United Nations A/AC.290/2021/CRP.3

General Assembly

Conference room paper
10 March 2021

English only

Open-ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security
Third substantive session
8–12 March 2021

Chair's Summary

Australian comments: *the purpose of these comments is to ensure key Australian positions summarized in this document are reflected accurately. These comments do not represent Australia's complete position, nor provide Australian responses to the views of other states represented herein, nor do these comments engage on the question of which views summarized were the views of 'states' vs 'some states' (noting para 3 below, that this document 'should not be seen as reflecting the consensus view of States on any specific points covered in it').*

A. Context

1. 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 in the context of international security. In addition to the many areas of agreement reflected in its 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.

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

3. This summary is issued under the responsibility of the Chair and reflects his understanding of the main points that were discussed during the meetings of the Open-ended Working Group. It may not reflect the full contributions of all delegations and should not be seen as reflecting the consensus view of States on any specific points covered in it. The full compendium of national statements and proposals that were submitted for circulation is available at https://www.un.org/disarmament/open-ended-working-group.

B. Overview of Discussions

4. The OEWG process offered an opportunity for all States to express their views, concerns and aspirations in a democratic, transparent and inclusive manner. While the OEWG sought to identify areas of convergence and consensus, its discussions were also a record of the diversity of perspectives, ideas and proposals of Member States, and may serve as a useful basis for future work seeking to further develop common understandings on the use of ICTs by States in the context of international security.

5. Throughout their deliberations at the OEWG, States underscored the linkages and synergies between each of the elements of its mandate: international law governs actions and relations between States and voluntary, non-binding norms provide additional guidance on what constitutes responsible State behaviour. 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.

Threats

6. 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.

7. 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 recognized the legitimate right of militaries to develop and use ICT capabilities noting~~ed~~ that the threat lies in a States' use of such capabilities contrary to their obligations under international law, as well as the agreed voluntary norms of responsible state behaviour. 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.

8. 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

9. 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.

10. 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 and some States noted with concern that such measures impede~~s~~ 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.

11. Specific principles of international law 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.

12. 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.

13. 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.

14. 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 conduct of their organs and of persons or entities exercising elements of governmental authority ~~entities owned by or under the control of the State.~~ as well as conduct which they otherwise direct or control.

15. 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.

16. Recalling that the question 'if international law applies to state conduct in cyberspace' has been resolved in the affirmative and that the focus is now on *how* it applies, States discussed how to address this question. Noting the agreement that existing international law (complemented by voluntary norms of responsible state behavior, confidence building measures and capacity building) already provides a binding framework for addressing State conduct in cyberspace, some States expressed the view that the most efficient and effective way to address outstanding questions is for States to publicly articulate views on the application of specific rules of international law and to behave consistent with those positions. If States are committed, this process could quickly deliver clarity and deepen understandings on key questions of how international law applies to state conduct as well as contributing to the development of applicable customary international law. Development of norms implementation guidance would complement efforts to clarify responsible State behavior in cyberspace, as would capacity building to facilitate broad and meaningful participation. Combined, this would promote more effective implementation and greater adherence to international law and the agreed norms, as well as a stronger basis for holding States accountable for their actions in cyberspace. This path would also avoid protracted treaty negotiations, which may give rise to proposals that seek to erode the full suite of rights, obligations and protections afforded by existing international law, and which after its negotiation would necessarily require interpretation similar to that described in the preceding sentences. [~~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, a~~n~~ new 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.

17. 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, they nevertheless apply to State activities in cyberspace, and further that *i*nternational law can develop progressively, including through opinio juris and State practice. The possibility over time of developing further complementary binding measures concurrently with the implementation of norms was raised~~.~~. Furthermore, a political commitment was proposed as one possible way forward.

18. 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.

19. 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, [1] 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.

20. 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.

[1] A/RES/75/32.

Rules, Norms and Principles for Responsible State Behaviour

21. In their discussions at the OEWG, States recalled that voluntary, non-binding norms of responsible State behaviour do not alter or replace international law, but rather ~~should be viewed as being~~ they provide additional specific guidance on what constitutes responsible State behaviour 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".

22. 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".[2]

23. 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.

24. 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.

25. During discussions, 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".[3] 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.

[2] A/RES/73/27, operational paragraph 1.
[3] Annexed to this resolution is a Voluntary self-assessment tool for national efforts to protect critical information infrastructures.

26. Further to the above paragraph, written proposals made by States at the OEWG on the elaboration of existing norms, guidance on implementation as well as new norms are annexed to this summary.

27. Some States also noted the proposal for an international code of conduct for information security tabled in 2015.[4]

28. 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 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

29. 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.

30. 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.

31. 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,

[4] A/69/723, referenced in A/70/174, para 12.

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.

32. 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

33. 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[5]. In this regard, States stressed the need for sufficient financial and human resources to be allocated to capacity-building programmes.

34. 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.

35. 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.

[5] 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).

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

37. 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.

38. 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

39. 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.

40. 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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.

Annex [Australia has not provided specific comments on this Annex, but notes that proposals receiving consensus support were reflected in the substantive OEWG report; we look forward to further discussion on the remainder, as appropriate]

Specific language proposals under agenda item "Rules, norms and principles" from written submissions by delegations

Noting that in their written contributions, many delegations made reference to existing norms, the below only reflects additional language proposals.

Armenia

- The states will refrain from any action that might result in attempted disruption of the integrity of critical infrastructures and government activities, and offer through secure channels timely clarifications to prevent further possible escalation.

Australia, Czech Republic, Estonia, Japan, Kazakhstan and United States of America

Text providing guidance on implementation of 2015 norms ¶13(f) and (g)

- In providing guidance for the implementation of these norms, States should note that highlighting particular sectors as critical infrastructure is not intended to be an exhaustive list and does not impact on the national designation, or not, of any other sector, nor does it implicitly condone malicious activity against a category not specified.
- The OEWG developed its report in the context of the COVID-19 pandemic. In these circumstances, the OEWG underscored that all states considered medical services and medical facilities to be critical infrastructure for the purposes of norms (f) and (g).

Belarus

- States should reaffirm their commitments to the principle of abandonment of militarization of existing ICTs and the creation of new ICTs specifically designed to harm information resources, infrastructure and critical facilities of other countries.

Canada

Proposed norms guidance text to include in para 41

While the 2015 GGE norms articulate what actions States should or should not take, States underscored the need for guidance on how to operationalize them, and offered the following guidance on these norms. In the understanding of the OEWG, both the norms and the guidance are without prejudice to, and do not alter or diminish in any way, State's existing rights and obligations under international law.

a. Consistent with the purposes of the United Nations, including to maintain international peace and security, States should cooperate in developing and applying measures to increase stability and security in the use of ICTs and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security; (2015 ¶13(a)).

i. This norm is general in nature. The implementation of the entire range of norms, as well as the specific guidance provided below, will contribute to the further operationalisation of this norm States should take a collaborative approach to working with each other and with non-governmental stakeholders, including industry, academia and civil society.

ii. To do so, States should, as appropriate, and when possible:

- Adopt and implement comprehensive national cyber security strategies. Whenever possible, these should promote international cooperation on cybersecurity

- Establish and maintain incident-response functions, for example, Computer Emergency Response Teams (CERTs) which are able to coordinate, share good practices, and cooperate in response to ICT incidents.
- Publish statements to the effect that they will act in accordance with the framework of responsible State behavior in cyberspace, as articulated in the 2015 UN GGE report
- Participate in regional and bilateral initiatives that aim to develop and implement confidence-building measures.

iii. Member States should be encouraged to compile and streamline the information that they present on their implementation of the accepted norms.

b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences (2015 ¶13(b)).

i. States could establish the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of serious ICT incidents and to determine appropriate responses

ii. Once those structures and processes are in place, States could develop ICT incident assessment or severity templates to evaluate and assess ICT incidents.

iii. Transparency about and harmonization of such templates by regional organizations could ensure commonality in how States consider ICT incidents and improve communication between States. Wherever possible, the templates should be in line with existing practices and avoid duplication.

iv. When considering all relevant information in the case of an ICT incident, States should conduct research into possible gendered impacts, and work inclusively with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of LGBT and women's rights.

v. States should consider the impact of ICT incidents on human rights, including the rights to freedom of expression, association and peaceful assembly, the right to be free from arbitrary or unlawful interference with privacy, as well as the rights of people with disabilities.

vi. States should recognize that responses to security incidents often requires involvement from various stakeholders, not just national CERT/CSIRTs, and improve collaboration through training and capacity building with all stakeholder groups. States should encourage digital security training and other capacity building and assistance by stakeholders, including civil society, aimed at preventing security incidents, particularly to vulnerable communities and other users at risk.

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (2015 ¶13(c)).

i. With respect to the implementation of this norm:
- If a State identifies malicious cyber activity emanating from another State's territory or cyber infrastructure, a first step could be notifying that State. Computer Emergency Response Teams (CERTs) are crucial to being able to identify such activity.
- Given that ICT incidents can emanate from or involve third States, it is understood that notifying a State does not imply responsibility of that State for the incident.
- The notified State should acknowledge receipt of the request via the relevant national point of contact.
- When a State has knowledge that its territory or cyber infrastructure is being used for an internationally wrongful act conducted using ICTs that is likely to produce serious adverse consequences in a State, the former State should endeavor to take reasonable, available and practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences.

- A State may gain knowledge of such an act following a notification from an affected State. Such notification must be made in good faith and should be accompanied with supporting information. Supporting information may include sharing possible Indicators of Compromise (IoCs), such as IP address and computers used for malicious ICT acts and malware information.
- States should be encouraged to ensure that non-State actors, including the private sector, are prevented from conducting malicious ICT activities for their own purposes or those of State or other non-State actors to the detriment of third parties including those located on another State's territory. This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools - certification processes, best-practices guides, response mechanisms to incidents and, as appropriate, national regulations.
- This norm should not be interpreted as requiring a State to monitor proactively all ICTs within its territory, or to take other preventative steps.

ii. A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates.
- In such cases, assistance may be sought from other States, or from a private entity, which if provided should be done in a manner consistent with national law, and international human rights law.

d. States should consider how best to cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats. States may need to consider whether new measures need to be developed in this respect. (2015 ¶13(d)).

i. In implementing this norm, States should:
- Consider, as appropriate, supporting the work of the UN Commission on Crime Prevention and Criminal Justice, including by renewing the mandate of the open-ended intergovernmental Expert Group, and supporting its ongoing efforts to study, in a comprehensive manner, the problem of cybercrime.
- Support the efforts of the United Nations Office on Drugs and Crime to continue to provide, upon request and based on national needs, technical assistance and sustainable capacity-building to Member States to deal with cybercrime, through the Global Programme on Cybercrime and, inter alia, its regional offices, in relation to the prevention, detection, investigation and prosecution of cybercrime in all its forms, recognizing that cooperation with Member States, relevant international and regional organizations, the private sector, civil society and other relevant stakeholders can facilitate this activity.
- Implement existing measures in a manner that is consistent with their obligations and consider taking new measures, such as adopting national legislation to combat cybercrime, in a manner that is consistent with States' human rights obligations and that ensures judicial guarantees.

e. States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions A/HRC/RES/20/8 and A/HRC/RES/26/13 (The promotion, protection and enjoyment of human rights on the Internet), as well as General Assembly resolutions A/RES/68/167 and A/RES 69/166 (The right to privacy in the digital age), to guarantee full respect for human rights, including the right to freedom of expression. (2015 ¶13(e))

i. States should:
- Comply with their obligations under national and international law, when considering, developing or applying national cybersecurity policies or legislation or when designing and putting into place cyber security related initiatives or structures including measures to ensure the protection of all human rights.

- In doing so, States should incorporate perspectives from all relevant and affected stakeholders at the earliest stages of cyber security policy development and implementations to safeguard a holistic consideration of the implications of cybersecurity measures.
- Civil society engagement is particularly important given their role as a key actor in promoting State compliance with their human rights obligations and commitments.
- Take into consideration that individuals have the same rights online as they do offline, and should bear in mind the differential threats that women and individuals belonging to minority and vulnerable groups may experience in the context of human rights.
- Conduct gender audits of national or regional cyber security policies to identify areas for improvement.
- Consider incorporating measures to address the human rights implications of ICTs in their National Action Plans on Business and Human Rights.

f. A State should not conduct or knowingly support ICT activity contrary to its 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 (2015 ¶13(f)).

i. Each State determines which infrastructures or sectors it deems critical, in accordance with national priorities and methods of categorization of critical infrastructure. Examples of critical infrastructure sectors that provide essential public services can include energy, water, sanitation, health, education, finance, transport, telecommunications and crisis response organizations. Critical infrastructure could also include technical infrastructure essential to elections, referenda, or plebiscites and technical infrastructure essential to the general availability or integrity of the Internet. Highlighting these infrastructures as examples by no means precludes States from designating other infrastructures as critical, nor does it condone malicious activity against categories of critical infrastructure that are not specified above.

ii. States should consider the potentially harmful effects of their ICT activities on technical infrastructure essential to the general availability or integrity of the Internet.

g. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions (2015 ¶13(g)).

i. In order to contribute to a global culture of cybersecurity, States should consider, as appropriate, sharing information on best practices for protecting critical infrastructures, including all elements identified in this resolution and on:

    - Baseline security requirements;
    - Incident notification procedures;
    - Incident handling tools and methodologies;
    - Emergency resilience; and
    - Lessons learned from previous incidents.

ii. Capacity-building and other measures to build a global culture of cybersecurity should be developed inclusively and seek to address the gender dimensions of cyber security.

iii. Given the varied and distributed nature of critical infrastructure ownership, States should, as appropriate, and in consultation with the relevant stakeholders, promote minimum standards for the security of critical infrastructures and promote cooperation with the private sector, academia and the technical community in critical infrastructure protection efforts.

iv. States should, as appropriate, participate in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of critical infrastructure that provides services regionally or internationally against existing and emerging threats.

v. Efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation.

vi. In providing guidance for the implementation of norms (f) and (g), States note that highlighting particular sectors as critical infrastructure is not intended to be an exhaustive list, and does not impact on the national designation, or not, of any other sector, nor does it implicitly condone malicious activity against a category not specified.

vii. The OEWG underscored that all States considered healthcare infrastructure, medical services and facilities to be critical infrastructure for the purposes of norms (f) and (g). The need to affirm the protection of health infrastructure was felt particularly strongly given that the OEWG developed its report in the context of the COVID-19 pandemic.

h. States should respond to appropriate requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. States should also respond to appropriate requests to mitigate malicious ICT activity aimed at the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty (2015 ¶13(h)).

i. Implementing this norm involves consideration of appropriate requests for assistance and consideration of the nature of assistance that can be offered in a timely manner. States receiving an appropriate request for assistance following an ICT incident should consider, when possible, reasonable and appropriate:

- Acknowledging receipt of the request via the relevant national point of contact;
- Determining, in a timely fashion, whether it has the capacity and resources to provide the assistance requested. This may include identifying the expertise in the country from a range of stakeholders;
- In its initial response, indicating the nature, scope and terms of the assistance that might be provided, including a timeframe for its delivery; and
- In the event that assistance is agreed upon, promptly providing the arranged assistance.
- Ensuring that requests for assistance, including relevant processes and resources such as frameworks and templates, and responses are consistent with human rights obligations.

ii. Implementation of this norm would be further enabled by the prior existence of national structures and mechanisms, including a national point of contact, templates for assistance requests and confirmation of the assistance to be provided, and through targeted capacity-building and technical assistance. Bilateral and multilateral cooperation initiatives, international and regional organizations and fora can play a role in facilitating their development.

Approaches that could positively contribute to the implementation of this norm could include: greater public-private-CSO collaboration, nationally and internationally, especially to take preventative actions; improving the capacity of incident response teams through a tailored approach to cyber capacity development; and specialised training to build cyber capacity at all levels of States and across society.

i. States should take reasonable steps to ensure the integrity of the supply chain so that end users can have confidence in the security of ICT products. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (2015 ¶13(i)).

i. To implement this norm, States should:

- Take steps, including through existing fora, to prevent the proliferation of malicious ICT tools and techniques. In doing so, States should encourage the legitimate activities

of research communities, academia, industry, law enforcement, CERTs/ CSIRTs and other cyber protection agencies in ensuring the security of their ICT systems.
- Consider the exchange of information on ICTs related vulnerabilities and/or harmful hidden functions in ICT products.
- Work to implement security controls, based in risk management.

j. States should encourage responsible reporting of ICT vulnerabilities and share information on available remedies to such vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure (2015 ¶13(j)).

i. To implement this norm, States should:
   - Establish national structures that enable a responsible reporting and handling of ICT vulnerabilities;
   - Encourage appropriate coordination mechanisms amongst public and private sector entities;

ii. In addition, and to avoid misunderstandings or misinterpretations, including those stemming from non-disclosure of information about potentially harmful ICT vulnerabilities, States are encouraged to share, as appropriate, to the widest possible extent, technical information on serious ICT incidents, by using existing CERT to CERT coordination mechanisms, as well as mechanisms put in place by regional organizations (such as networks of points of contact). States should ensure that such information is handled responsibly and in coordination with other stakeholders, as appropriate.

k. States should not conduct or knowingly support activity to harm the information systems of the authorized emergency response teams (sometimes known as computer emergency response teams or cybersecurity incident response teams) of another State. A State should not use authorized emergency response teams to engage in malicious international activity. (2015 ¶13k)).

China

- States should pledge not to use ICTs and ICT networks to carry out activities which run counter to the task of maintaining international peace and security.

State sovereignty in cyberspace

- States should exercise jurisdiction over the ICT infrastructure, resources as well as ICT-related activities within their territories.
- States have the right to make ICT-related public policies consistent with national circumstances to manage their own ICT affairs and protect their citizens' legitimate interests in cyberspace.
- States should refrain from using ICTs to interfere in internal affairs of other states and undermine their political, economic and social stability.
- States should participate in the management and distribution of international Internet resources on equal footings.

Critical infrastructure protection

- States have the rights and responsibilities regarding legal protection of their critical ICT infrastructures against damage resulting from threats, interference, attack and sabotage.
- States should be committed to refraining from launching cyber attacks on the critical infrastructures of other states.
- States should not exploit policy and technical advantages to undermine the security and integrity of critical

infrastructures of other states.

- States should increase exchanges on standards and best practices with regard to critical infrastructure protection and encourage enterprises to embark on such exchanges.

Data security

- States should take a balanced approach with regard to technical advancement, business development and safeguarding national security and public interests.
- States have the rights and responsibilities to ensure the security of personal information and important data relevant to their national security, public security, economic security and social stability.
- States shall not conduct or support ICT-enabled espionage against other states, including mass surveillance and theft of important data and personal information.
- States should pay equal attention to both development and security, and push for the lawful, orderly and free flow of data. States should facilitate exchanges of best practices and cooperation in this regard.

Supply chain security

- States should not exploit their dominant position in ICTs, including dominance in resources, critical ICT infrastructures and core technologies, ICT goods and services to undermine other states' right to independent control of ICT goods and services as well as their security.
- States should prohibit ICT goods and services providers from illegal obtainment of users' data, control and manipulation of users' devices and systems by installing backdoors in goods. States should also prohibit ICT goods and services providers from seeking illegitimate interests by taking advantage of users' dependence to their products, or forcing users to upgrade their systems or devices. States should request ICT goods and services providers to make a commitment that their cooperation partners and users would be noticed in a timely manner if serious vulnerabilities are detected in their products.
- States should be committed to upholding a fair, just and non-discriminatory business environment. States should not use national security as a pretext for restricting development and cooperation of ICTs and limiting the market access for ICT products and the export of high-tech products.

Counter-terrorism

- States should prohibit terrorist organizations from using the Internet to set up websites, online forums and blogs to conduct terrorist activities, including manufacturing, publication, storage, and broadcasting of terrorist audio and video documents, disseminating violent terrorist rhetoric and ideology, fund-raising, recruiting, inciting terrorist activities etc.
- States should conduct intelligence exchanges and law-enforcement cooperation on countering terrorism. For instance, one state should store and collect relevant online data and evidence in a timely manner upon request from other states for cyber-related terrorism cases, provide assistance in investigation and deliver prompt response.
- States should develop cooperative partnership with international organizations, enterprises and citizens in fighting cyber terrorism.
- States should request Internet service providers to cut off the online dissemination channel of terrorist content by closing propaganda websites and accounts and deleting terrorist and violent extremist content.

Croatia, Finland, France and Slovenia

- States should be encouraged to take measures to prevent non-State actors, including the private sector, from conducting ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory.
- This aim could be achieved by working with the private sector to define permissible actions using a risk-based approach and to develop concrete tools - certification processes, best-practices guides, response mechanisms to incidents and, as appropriate, national regulations.

Cuba

This situation calls for the implementation of specific regulations complementary to international law aimed, among others, at the following equally important elements:

- Preventing the application of unilateral measures and measures against states measures that hinder universal access to the benefits offered by ICTs.
- Mitigating the malignant effects of attribution in the face of cyber-attacks.
- Preventing the militarization of cyberspace.
- Protecting citizens' private data more effectively by promoting international regulations in this respect.
- Complementing legislation on cyberterrorism in order to face cybersecurity incidents and problems, such as cyberattacks.Define by consensus what is understood by a cyberattack.
- Operationalizing the application, with greater objectivity, of the principles of international law in this area.

Czech Republic

- States should not conduct or knowingly support cyber activity that would harm medical services or medical facilities, and should take measures to protect medical services from harm.[6]
- the need to comply with existing obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.[7]
- the need to incorporate perspectives from all relevant and affected stakeholders at the earliest stage of cyber security policy development to ensuring a holistic consideration of the implications of cybersecurity measures for human rights.[8]

Ecuador

- **Guidance** on norm 13.b (GGE 2015)[9]**:**
  i) States could establish the national structures, policies, processes and coordination mechanisms necessary to facilitate careful consideration of severe ICT incidents and to determine appropriate responses;
  ii) then States could develop ICT incident assessment or severity templates to evaluate andassess ICT incidents;
  iii) transparency about and harmonisation of such templates by regional organisations could ensure commonality in how States consider ICT incidents and improve communication between States;
  iv) when considering all relevant information in the case of an ICT incident, States should conduct research on possible gendered impacts, and work inclusively with all stakeholders to understand the broader context of an ICT incident, including its impact on the enjoyment of women's rights.

- following guidance is proposed for the implementation of norm 13.c[10]:
  i) if a State identifies malicious cyber activity emanating from another State's region or cyberinfrastructure, a first step could be notifying that State. Computer Emergency Response Teams (CERTs) are crucial to being able to identify such activity;
  ii) given that ICT incidents can emanate from or involve third States, it is understood that notifying a State does not imply responsibility of that State for the incident;
  iii) the notified State should acknowledge receipt of the request via the relevant national point of contact;
  iv) when a State has knowledge that its territory or cyberinfrastructure is being used for an internationally wrongful act that is likely to produce serious adverse consequences in another State, the former State should endeavour to take reasonable, available and practicable measures within its territory and capabilities, consistent with its domestic and international law obligations, to cause the internationally wrongful act to cease, or to mitigate its consequences;
  v) this norm should not be interpreted as requiring a state to monitor proactively all ICTs within its territory, or to take other preventive steps;
  vi) a State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates;
  vii)in such cases, assistance may be sought from other States, or from a private entity, in a manner consistent with national law. Commitment by states to cooperate with other nations and assist them in the event of a crisis is instrumental, particular emphasis should be made on the differentiated impact that an ICT incident on a specific Infrastructure could have in a developing country.

---

[6] https://www.icrc.org/en/document/norms-responsible-state-behavior-cyber-operations-should-buildinternational-law

[7] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[8] https://freedomonlinecoalition.com/wp-content/uploads/2020/02/FOC-Statement-on-Human-Rights-and-Cyber- Security-07.02.pdf.

[9] in case of ICT incidents, States should consider all relevant information, including the broader context of the event, the challenges of attribution in the ICT environment and the nature and extent of the consequences.

[10] States should not knowingly allow their territory to be used for internationally wrongful act using ICTs.

- The draft should also include new norms; among others the following:
  "States should not conduct ICT operations intended to disrupt the technical infrastructure essential to political processes, such as elections, referenda or plebiscites."

India

- (On PARA 39): Proposal for new norm related to need for an agreed standard of essential security in cyberspace on the most effective ways to optimize the promising technologies while safeguarding the public. To this end, the states shall strongly endorse the widespread adoption and verified implementation of basic cyber hygiene.
- Protection of critical information infrastructure is the responsible behavior of the States. Threat to CII can spoil integrity of information and damage economy and economic development of the nation. States must consider protection of CII with public-private partnership. States should not conduct the ICT operations to disrupt CII. States should not create harmful functions in ICT products. States should be responsible to notify users when significant vulnerabilities are identified and notify to vendors to patch up the vulnerabilities. States should work collaboratively of CII, exchange of information on threats and sharing of mitigation tools and techniques.

Islamic Republic of Iran

- The roles of States, with the primary responsibility for maintaining a secure, safe and trustable ICT environment, should be enhanced in ICT environment governance, including policy and decision making, at global level. The envisaged governance should be realized in a manner which strengthen state sovereignty and shall not affect rights of the states in making their choice of development, governance and legislation models in the ICT environment.
- States should refrain from the threat or use of force against the territorial integrity or political independence of any state within and through ICT environment.
- No state has the right to intervene through cyber-related ways and means, directly or indirectly and for any reason, in the internal or external affairs of other states. All forms of intervention and interference or attempted threat against political, economic, social and cultural systems as well as cyber-related critical infrastructure of the States shall be condemned and prevented. (UNGA resolution 2131 of 21 December 1965)
- States shall not use ICT advances as tools for economic, political or any other type of coercive measures, including limiting and blocking measures against target states. (UNGA resolution 2131 of 21 December 1965)
- States should ensure appropriate measures with a view to making private sector with extra- territorial impacts, including platforms, accountable for their behaviour in the ITC environment. States must exercise due control over ICT companies and platforms under their Page 8 of 11 jurisdiction, otherwise they are responsible for knowingly violating national sovereignty, security and public order of other states.
- States should refrain from, and prevent, abusing ICT supply chains developed under their control and jurisdiction, to create or assist development of vulnerability in products, services and maintenance compromising sovereignty and data protection of the target states.

Japan

Japan's new proposal to the OEWG is to add the following language as guidance to norm (i) on ensuring the integrity of supply chain:

- "States have the right and responsibility to ensure the use of trusted suppliers and vendors for ICT equipment and systems, particularly to address national security concerns and protection of privacy. Reasonable steps may include legislation or administrative measures to secure supply chain security, to support development of reliable and trustworthy technology and industry, to diversify suppliers."

Netherlands

- "State and non-state actors should neither conduct nor knowingly allow activity that intentionally and substantially

damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace" [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g)

- "State and non-state actors must not pursue, support or allow cyberoperations intended to disrupt the technical infrastructure essential to elections, referenda or plebiscites," [would be] guidance for implementation of UN GGE 2015 recommendation 13(f) and therefore bringing this also under the scope of UN GGE 2015 recommendation 13(g)

Non-Aligned Movement

- Member States should be encouraged to compile and streamline the information that they presented on their implementation of international rules and the relevant proposed repository, with a view to regulating specific aspects of State use of ICTs from the international security perspective and identifying areas of mutual concern.
- Member States should not conduct or knowingly support any ICT activities that intentionally damages or impairs the use and operation of critical infrastructures of other Member States in contravention of international law.
- Member States should be urged to consider the exchange of information on ICTs related vulnerabilities and/or harmful hidden functions in ICT products and to notify users when significant vulnerabilities are identified.
- Member States should also take into account the Resolution 73/27 of the United Nations General Assembly in the conduct of all ICT related activities.

- NAM reiterates its strong concern at the growing resort to unilateralism, and in this context, underlines that multilateralism and multilaterally agreed solutions, in accordance with the UN Charter, provide the only sustainable method of addressing international security issues.
- NAM reiterates that all States should refrain from the threat or use of force against the territorial integrity or political independence of any state within and through ICTs environment.
- NAM calls for the intensification of efforts towards safeguarding cyberspace from becoming an arena of conflict and ensuring instead the exclusive peaceful uses which would enable the full realization of the potential of ICTs for contributing to social and economic development.
- NAM underscores the importance of avoiding undue restrictions, including through unilateral coercive measures, on the peaceful uses of ICTs, international cooperation or technology transfer.
- NAM emphasizes that States have the primary responsibility to maintain an open, secure, stable, accessible and peaceful ICTs environment.
- NAM stresses that all States should not knowingly conduct or support ICT activity in contrary to their obligations under international law that intentionally damages or impairs the use and operation of critical infrastructures.

Pakistan

- Member States should be encouraged to continue to consider, as appropriate, the possible adoption of a legally and/or politically binding instrument(s) in order to regulate specific aspects of State use of ICTs in the context of international security.
- Member States should be encouraged to arrive at an agreed common definition of what constitutes "critical infrastructure", with a view to agreeing on the prohibition of ICT activitythat knowingly or intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure.
- Member States should be encouraged to cooperate to reach agreement on prohibiting the creation of harmful hidden functions or accumulation of vulnerabilities in ICT products, as well as to commit to responsible and timely reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities.
- Member States should seek to facilitate cooperation with ICT products and services providers to prevent the exploitation or abuse of users' data and privacy.
- Member States should commit not to use ICTs for carrying out activities which run contrary to the maintenance of international peace and security, and refrain from using ICTs to interfere in the internal affairs of other States in any manner.

- Member States should cooperate to address the challenges associated with attribution in the ICT environment. Developing a common approach to attribution in a universal setting under the UN auspices remains the most effective way forward in this regard.
- Member States must be urged to arrive at an agreement on prohibiting ICT activity intended to disrupt the technical infrastructure essential to elections or referendums or plebiscites.
- Member States should be encouraged to develop and implement norms in a manner that avoids undue restrictions on the peaceful uses of ICTs, international cooperation in this field or technology transfer.

Republic of Korea

Suggestion for guidance for GGE 2015 paragraph 13 (c):

- *When an affected State notifies another State that ICT incidents has emanated from or involve the notified State's territory with qualified information, the notified State should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease, or to mitigate its consequences. It should be understood that said notification does not imply responsibility of the notified State for the incident.*
- *It should be understood that said notification does not imply responsibility of the notified State for the incident.*
- *The minimum requirement of qualified information may include Indicator of Compromise (IoC), such as IP address, location of perpetrators and computers used for malicious ICT acts and malware information.*