Joint comments from the EU and its Member States on the initial ‘pre-draft’ report of the Open-Ended Working Group on developments in the field of Information and Telecommunication in the context of international security.

1. The EU and its Member States welcome the initial “pre-draft” report of the Open-Ended Working Group (OEWG) on developments in the field of Information and Telecommunication in the context of international security, presented by the OEWG Chair.

2. The Candidate Countries the Republic of North Macedonia, Montenegro and Albania, the country of the Stabilisation and Association Process and potential candidate Bosnia and Herzegovina as well as the Republic of Moldova and Georgia, align themselves with the following comments.

3. This initial “pre-draft” reflects the rich and substantive discussion at the first and second sessions of the OEWG, in particular the widespread acknowledgement that we are not starting from scratch and that the consecutive reports of the UN Group of Governmental Experts (UN GGE) are the foundation to provide guidance for additional discussions and recommendations. Through the remaining intersessional meetings and the final OEWG session, we aim to adopt by consensus a comprehensive document with realistic outcomes.

4. The EU and its Member States believe that the role of other stakeholders should be more evenly reflected in the report, either by dedicating a specific section in the introduction and in the recommendations, which highlights both the contributions and the need for further cooperation with each group of stakeholders (government, business, non-governmental organizations and academia), or by allowing a dedicated paragraph in each thematic section of the report, or both. In addition, we recommend that the informal conclusions drafted by Mr David Koh, Chair of the intersessional multi-stakeholder meeting (2-4 December 2019), should be annexed to the OEWG final report.

5. In addition, the EU and its Member States, welcoming the wide variety of actors participating in OEWG process and the inclusiveness of the OEWG mandate, underline the importance of promoting gender equality, as well as narrowing the “gender digital divide” and support further effective and meaningful recommendations in this regard.

6. The EU and its Member States acknowledge the urgency and the potential far reaching impact of the COVID-19 crisis posing particular challenges to all UN Member States and their societies. The EU and its Member States call upon the Chair and Delegations to consider how best the process should fulfil its mandate in order to adopt a consensual report, as well as demonstrate the much needed flexibility to address these issues.
On existing and potential threats

7. The EU and its Member States are concerned by the rise of malicious behaviour in cyberspace by both state and non-state actors, including the abuse of Information and Communications Technologies (ICTs) for malicious purposes as well as cyber-enabled theft of intellectual property. Such behaviour undermines and threatens the integrity, security, economic growth and stability of the global community, and can lead to destabilising and cascading effects with enhanced risks of conflict.

8. The EU and its Member States believe that it is important to recall that some ICT technologies related to cyberspace can be of dual nature and that they can be deployed for both civilian and military applications. The unique character of ICT technologies underscores the importance of maintaining a technology neutral approach in the course of our work, as recognized by previous UN GGE reports. This point should be further highlighted in the final report.

9. The EU and its Member States underline the severity of threats against critical infrastructure. Critical infrastructures are no longer confined to the borders of States but are increasingly becoming transnational and interdependent; the scale of the threat remains a major concern. Therefore, the protection of critical infrastructure is of such importance, that the EU and its Member States would suggest for the OEWG report to consider these threats, including the one posed against the general availability or integrity of the public core of the Internet.
On international law

10. The EU and its Member States reaffirm that a universal cyber security framework can only be grounded in existing international law, including the Charter of the United Nations in its entirety, international humanitarian law, and international human rights law. Addressing issues as to how existing international law and international humanitarian law, including the principles of humanity, necessity, proportionality and distinction, apply to the use ICTs by States increases accountability and transparency and reduces uncertainty and the risk of misunderstandings, which is fundamental to maintaining long-term peace and stability and reducing the risk of conflict in cyberspace, and should be referred to as such in the final report.

11. In this context, the EU and its Member States welcome paragraph 25 of the initial pre-draft report, which recalls the view that international humanitarian law (IHL) is fully applicable in cyberspace and that IHL applicability in cyberspace should not be misunderstood as legitimizing the use of force between States in this domain, which is governed by the Charter of the United Nations. International law, including the applicability of IHL in cyberspace, sets clear boundaries for the legality of the use of force between states, also in times of conflict.

12. The EU and its Member States continue to support ongoing efforts to promote the application of existing international law to cyberspace, including on exchanging information and best practices thereon, and encourage all UN Member States to share with other countries their national positions on their understanding on the application of international law as applied to the use of ICTs by states. The EU fully supports efforts to bring more clarity on how existing international law applies in order to enhance common understanding on this issue.

13. The EU and its Member States are of the view that the report should more clearly distinguish between on the one hand the consensus reached in 2013 and 2015 and on the other hand the discussion at the OEWG meetings on topics beyond this consensus. In this regard, the 2013 and 2015 GGE consensus reports constitute the baseline for our discussion. This was universally acknowledged during the meetings and should be acknowledged as such in the report. Although paragraph 27 fails to mention all international law aspects as included in the previous consensus reports, the various questions on how international law applies in the use of ICTs raised should belong in a separate paragraph to the mentions by any means to a new instrument.

---

1 In this context, the EU and it Member States recall that at the second substantive session of the OEWG a number of states made references to the Freedom Online Coalition Statement (FOC) on Human Rights Impact of Cybersecurity Laws, Practices and Policies, which expresses deep concern regarding “the practices by some States of asserting excessive control over the Internet under the pretence of ensuring national security while disregarding international human rights law and the principles of an open, free, secure, interoperable and reliable Internet.”
14. The EU and its Member States express their concern regarding calls for the need to adapt existing international law as a means to or to develop a new legal instrument. At this stage, the EU and its Member States do not see the necessity for the establishment of any structure to develop any new international legal instrument for cyber issues. In addition, the EU and its Member States are strongly concerned about the risk of entering into a divisive and lengthy process with no substantive and constructive result which risks undermining the ongoing practical efforts to tackle the real, pertinent and pressing problem of increasing cyber incidents, and also risks impacting on work aimed at preventing conflict prevention and promoting stability in cyberspace.

15. The EU and its Member States remain ready to consider recommendations that aim to advance greater stability in cyberspace, through the reaffirmation of our commitments to adhere to existing international law and the eleven norms of responsible behaviour in cyberspace in the use of ICTs in cyberspace. These recommendations should focus on the implementation and a better understanding of the norms.

16. The EU and its Member States reaffirm their commitment to the settlement of international disputes in cyberspace by peaceful means to contribute to conflict prevention, the mitigation of cybersecurity threats and greater stability in international relations. In this regard, the EU and its Member States have developed a “cyber diplomacy toolbox” that allows the EU and its Member States to use Common Foreign and Security Policy measures through various joint policies and, when necessary, to respond to malicious cyber activities from cooperation and stabilisation measures to restrictive measures, as well as attribution. Attributing malicious cyber activities remains a sovereign decision by a State. The EU and its Member States recall the existing norms and mechanisms for the settlement of disputes, including the Security Council and the International Court of Justice.

17. Furthermore, the EU and its Member States note that we should develop ways and practical means to build capacities for States in the areas of international law, national legislation and policy in order to enhance a common understanding as to how existing international law applies to the use of ICTs by States.

18. The EU and its Member States note the recommendation for the International Law Commission (ILC) to 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 legal norms and mechanisms for the settlement of disputes, including the Security Council and the International Court of Justice.

---

security. However, the duration of such effort, the amount of state law and practice and whether the ILC is able to add another comprehensive study to their program of work at this stage should be carefully considered before being formulated as a recommendation, as well as making such request.
On rules, norms and principles for responsible state behaviour

19. The EU and its Member States welcome the repeated call upon States to be guided in their use of ICTs by the 2015 GGE report, consensually endorsed by the UN General Assembly (UNGA) in resolution 70/237, and on further implementation of these agreed norms and confidence building measures, which play an essential role in maintaining peace and preventing conflict.

20. The EU and its Member States encourage focusing our collective efforts on advancing the implementation of said norms. As such, the recommendations should emphasize the need to share best practices on the implementation of norms of responsible State behaviour in order to further guide and contribute to the dissemination of responsible endeavours. The recommendation could also add a layer of understanding by deepening the previously agreed norms including the principles of, and recommendations for, implementation such as those proposed by Netherlands, Croatia, France, Finland and Slovenia. Furthermore, the EU and its Member States will contribute to the discussion and guidance through sharing existing efforts on the implementation of 2015 UN GGE norms.

21. The EU and its Member States recall that important efforts have been made by other intergovernmental processes under UN auspices, including the ongoing UN GGE on responsible behaviour in cyberspace in the context of international security and multi-stakeholder fora, which can be used as guidance on further implementation of the existing UN GGE reports. The OEWG is encouraged to give careful consideration to the recommendations developed in these fora as potentially highly relevant in the OEWG context.

---

4 Netherlands’ Position Paper on the UN OEWG on developments in the field of ICTs in the context of international security and UN GGE on advancing responsible State behaviour in cyberspace in the context of international security; and Croatia, Finland, France and Slovenia non paper on deepening our understanding on GGE norms on responsible behaviour (FFT Paper).

5 Such as for example the Paris Call for trust and security in cyberspace or the Global Commission on the Stability of Cyberspace (GCSC).
On confidence building measures

22. With regard to confidence-building measures (CBMs), the EU and its Member States underline the importance of CBMs as a practical means of preventing conflicts.

23. The EU and its Member States welcome the initiative to establish a mechanism to share best practices on CBMs, in coordination with interested regional and sub-regional bodies, without prejudice to the further development and implementation of CBMs at different levels. Advancing the operationalisation of such a mechanism should focus on voluntary cooperation with other States, including through existing fora, on their implementation, and should not pre-empt the development and implementation of additional CBMs, notably in regional organizations.

24. As proposed, the OEWG should consult with relevant regional organizations on CBM implementation in order to share best practices in view of the development and implementation of CBMs at the global level, without duplicating any regional efforts, with an aim as a first step to increase transparency; for instance, through the establishment of a global registry of national Points of Contacts. Such coordination between the relevant part of the United Nations system and interested regional organizations should be conducted in accordance with the decision-making processes of these regional organizations.
On capacity building

25. The EU and its Member States underline the importance of capacity-building as a means to strengthen resilience globally, with particular attention to developing countries.

26. The EU and its Member States note the recommendation to establish a global pairing mechanism for enhancing coherence in capacity-building efforts in the use of ICTs and would welcome dedicated discussions on the form of a facilitation mechanism, including on the relevant issues to address, such as financial aspects, scope, etc, bearing in mind that such mechanism should contribute to existing global multi-stakeholder efforts while avoiding duplication. As a first step, the EU and its Member States stand ready to share additional information on their existing capacity-building programmes, and invite developing countries and other potential partners to further specify their needs and expectations in this area.

27. The EU and its Member States actively promote the Busan Principles, namely ownership, sustainability, inclusive partnerships and shared responsibility, trust, transparency and accountability to guide ICT-related capacity-building efforts in the field of international security.

28. In addition, the EU and its Member States believe that ICT-related capacity-building efforts in the field of international security should also be guided by the following principles:
   a. the understanding that existing international law and existing norms apply in cyberspace;
   b. rights-based and gender-sensitive by design, with safeguards to protect fundamental rights and freedoms;
   c. in line with a democratic and efficient multi-stakeholder internet governance model;
   d. supporting the principles of open access to the Internet for all without undermining the integrity of infrastructure, hardware and services;
   e. supporting a shared responsibility approach that entails involvement and partnership across public authorities, the private sector and citizens and promoting international cooperation.

29. The EU and its Member States also support the recommendation to further cooperate to build capacity to identify and protect national and transnational critical infrastructure, as well as supranational critical information infrastructure – which has been a long-standing priority for the EU. This is why the EU is sponsoring, in cooperation with Singapore, a CBM on the Protection of ICT Enabled Critical Infrastructures, within the ASEAN Regional Forum (ARF), and would encourage sharing best practices on the implementation progress of this CBM in order to support our work.
On regular institutional framework

30. The EU and its Member States emphasize that any regular institutional framework should respect a number of principles: avoiding duplication of existing work, be consensus-driven, include open-ended consultations where appropriate with interested stakeholders, and support dialogue that provides for results-oriented, expert discussions, and that takes forward work in practical and tangible manner.

31. Bearing in mind the position of the EU and its Member States that the time is not appropriate to make any recommendation on a regular institutional framework, many provisions for any regular institutional framework, including the purpose, scope, financing, participation etc. will require further discussion, and we should aim to resume our work to support both a complementary approach with the UN GGE on advancing responsible behaviour, which will finish its work in 2021, and a constructive approach to build upon the work of both groups.
General remarks on the recommendations

32. The EU and its Member States take note of the recommendations presented by the OEWG Chair in his initial “pre-draft” report and welcome these efforts. The EU and its Member States are supportive of recommendations that facilitate practical implementation of norms of responsible State behaviour and CBMs, with the aim of making tangible progress towards greater stability in cyberspace. In that regard, we encourage the second “pre-draft” report to delineate clearly what would be addressed in the regular work of the Secretary General, such as sharing best practices and national views on the different issues of OEWG’s mandate, from the establishment of a global repository, by defining the scope and coordination instruments, including financial aspects. The purpose of such clarifications would be to avoid overloading our work and duplicating ongoing efforts, as well as to ensure that existing instruments are used appropriately and efficiently.