Initial "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. *Over this period, information and communications technologies (ICTs) have been a catalyst for human progress. ICTs and global connectivity have transformed societies and economies, and expanded opportunities for cooperation for the common good of humankind*.

3. *The General Assembly has recognized repeatedly that scientific and technological developments could have both civilian and military applications and that progress in science and technology for civilian applications needs to be maintained and encouraged. It has also acknowledged that technology can be used for purposes that are inconsistent with the objectives of maintaining international stability and security. Similar to other scientific and technological advancements, ICTs are positively transforming the human condition, while also creating profound and unique challenges. In this regard, States should ensure the responsible development and use of ICTs so that their citizens can reap the full benefits of these innovations.*

4. *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.*

5. *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 framework of international law, voluntary norms and confidence-building measures. Notably, the 2013 and 2015 reports recognized 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. In resolution 70/237, Member States agreed by consensus to be guided in their use of ICTs by the 2015 report.*

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

6. *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, is an opportunity to advance consideration of ICTs in the context of international security. It provides an inclusive platform for all Member States to participate, express their views and extend cooperation on the international security dimension of ICTs. Mandated to produce a consensus report, the OEWG is uniquely positioned to seek common ground and mutual understandings among all Member States of the United Nations on a subject of global consequence.*

7. *The OEWG's discussions were guided by the principles of inclusivity and transparency, with the aim of maintaining and promoting trust. As the international security dimension of ICTs cuts across multiple domains and disciplines, a wealth of expertise is held by other stakeholders on specific issues within the OEWG's mandate. In order to draw 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.*

8. *The OEWG has taken note of trends in the digital domain that 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. This includes the growing exploitation of ICTs for malicious purposes, which may inhibit securing the benefits of ICTs.*

9. *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 remains an urgent priority for the international community. The OEWG also 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. In this regard, the OEWG welcomes the high level of participation of women delegates at the OEWG and the prominence of gender perspectives in its discussions.*

10. *Developments in ICTs have implications for all three pillars of the United Nations' work: peace and security, human rights and sustainable development. In parallel to the work on the topic of ICTs in the context of international security, discussions on other aspects of digital technologies have advanced in various UN bodies and agencies. These 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.*

11. *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*

[3] A/RES/53/70.

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.

12. *The OEWG recognizes that the individual elements comprising its mandate are interrelated and mutually reinforcing, and are to be considered through a human-centric lens. 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 respect for 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. In light of these synergies, the following sections of the report are to be considered as complementary and interdependent.*

13. *Sections B-G below reflect the substantive discussions of the OEWG and 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. Misuse can undermine trust within and among States, the enjoyment of human rights and the potential for economic and social development. There is growing concern about the potential implications of the malicious use of ICTs for the maintenance of international peace and security. Harmful ICT incidents are increasing in frequency, precision and sophistication, and are constantly evolving and diversifying. Increasing connectivity and reliance on ICTs may also bring unintended risks, making societies more vulnerable to malicious ICT activities.

14. 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 ICT capabilities previously only available to States were now accessible to non-State actors, including terrorists and criminals.

15. States expressed the view that the development or use of offensive ICT capabilities, as well as the stockpiling of vulnerabilities, are contributing to the militarization of the digital space. Pursuit of increasing automation and autonomy in ICT operations was also put forward as a specific concern. States highlighted as a central threat the possibility that ICTs could be used in a manner inconsistent with a State's obligations under international law. 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. Concerns were also raised about the exploitation of harmful hidden functions and the integrity of global ICT supply chains.

16. States underscored that a lack of awareness, resilience and adequate capacities constitutes a threat in and of itself as all countries are increasingly reliant on digital technologies.

17. It was noted that threats may have a differentiated impact on different actors, including on youth, the elderly, women and men, on vulnerable populations, particular professions, and other categories of actors, as well as on States with different levels of ICT security and resilience.

18. States noted significant technological trends, including progress in machine learning, encryption, 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, including digitized personal data. While recognizing the substantial beneficial applications of these innovations, States cautioned that technological advances and new applications may also expand attack surfaces, amplify vulnerabilities in the ICT environment or facilitate novel malicious activities. At the same time, there was broad agreement that measures to promote responsible State behaviour should remain technology-neutral.

19. While States observed that critical infrastructure is defined differently in accordance with national prerogatives and priorities, they emphasized the severity of threats to particular categories of infrastructure, including for instance the health and financial sectors and electoral infrastructure. Transborder and transnational critical infrastructure was highlighted as at risk as was supranational critical information infrastructure, notably those global systems upon which public or financial services rely. In this regard, States underscored that attacks on critical infrastructure pose not only a threat to security, but also to economic development and people's livelihoods.

20. 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 would produce more effective and far-reaching results. The positive contributions of the private sector, civil society and academia were also emphasized in this regard.

21. The following sections reflect the OEWG's discussions of how the international community might actively strengthen its collective resolve to address these threats. The concluding section contains the OEWG's recommendations.

C. International Law

Existing obligations under international law, in particular the Charter of the United Nations, 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.

22. 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.

23. Specific principles of the UN Charter highlighted include 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.

24. States had an interactive exchange of views on the relevance and applicability of specific bodies of law to the international security dimension of ICTs, including international humanitarian law, international human rights law, international criminal law, as well as international customary law. It was also noted that the responsibilities of States with regard to internationally wrongful acts are applicable to their use of ICTs.

25. 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 conflict in any domain.

26. During the discussion the view was expressed 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 noted that efforts should therefore be directed to reaching common understanding on how the already agreed normative framework applies and can be operationalized.

27. At the same time, during the discussion, it was also noted that there may be a need to adapt existing international law or develop a new instrument to address the unique characteristics of ICTs. In particular, 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, including the protection of civilians and civilian objects, apply to ICT operations in the context of armed conflict. In this regard, it was noted that the issue of the applicability of international humanitarian law to the use of ICTs by States needed to be handled with prudence.

28. In this context, 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 necessitates a stronger, internationally agreed framework. It was noted 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.

29. 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 in this regard. Developing complementary binding measures concurrently with the implementation of norms was also proposed. A politically binding commitment[4] with regular meetings and voluntary State reporting, was also suggested as a possible middle ground approach.

30. States proposed that a first step to further develop common understandings could be increased exchanges on their interpretation of how international law applies to the use of ICTs by States. States

[4] 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/.

proposed several ways to share their national views, 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.

31. In addition, it was proposed that guidance notes could be developed 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.

32. From the perspective of maintaining peace and preventing conflict, it was noted that greater focus could be placed on adherence to key Charter principles such as the settlement of disputes by peaceful means and refraining from the threat or use of force. In this context, States recalled existing mechanisms for the settlement of disputes, including the Security Council and the International Court of Justice. It was suggested that developing a common approach to attribution at the technical level could lead to greater accountability, transparency, and could help support legal recourse for those harmed by malicious acts.

33. In order for all States to participate on an equal footing in discussions on how international law applies to the use of ICTs by States, it was stressed that there was a 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 regarding the 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 States' obligations under international law, 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.

34. 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 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.

35. States, bearing in mind General Assembly resolution 73/27, also reaffirmed the voluntary, non-binding norms of responsible State behaviour of the 2015 GGE report,[5] recalling that consensus resolution 70/237 calls upon States to be guided in their use of ICTs by the 2015 GGE report, which includes the 11 voluntary, non-binding norms.

36. Attention was drawn to the international code of conduct for information security tabled in 2015.[6] 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".

37. 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. Different cooperative approaches were also proposed, such as developing a roadmap to assist States in their implementation efforts.

38. States, during discussions and through written submissions, also proposed suggestions for the "upgrading" as well as further elaboration of norms. Proposals included, *inter alia*, that States should affirm their commitment to international peace and security in the use of ICTs; that it should be reaffirmed that States hold the 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 harm medical facilities. States also proposed the need to further ensure 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 supranational critical information infrastructure could be considered a special category of critical infrastructure, and that its protection was the shared responsibility of all States.

39. *[placeholder: additional proposals by Member States for new norms could be introduced here]*

40. The need to encourage partnerships and joint efforts with the private sector and other stakeholders on the implementation of norms was highlighted, including with regard to ensuring sustainable capacity-building efforts. It was noted that all stakeholders had responsibilities in their use of ICTs.

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

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 providing a "safety valve" for the reduction of tensions. CBMs can strengthen the overall security and resilience 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. They 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 recognized that regional organizations 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.

41. In their discussions at the OEWG, States highlighted the need to translate confidence-building measures into concrete actions that are implementable by all States.

42. States noted the continuing relevance of the CBMs recommended in the consensus GGE reports. Measures highlighted for priority attention included 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, training for diplomats, exchanging lessons on establishing and exercising secure crisis communication channels, and operational exercises at the technical level between Computer Emergency Response Teams (CERTs) or Computer Security Incident Response Teams (CSIRTs).

43. 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 of the normative framework that guides the use of ICTs by States.

44. In particular, States stressed that establishing national Points of Contact (PoC) constitutes a prerequisite for the implementation of many 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. 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 success. The value of regularly conducting exercises among a network of PoCs was also emphasized, as it can help to maintain readiness and ensure that PoC directories remain updated.

45. 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 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.

46. 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 adequate resources and capacities, are essential to ensuring that CBMs serve their intended purpose. In this regard, 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 cross-regional or inter-organizational exchanges have served. 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 are used to promote CBMs as well. States also proposed that some CBMs developed at the regional level could be universalized.

47. 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 have, through the development of principles and commitments, 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. The international community's ability to prevent or mitigate the impacts 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.

48. In their discussions at the OEWG, States reiterated the recommendations on international cooperation and capacity-building in the consensus GGE reports. They emphasized the critical function that capacity-building can play with regard to empowering all States and other relevant actors to fully participate in the global normative framework, 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 the voluntary, non-binding 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.

49. States noted that capacity-building helps to address the systemic and transnational risks arising from a lack of ICT security, disconnected 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 supranational critical information infrastructure was deemed to be of particular importance.

50. There was a general acknowledgement that in addition to technical skills, there is a pressing need for building expertise across a range of diplomatic, policy, legislative and regulatory areas.

51. Many challenges were identified that hinder or reduce the effectiveness of capacity-building. The lack of coordination at the international level was highlighted as a significant concern. Practical challenges in the design, delivery, sustainability and accessibility of capacity-building activities, and the lack of specific metrics to measure their impact, were also raised. Once capacity has been built, some countries face the challenge of talent retention in a competitive market for ICT professionals. States highlighted that lack of access to ICT security-related technologies was also an issue.

52. States underscored that ICT-related capacity-building efforts would be more effective if they were guided by widely accepted principles.[7] To this end, States stressed the importance of national ownership in the identification of capacity-building and technical assistance needs and priorities. They also noted that capacity-building should be demand-driven, tailored to specific needs and contexts, evidence-based, results-oriented, and have sustainable impacts. Capacity-building initiatives should be transparent and accountable. Additionally, it was emphasized that capacity-building should be non-discriminatory, politically neutral, gender sensitive, and focus on peaceful outcomes. In this regard, States underscored that technical capacity-building and capacity-building on the normative framework should go hand-in-hand.

53. 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.

54. The importance of a multi-stakeholder approach in capacity-building 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.

55. States stressed that there was a need for greater coordination in capacity-building efforts. In this regard, States suggested that existing platforms within the United Nations and in the wider global community could be used to strengthen 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 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.

56. 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. 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.

[7] These include general principles, such as the 2011 Busan Partnership for Effective Development Co-operation ("Busan Principles"), as well as those developed specifically for capacity-building in ICT-related fields.

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. Through the OEWG many States participated for the first time in inclusive discussions under United Nation auspices on this topic. This active and broad engagement has demonstrated the commitment of Member States to continue to work together on this subject of fundamental importance to all.

57. 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.

58. The consensus GGE reports of 2010, 2013 and 2015 called attention to the need for regular dialogue on the international security dimension of ICTs. The 2010 report[8] recommended further dialogue among States to discuss norms, reduce collective risk and protect critical infrastructure. In 2013, in recognition that the speed of ICT developments and the scope of the threat merited strengthening cooperation and finding common ground, the GGE recommended regular institutional dialogue with broad participation under the auspices of the United Nations, as well as encouraged dialogue in bilateral, regional and other international forums.[9] The 2015 GGE reiterated the need for regular dialogue at the United Nations, while cautioning against duplication of efforts.[10]

59. States suggested many potential purposes for regular dialogue, including awareness raising and information exchange; developing guidance to support and monitor the implementation of existing commitments and recommendations; building trust and confidence; coordinating, strengthening and monitoring effectiveness of capacity-building; identifying and exchanging good practices; encouraging further study and discussion on areas where no common understanding has yet emerged; and negotiation of further commitments of a voluntary or binding nature. It was also emphasized that any platform for regular institutional dialogue should be a process building on previous agreements, inclusive, consensus driven, sustainable, results-oriented, with specific objectives that take forward agreements in practical and tangible ways.

60. States noted that there are established venues within the UN Disarmament Machinery where ICTs and international security could be addressed within existing resources, including the General Assembly's First Committee and the United Nations Disarmament Commission. It was also recalled that a variety of external venues for regular dialogue on these topics already exist, including at the regional and sub-regional levels. Nevertheless, States emphasized that while these are complementary efforts, they are not a substitute for regular dialogue under UN auspices due to its inter-governmental nature, inclusiveness and legitimacy.

61. Noting that many parts of the UN address digital technology issues, including their development, rights and crime dimensions, States recognized the need for a dedicated mechanism under UN auspices focusing on international security issues. It was recalled that there are established forums within the UN system focused on issues relating to ICTs and terrorism, crime, human rights and Internet governance. Greater exchange and exploration of synergies between these bodies, such as

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

through joint meetings of committees of the General Assembly, while respecting the expert nature or specialized mandate of each, was encouraged.[11]

62. A variety of proposals were made to take forward regular institutional dialogue. It was noted that the GGE process since 2004 has been a form of regular dialogue. It was also suggested that the format of the OEWG, with its inclusive membership and transparent discussions, should become the standard for discussion and therefore the renewal of its mandate was called for. It was highlighted that there was value in having the sixth Group of Governmental Experts meeting in parallel to the OEWG, stressing their complementarity and the opportunity to capitalize on the unique features of each process. Looking beyond the mandates of the OEWG and sixth GGE, a further suggestion was that regular institutional dialogue could be the follow-up mechanism to a politically binding instrument.[12] Another possibility raised was that an inter-governmental specialized agency could be established.

63. In addition to questions concerning the four characteristics—"regular", "institutional", "broad participation", and "under UN auspices"—noted in the OEWG mandate,[13] additional queries were raised concerning the duration of such dialogue, the timing of establishing a new mechanism for dialogue prior to the conclusion of the work of the sixth GGE, potential locations, and budgetary considerations.

64. The OEWG's mandate provided for the possibility of holding intersessional consultative meetings with other stakeholders, including the private sector, non-governmental organizations and academia. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich exchange between States and other stakeholders. The OEWG also heard interventions from non-governmental organizations during an informal multi-stakeholder segment at its first and second sessions. In order to further inform their engagement with the OEWG, some States noted that they have conducted domestic multi-stakeholder consultations or calls for submissions.

65. It was recalled that States hold primary responsibility for national security, public safety and rule of law. It was also noted that regular dialogue should be primarily intergovernmental in nature, and an appropriate mechanism to leverage the experience and knowledge of 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.

---

[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.

[12] Similar to the mechanisms established under the UN Programme of Action on Small Arms and Light Weapons, with biennial meetings of States to consider the national, regional and global implementation of the PoA, and a quinquennial review conference to review progress. See A/CONF.192/15 section IV.1.(a) and (b).

[13] 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.

H. Conclusions and Recommendations

66. 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.

67. 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.

68. 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 regular institutional dialogue, 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]*