogue could support the goal of strengthening international peace, stability and prevention of conflicts in the ICT environment, as well as the most appropriate

[8] A/65/201, paragraph 18(i); A/68/98*, paragraph 29; A/70/174, paragraphs 18 and 33.

format to achieve that goal. It was suggested that the establishment of a regular institutional dialogue would be an important outcome of the OEWG.

65. States expressed a range of views as to the specific objectives of regular institutional dialogue and which format of regular dialogue could best support these objectives. One set of proposed objectives for regular dialogue comprises awareness raising and information exchange; developing guidance to support and monitor the implementation of existing commitments and recommendations; building trust and confidence; coordinating and strengthening the effectiveness of capacity-building; identifying and exchanging good practices; and encouraging further study and discussion on areas where no common understanding has yet emerged. It was suggested that a mechanism for dialogue supporting these objectives could be the establishment of annual meetings under the purview of the existing UN disarmament machinery.

66. Another set of proposed objectives for regular dialogue comprises negotiations of further commitments of a voluntary or binding nature, including regulatory, compliance and verification efforts. It was suggested that a mechanism for dialogue supporting these objectives could consist of meetings leading to negotiation of a binding instrument and possibly institutional structures to support it.

67. A format attending to both sets of purposes was also proposed. Such a format could serve as a follow up to encourage implementation and adherence to existing commitments, while establishing a periodic opportunity to assess whether additional measures are necessary. It was suggested that a mechanism for dialogue supporting these objectives could be through follow up to a politically-binding declaration based on consensus resolution 70/237. In this proposal, regular meetings under UN auspices could focus on supporting implementation and operationalization of existing commitments, in combination with a periodic review function for consideration of the necessity for new measures or further refinement of the existing normative framework.

68. It was also suggested that the OEWG's mandate contained in resolution 73/27 could be renewed for a limited period or indefinitely. It was also noted that different formats for dialogue are not necessarily mutually exclusive. A format with broad participation may be complementary to one with more limited membership. Together they may provide the opportunity to capitalize on the unique features of each.

69. In addition to the four characteristics—"regular", "institutional", "broad participation", and "under UN auspices"—noted in the OEWG mandate,[9] States also emphasized that any platform for regular institutional dialogue should be a process with specific objectives, building on previous agreements, and be inclusive, consensus driven, sustainable, practical and results-oriented. The need for further consideration of the duration of a future dialogue, its timing, potential locations, and budgetary considerations were also raised.

70. A variety of forums within the UN system focus on the digital dimensions of other issues, including terrorism, crime, development, human rights and Internet governance.[10] It was highlighted that

[9] See background paper issued by the Chair of the OEWG, "'Regular Institutional Dialogue' in the Consensus Reports of the United Nations Groups of Governmental Experts and the Mandate of the OEWG", December 2019, pp. 2-3. https://unoda-web.s3.amazonaws.com/wp-content/uploads/2020/01/background-paper-on-regular-institutional-dialogue.pdf.

[10] 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.

any future process of regular dialogue should remain focused on international peace and security so as not to duplicate existing efforts and activities. It was suggested that greater exchange between these forums and the international security discussion, such as through joint meetings of committees of the General Assembly, while respecting the expert nature or specialized mandate of each, could help to reinforce synergies and improve coherence.

71. It was recalled that States hold primary responsibility for national security, public safety and the rule of law. It was also noted that regular dialogue should be primarily intergovernmental in nature, and appropriate mechanisms for engagement with other stakeholder groups would need to be found. In their interventions, States acknowledged that building a more resilient and secure ICT environment necessitates multi-stakeholder cooperation and partnerships. While recognizing the unique role and responsibility of States in relation to security, there was growing appreciation that States may benefit from the expertise in non-governmental communities and that responsible behaviour of other actors makes an essential contribution to this environment.

H. Conclusions and Recommendations

72. The OEWG presented a historic first opportunity for all UN Member States to discuss, under the auspices of the United Nations, matters related to ICTs and international security. The OEWG's discussions, building on the foundation provided by the consensus reports of the GGEs, were guided by the principles of inclusivity and transparency, with the aim of maintaining and promoting trust, in the fulfilment of its mandate. Its formal and informal sessions were characterized by substantive exchanges among Member States, as well as with the private sector, non-governmental organizations, civil society and academia. The strong engagement by States and other stakeholders throughout the work of the OEWG 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 posed by the malicious use of ICTs.

73. 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 normative framework of cooperative measures to address existing and potential threats in the sphere of ICTs. Regular institutional dialogue will provide the opportunity for the framework to be further developed and operationalized through advancing common understandings and the exchange of lessons learned and practices in implementation. Regular institutional dialogue can in itself also build more confidence and increase capacity amongst States.

74. In fulfilling the requirements specified by its mandate, the OEWG makes the following recommendations.

a) With regard to international law, reaffirming that international law, 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, the OEWG recommends that:

- Member States be invited to 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 about national views and practice on how international law applies to State use of ICTs in the context of international security.

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

- The Secretary-General be requested to establish a repository of national views and practice on how international law applies to the use of ICTs by States in the context of international security.

- The International Law Commission be requested by the General Assembly to undertake a study of national views and practice on how international law applies in the use of ICTs by States in the context of international security.

- *[other recommendations]*

- Member States continue to consider, at the multilateral level, how international law applies in the use of ICTs by States in the context of international security.

b) With regard to rules, norms and principles of responsible behaviour of States, reiterating that voluntary, non-binding norms are consistent with international law, and recalling that in 2015 the General Assembly agreed by consensus that all States should be guided in their use of ICTs by the 2015 report of the Group of Governmental Experts, which sets out 11 voluntary, non-binding norms of responsible State behaviour, the OEWG recommends that:

- Member States be invited to 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 their implementation of international rules, norms and principles of responsible behaviour of States in the use of ICTs.

- The Secretary-General be requested to establish a repository of national practices regarding international rules, norms and principles of responsible behaviour of States, which could be further developed into guidance on implementation. The use of surveys or templates on a voluntary basis are encouraged in this regard.

- Further guidance on the implementation of norms of responsible State behaviour be developed and widely disseminated at national, regional, interregional and global levels including through the United Nations. States in a position to contribute expertise or resources to the development and dissemination of such guidance are encouraged to do so.

- *[other recommendations]*

- Member States continue to consider, at the multilateral level, international rules, norms and principles of responsible behaviour of States.

c) With regard to confidence-building measures (CBMs), highlighting that CBMs should be developed and implemented progressively, including at the bilateral, regional and multilateral levels, so as to enhance mutual trust, the OEWG recommends that:

- The Secretary-General be requested to establish a repository of CBMs adopted at regional and sub-regional levels to enable the sharing or exchange of information on CBMs and identify potential capacity and resource gaps. The repository would be established in coordination with interested regional and sub-regional bodies and without prejudice to further elaboration of CBMs at the global, regional or sub-regional level.

- Members States be encouraged to, on the basis of such a repository, potentially identify the CBMs appropriate to their specific contexts, and cooperate with other States on their implementation.

- The Secretary-General be requested to establish, in coordination with interested regional and sub-regional bodies, a global registry of national Points of Contacts at the policy or diplomatic level, bearing in mind coordination with other such registries, including at the regional and sub-regional levels.

- Member States, which have not yet done so, be encouraged to nominate a national Point of Contact at the policy or diplomatic level, taking into account differentiated capacities.

- Members States be encouraged to explore mechanisms for regular cross-regional exchanges of lessons and good practices, taking into account differences in regional contexts and the structures of relevant organizations.

- *[other recommendations]*

- Member States continue to consider CBMs at the bilateral, regional and multilateral levels.

d) With regard to capacity-building, emphasizing its critical functions for empowering all States and other relevant actors to fully participate in the global normative framework, for promoting adherence to international law and the implementation of norms of responsible State behaviour, and for building trust between and within States, the OEWG recommends that:

- ICT-related capacity-building efforts in the field of international security should be guided by the following principles:

    - *[insert agreed principles]*

- Member States be invited to 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.

- The Secretary-General be requested to establish a global mechanism for enhancing coherence in capacity-building efforts in the use of ICTs, possibly in the form of a facilitation mechanism, in coordination with existing efforts, including at the regional and sub-regional levels. States

in a position to contribute expertise or resources to the development of such a mechanism are encouraged to do so.

- Member States be encouraged to further cooperate to build capacity to identify and protect national and transnational critical infrastructure as well as supranational critical information infrastructure.

- *[other recommendations]*

- Member States continue to consider capacity-building at the multilateral level.

e) With regard to <u>regular institutional dialogue</u>, affirming that the increasing dependency on ICTs and the scope of threats stemming from their misuse necessitates urgent action to enhance common understandings and intensify cooperation through multilateral discussions, the OEWG recommends that:

- The 76th session of the General Assembly of the United Nations convene a new open-ended working group of the General Assembly acting on a consensus basis to continue the consideration of developments in the field of information and telecommunications in the context of international security.

- States be encouraged to consider establishing sponsorship programmes and other support mechanisms to ensure broad participation. States in a position to support such programmes and mechanisms are encouraged to do so.

- The 76th Session of the General Assembly of the United Nations also consider requesting the Secretary-General to establish a new group of governmental experts.

- *[other recommendations]*