Proposed amendments to the OEWG First Draft report as discussed ad referendum including by Australia, Egypt, Indonesia, Russia, and the United Kingdom. France was consulted on paragraph 75. Unless marked "subject to consultation", suggested amendments received in-principle support from the countries listed. Delegations focused on redline issues only, with the objective of proposing solutions for consensus. All delegations reserve the right to consult and to make further comments, and look forward to fruitful consensus-orientated exchanges of views on the First Draft at the formal OEWG meetings commencing Monday 9 March.

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

Substantive Report [FIRST DRAFT]

A. Introduction

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

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

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

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

5. As ICTs can be used for purposes that are inconsistent with the objectives of maintaining international peace, stability and security, the General Assembly has recognized [1] that the dissemination and use of ICTs affect the interests of the entire global community and that broad international cooperation would lead to the most effective responses.

6. In light of the above, the Open-ended Working Group on developments in the field of

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

[1] See, for example A/RES/53/70, pp 6.

7. *[A preference for norms to be reference before international law was raised – **subject to consultation.**]* The OEWG represents the latest milestone in international cooperation towards an open, secure, stable, accessible and peaceful ICT environment. On six occasions since 2003, groups of governmental experts (GGEs) have been established to study existing and potential threats in the sphere of information security and possible cooperative measures to address them. [2] Through their three consensus reports (2010, 2013 and 2015[3]), which are cumulative in nature, these Groups have reaffirmed that international law, in particular the Charter of the United Nations, is applicable and essential to maintaining peace, security and stability in the ICT environment. They also recommended 11 voluntary, non-binding norms of responsible State behaviour and recognized that additional norms could be developed over time. Furthermore, specific confidence-building, capacity-building and cooperation measures were recommended. In General Assembly resolution 70/237, Member States agreed by consensus to be guided in their use of ICTs by the 2015 GGE report, thereby consolidating an initial framework for responsible State behaviour in the use of ICTs In this regard, the OEWG also noted General Assembly Resolution 73/27.

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

9. While States are primarily [*reflects previous agreed language and paras 69 &108*] responsible for the maintenance of international peace and security, all stakeholders have a responsibility to use ICTs in a manner that does not endanger peace and security. As the international security dimension of ICTs cuts across multiple domains and disciplines, the OEWG has benefited from the expertise, knowledge and experience shared by representatives from inter-governmental organizations, regional organizations, civil society, the private sector, academia and the technical community. The three-day informal consultative meeting of the OEWG held in December 2019 produced a rich discussion between States and a wide variety of other stakeholders. [4] In addition, these stakeholders have provided concrete proposals and examples of good practice through written contributions and informal exchanges with the OEWG. Some delegations have also conducted multi-stakeholder consultations at their own initiative to inform their contributions to the OEWG.

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

[2] A/RES/58/32, A/RES/60/45, A/RES/66/24, A/RES/68/243, A/RES/70/237, A/RES/73/266.

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

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

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

12. The OEWG recognizes the importance and complementarity of specialized discussions on aspects of digital technologies addressed by other UN bodies and fora. These topics include matters related to sustainable development, human rights (including on privacy and freedom of expression, including the freedom to seek, receive or impart and information and ideas), data protection [*ICCPR language; data protection retained, but moved to show its not specifically reference in ICCPR;* ***subject to consultation***] digital cooperation, Internet governance, cybercrime and the use of the Internet for terrorist purposes.

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

14. States, and norms reflect [*reflects agreed language*] expectations of responsible State behaviour. Measures that build confidence and capacity reinforce adherence to international law, encourage the operationalization of norms, provide opportunities for enhanced cooperation between States, and empower each State to reap the benefits of ICTs for their societies and economies.

B. Agreed conclusions and recommendations

14. Having considered the substantive aspects of the OEWG's mandate, States agreed on the following conclusions and recommendations, including concrete actions and cooperative measures to address ICT threats and to promote an open, secure, stable, accessible and peaceful ICT environment.

Existing and Potential Threats

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

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

17. States also agreed that any use of ICTs by States in a manner inconsistent with their obligations under international law undermines international peace and security, trust and stability between States, and may increase the likelihood of future conflicts between States.

18. States agreed that there are potentially devastating humanitarian consequences of malicious ICT activities on critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public such as but not limited to medical facilities, energy,

water, transportation and sanitation. Malicious ICT activities against CI and CII that undermine trust and confidence in political and electoral processes, public institutions, or that impact the financial system, are also a real and growing concern. Such infrastructure may be owned, managed or operated by the private sector, may be shared or networked with another State or operated across different States. As a result, inter-State or public-private cooperation may be necessary to protect its integrity, functioning and availability.

19. States also agreed that ICT activity contrary to obligations under international law that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public, poses a threat not only to security, but also to economic development and livelihoods, and ultimately the safety and wellbeing of individuals.

19bis Concern was expressed regarding the development of ICT capabilities for purposes that undermine international peace and security. [*In the event time does not allow consensus-based agreement to 'Part C: Discussion Section' (see also para 120bis), for many delegations this point is important to retain in the body.* ***Subject to consultation***].

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

21. States agreed that threats may be experienced differently by States according to their lev els of digitalization, capacity, ICT security and resilience, infrastructure and development. Threats may also have a different impact on different groups and entities, including on youth, the elderly, women and men, people who are vulnerable, particular professions, small and medium-sized enterprises, and others. In light of the increasingly concerning digital threat landscape, and recognizing that no State is sheltered from these threats, States agreed on the urgency of implementing and further developing cooperative measures to address such threats It was affirmed that acting together and inclusively whenever feasible would produce more effective and far-reaching results. The value of further strengthening collaboration, when appropriate, with civil society, the private sector, academia and the technical community, was also emphasized in this regard.

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

22 Bis: It was emphasized that measures to promote responsible State behaviour should remain technology-neutral, underscoring that it is the misuse of technologies, not the technologies themselves, that is of concern. [*In the event time does not allow consensus-based agreement to 'Part C: Discussion Section' (see also para 120bis), for many delegations this point is important to retain in the body.* ***Subject to consultation***].

International Law (Suggestion was made to swap the order of IL and norms section – **subject to consultation)**

23. Pursuant to General Assembly Resolution 73/27, which established the OEWG, States affirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible

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

24. Specific principles of international law [*state sovereignty not listed in A2 of the UN Charter; delete Charter to ensure accuracy*] which were reaffirmed include, among others, State sovereignty; sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security and justice are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.[5]

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

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

The OEWG recommends that

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

28. States in a position to do so continue to support, in a neutral and objective manner, additional efforts to build capacity, in accordance with the principles contained in paragraph 55 of this report, in the areas of international law, national legislation and policy, in order for all States to develop their own understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community.

29. States continue to study and undertake discussions within future UN processes on how international law applies to the use of ICTs by States as a key step to clarify and further develop common understandings on the issue, and to consider additional initiatives in this regard.

[5] A/RES/73/27, pp. 16.
[6] A/RES/75/32, op. 2.

Rules, Norms and Principles for Responsible State Behaviour

30. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. States stressed that such norms reflect the expectations of the international community, set standards regarding the behaviour of States in their use of ICTs. [

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

32. While agreeing that the protection of all critical infrastructure is equally vital, along with ensuring the general availability or integrity of the Internet, States further agreed that the COVID-19 pandemic accentuated the importance of protecting healthcare infrastructure including medical services and facilities as part of the norms addressing critical infrastructure.

33. States agreed on the importance of supporting and furthering efforts to implement norms, rules and principles [***subject to consultation***]; at the global, regional and national levels.

34. 32bis: States reaffirmed General Assembly Resolution 70/237, including the importance of taking reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products, and the importance of responsible reporting of vulnerabilities [*In the event time does not allow consensus-based agreement to 'Part C: Discussion Section' (see also para 120bis), for many delegations this point is important to retain in the body.* ***Subject to consultation***].Given the unique attributes of ICTs, States reaffirmed that, taking into account the proposals on norms made at the OEWG, additional norms could continue to be developed over time. States also agreed that the further development of norms and the implementation of existing norms were not mutually exclusive but could take place in parallel, and that further study could also help clarify the relationship between International Law and rules, norms and principles of responsible behaviour of States.

The OEWG recommends that

35. States, on a voluntary basis, survey their national efforts to implement norms, develop and share guidance on norms implementation, and continue to inform the Secretary-General of these activities,

36. States should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages critical infrastructures or otherwise impairs the use and operation of critical infrastructure to provide services to the public [*amended to reflect agreed language (norm f)*]. Furthermore, States should continue to strengthen measures to protect [*for simplicity –* ***subject to consultation***]all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection.

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

[7] A/RES/75/32

38. States, recalling resolution 70/237 and also acknowledging resolution 73/27, further consider proposals [*non paper title coveys unclear status; but see para 120bis where the content of the paper is retained in Chair's summary*] made by States on the elaboration of rules, norms and principles of responsible behaviour of States in future discussions on ICTs within the United Nations, acknowledging that resolution 75/240 established an Open-ended Working Group on security of and in the use of information and communications technologies 2021 - 2025.

Confidence-building Measures

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

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

41. States agreed that the dialogue within the Open-ended Working Group was in itself a CBM, as it stimulates an open and transparent exchange of views on perceptions of threats and vulnerabilities, responsible behaviour of States and other actors and good practices, thereby ultimately supporting the collective development and implementation of the framework for responsible State behaviour in their use of ICTs.

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

43. Building on their essential assets of trust and established relationships, States agreed that regional and sub-regional organizations have made significant efforts in developing CBMs, adapting them to their specific contexts and priorities, raising awareness and sharing information among their members. In addition, regional, cross-regional and inter-organizational exchanges can establish new avenues for collaboration, cooperation, and mutual learning. As not all States are members of a regional organization and not all regional organizations have CBMs in place, it was noted that such measures are complementary to the work of the UN and other organizations to promote CBMs.

8

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

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

The OEWG recommends that

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

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

48. .

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

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

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

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

Capacity-building

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

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

capacity-building radiate beyond the initial recipients, and contribute to building a more secure and stable ICT environment for all.

54. Ensuring an open, secure, stable, accessible and peaceful ICT environment is a [*[delete but retain in para 55 below*] responsibility that requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is an important aspect of such cooperation and a voluntary act of both the donor and the recipient.

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

Process and Purpose [*suggestion to delete the subtitles: do they value add?* ***Subject to consultation;*** *Dot points changed to numbered sub paras –* ***subject to consultation****]*

a) Capacity-building should be a sustainable process, comprising specific activities by and for different actors.

b) 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.

c) Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.

d) Capacity-building should be undertaken with full respect for the principle of State sovereignty.

e) Access to relevant technologies may need to be facilitated.

Partnerships

f) Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.

g) As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared [*reflects NAM paper language*]but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.

h) The confidentiality of national policies and plans should be protected and respected by all partners.

People

i) Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.

j) The confidentiality of sensitive information should be ensured.

56. States agreed that capacity-building is a reciprocal endeavour, a so-called “two-way street”, in which participants learn from each other and where all sides benefit from the general improvement to global ICT security. The value of South–South, South–North, triangular, and regionally focused cooperation was also recalled.

57. States agreed that capacity-building can help to foster an understanding of and address the systemic and other risks arising from a lack of ICT security, insufficient coordination between technical and policy capacities at the national level, and the related challenges of inequalities

and digital divides. Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical information infrastructure was deemed to be of particular importance. Capacity-building may also help States to deepen their understanding of how international law applies. Information sharing and coordination at the national, regional and international levels can make capacity-building activities more effective, strategic and aligned to national priorities.

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

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

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

The OEWG recommends that

61. States be guided by the principles contained in paragraph 55 in their ICT-related capacity-building efforts in the field of international security, and other actors be encouraged to take these principles into consideration in their own capacity-building activities.

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

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

64. States and other actors in a position to offer financial, in-kind or technical assistance for capacity-building be encouraged to do so. Further promotion of coordination and resourcing of capacity-building efforts, including between relevant organizations and the United Nations, should be further facilitated.

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

Regular Institutional Dialogue

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

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

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

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

70. Consideration of developments in ICTs and international security at the United Nations focuses on its international peace, stability and conflict prevention dimensions. States agreed that future regular institutional dialogue should not duplicate existing UN mandates, efforts and activities focusing on the digital dimensions of other issues, including terrorism, crime, development, human rights and Internet governance. [10] States agreed that greater exchange between these forums and First Committee-established processes could help to reinforce synergies and improve coherence, while respecting the expert nature or specialized mandate of each body.

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

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

The OEWG recommends that

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

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

[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.

75. States note a variety of proposals for advancing responsible State behaviour in ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action. In considering these proposals, the concerns and interests of all States should be taken into account through equal State participation at the United Nations. In this regard, the Programme of Action, should be further elaborated, including at the Open-Ended Working Group process established pursuant to General Assembly resolution 75/240.

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

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

Note: Section C was not subject to paragraph/paragraph discussion by the informal group. See para 120bis for proposal if time does not allow consensus-based agreement of this section before Friday 12 March.

C. Discussions

78. Throughout the OEWG process, a high number of States participated consistently and actively, resulting in an extremely rich exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States. The following comprises a summary of these discussions.

Threats

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

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

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

International Law

82. Guided by the Group's mandate, and with the objective of maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT

environment and promoting common understandings, States had an exchange of views on how international law applies to the international security dimension of ICTs.

83. In their discussions at the OEWG, States recalled that international law, and in particular the Charter of the United Nations in its entirety, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. In this regard, States underscored the need to take steps to avoid and refrain from taking any measures not in accordance with the Charter of the United Nations and international law that impedes the full achievement of economic and social development by the population of the affected countries and that hinders their well-being. At the same time, States also highlighted that further understanding was required on how international law applies to State use of ICTs.

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

85. 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.

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

87. States recalled that the indication that an ICT activity was launched or otherwise originates from the territory or the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State and that accusations of organizing and implementing wrongful acts brought against States should be substantiated. Some States highlighted the importance of genuine, reliable and adequate proof in this context.

88. Some States expressed the view that existing international law, complemented by the voluntary, non-binding norms that reflect consensus among States, is currently sufficient for addressing State use of ICTs. It was also proposed that efforts should focus on reaching common understanding on how the already agreed normative framework applies through the development of additional guidance, and can be operationalized through enhancing implementation by all States. At the same time, other States expressed the view that due to the quickly evolving nature of the threat environment and the severity of the risk, an internationally agreed legally binding framework on ICTs is needed. It was also suggested that such a binding framework may lead to more effective global implementation of commitments and a stronger basis for holding actors accountable for their actions. States stressed that the development of any international legal framework to address issues related to the use of ICTs with implications on international peace and security should take into account the concerns and interests of all States, be based on consensus, and pursued within the UN with the active and equal participation of all States.

89. It was highlighted that while existing bodies of international law do not include specific reference to the use of ICTs in the context of international security, international law can develop progressively, including through opinio juris and State practice. The

possibility over time of developing complementary binding measures concurrently with the implementation of norms was raised. Furthermore, a political commitment was proposed as one possible way forward.

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

91. Also, in terms of ways forward, States proposed that a key first step to clarify and further develop common understandings could emanate from increased exchanges and in-depth discussions by States on how international law applies to State use of ICTs. It was noted that such exchanges in themselves could serve as an important confidence-building measure. Some States furthermore proposed several ways to voluntarily share their national views on how international law applies, including utilizing the annual report of the Secretary-General on developments in the field of information and telecommunications in the context of international security,[11] the Cyber Policy Portal of the United Nations Institute for Disarmament Research, or using a survey of national practice in the application of international law. The progress made in regional and other arrangements to exchange views and develop common understandings on how international law applies was also highlighted.

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

Rules, Norms and Principles for Responsible State Behaviour

93. In their discussions at the OEWG, States recalled that voluntary, non-binding norms of responsible State behaviour do not alter or replace, but rather should be viewed as being consistent with, international law and with the purposes and principles of the United Nations, including to maintain international peace and security and the promotion of human rights. States also noted General Assembly resolution 2131 (XX), 1965 entitled "Declaration on the Inadmissibility of Intervention in the Domestic Affairs of States and the Protection of their Independence and Sovereignty".

[11] A/RES/75/32

94. States recalled that General Assembly resolution 73/27, while presenting a set of 13 rules, norms and principles for responsible State behaviour, inter alia, affirms the 11 voluntary, non-binding norms "enshrined in the reports of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security of 2013 and 2015 adopted by consensus and recommended in resolution 71/28".[12]

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

96. States recognized that norms can help to prevent conflict in the ICT environment and contribute to ICTs peaceful use and full realization to increase global social and economic development. States highlighted that the implementation of norms should not result in undue restrictions on international cooperation and technology transfer, nor hinder innovation for peaceful purposes and the economic development of States in a fair and non-discriminatory environment. States also stressed the interlinkages between norms, confidence-building and capacity-building, and underscored the need for gender perspectives to be mainstreamed into norm implementation.

97. During discussion, proposals were made for the further elaboration of existing norms. States reiterated the equal importance of the protection of all critical infrastructure supporting essential services to the public which should include medical and healthcare facilities. They also drew attention to the importance of cooperating to protect critical infrastructure that provides services across borders or jurisdictions, given the potential impact of any damage to such infrastructure, as well as the importance of ensuring the general availability and integrity of the Internet. States recalled General Assembly resolution 64/211 entitled "Creation of a global culture of cybersecurity and the protection of critical information infrastructures".[13] *In addition, States also proposed further ensuring the integrity of the ICT supply chain, expressing concern over the creation of harmful hidden functions in ICT products, and the responsibility to notify users when significant vulnerabilities are identified. States furthermore expressed concern regarding the stockpiling of vulnerabilities. Some States proposed to formulate objective international rules and standards on supply chain security.*

98. Further to the above paragraph, a list of written proposals made by States at the OEWG on the elaboration of existing norms, guidance on implementation as well as new norms were compiled in a non-paper and will be made available online for future consideration by States.[14]

99. Some States also noted the proposal for an international code of conduct for information security tabled in 2015.[15]

100. Some States recognized the need to encourage and support further regional efforts as well as partnerships with other stakeholders such as the private sector and the

[12] A/RES/73/27, operational paragraph 1.
[13] Annexed to this resolution is a Voluntary self-assessment tool for national efforts to protect critical information infrastructures.
[14] https://www.un.org/disarmament/open-ended-working-group/
[15] A/69/723, referenced in A/70/174, para 12.

technical community on the implementation of norms. Such partnerships could be built, for example, to ensure sustainable capacity-building efforts to address differences in implementation capacities. In this regard, States recalled operational paragraph 1.13 of General Assembly resolution 73/27, which, inter alia, highlights that "States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services". States noted the importance of outreach and cooperative steps to ensure that various stakeholders, including the public and private sectors and civil society, uphold their responsibilities in the use of ICTs.

Confidence-building Measures

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

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

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

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

Capacity-building

105. In their discussions at the OEWG, States emphasized the important function that capacity-building can play in empowering all States to fully participate in the international discussions on the framework for responsible State behaviour, while also contributing to shared commitments such as the 2030 Sustainable Development Agenda[16]. In this regard, States stressed the need for sufficient financial and human resources to be allocated to capacity-building programmes.

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

107. The United Nations has an essential role to play in supporting States to raise the profile of capacity-building and by leveraging its convening power to support greater coordination of the variety of actors active in capacity-building. States suggested that existing platforms within the United Nations, its specialized agencies and in the wider international community could be used to strengthen already established coordination. These platforms could be used to share national views on capacity-building requirements, encourage the sharing of lessons and experiences from both recipients and providers of support, and facilitate access to information on capacity-building and technical assistance programmes. These platforms could also support the mobilization of resources or assist with pairing available resources with requests for capacity-building support and technical assistance. It was suggested that the development of a global cyber capacity-building agenda under the auspices of the United Nations could help to ensure greater coherence in capacity-building efforts and that voluntary self-assessment surveys may help States to identify and prioritize their capacity-building needs or ability to provide support.

108. While recalling the primary responsibility of States for maintaining a secure, safe and trusted ICT environment, the importance of a multi-stakeholder approach to capacity-building that addresses technical and policy gaps in all relevant sectors of society was also emphasized. States noted in particular that sustainability in capacity-building can be enhanced by an approach that entails engagement and partnership with local civil society, the technical community, academic institutions and private sector

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

actors and through the creation of expert rosters and hubs. In this regard, it was also emphasized that national approaches to ICT security could benefit from adopting a cross-sectoral, holistic and multi-disciplinary approach to capacity-building, including by enhancing national coordination bodies with the participation of relevant stakeholders to assess the effectiveness of programmes. Such an approach may also help address challenges posed by newly emerging technologies.

109. 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.

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

Regular Institutional Dialogue

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

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

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

building among States; and hold regular review conferences. Broad participation and consultations were also foreseen under the PoA proposal.

114. States noted the establishment, through resolution 75/240 of 31 December 2020, of a new open-ended working group on security of and in the use of information and communications technologies 2021–2025, which shall start its activities upon the conclusion of the work of the Open-ended Working Group established pursuant to resolution 73/27 and consider its outcomes.

115. States also expressed the desire for the international community to ultimately return to a single consensus-based process under UN auspices. In this regard, States noted that different proposed formats for dialogue are not necessarily mutually exclusive. It was suggested that different formats could be complementary or could be merged in order to capitalize on the unique features of each and reduce duplication of efforts.

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

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

D. Final Observations

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

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

120. The OEWG has demonstrated the international community's collective resolve to continue to work together towards an open, secure, stable, accessible and peaceful ICT environment of benefit to all States and peoples. Throughout their deliberations at the OEWG, States underscored the linkages and synergies between each of the elements of its mandate: international law governs States actions and voluntary, non -binding norms provide additional guidance on what constitutes responsible state behaviour [*consistent with para 13*]. Both these elements reflect expectations of behaviour regarding State uses of ICTs in the context of international security. In this way, they also contribute to confidence-building by increasing transparency and cooperation between States and for reducing the risk of conflict. Capacity- building in turn is an enabler for all States to contribute to increased stability and security globally. Together, these elements constitute a global framework of cooperative measures to address existing and potential threats in the sphere of ICTs. Regular institutional dialogue will provide the opportunity for this framework to be further developed and operationalized through advancing common understandings, exchanging lessons learned and good practices in implementation, building confidence and increasing capacity amongst States.

120 bis Throughout the OEWG process, States participated consistently and actively, resulting in an extremely rich exchange of views. Part of the value of this exchange is that diverse perspectives, new ideas and important proposals were put forward even though they were not necessarily agreed by all States; including the [possibility question/idea] of additional legally binding obligations. The diverse perspectives are reflected in the attached Chairs Summary of the discussions and summary of specific language proposals under agenda item "Rules, norms and principles". These perspectives should be further considered in future UN processes, including in the Open-Ended Working Group established pursuant to General Assembly resolution 75/240 [*Text draws from para 78. In the event time doesn't allow for negotiation of discussion section, this para should be added to explain a Chair's Summary; which would comprise two parts: Part One Summary of discussions (Section C) and Part 2 Summary of specific language proposals under agenda item "Rules, norms and principles" (the existing non-paper, with "non-paper" removed from its title).*

———————