**Non-paper listing specific language proposals under agenda item "Rules, norms and principles" from written submissions and comments on the initial pre-draft of the OEWG report (as of 27 May 2020)**

***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 37 [of the initial pre-draft]:*

While these 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 the 2015 GGE norms:

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 and does not require its own specific guidance. The implementation of the entire range of norms will contribute to implementing the objectives of this norm.

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

with all stakeholders to understand the larger context of an ICT incident, including its impact on the enjoyment of women's rights.

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 that is likely to produce serious adverse consequences in another 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.
   - 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, in a manner consistent with national 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 the open-ended intergovernmental Expert Group, and 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.
   - 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.

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. States should:

- Consider the potentially harmful effects of their ICT activities on the general functionality of global ICT systems and the essential services that rely on them.

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 national and cross-border critical infrastructure against existing and emerging threats.

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:

- 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 and respond;

- In its initial response, indicating the nature, scope and terms of the

Bilateral and multilateral cooperation initiatives, international and regional organizations and fora can play a role in facilitating their development.

| |
|---|
| 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.

| |
|---|
| 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.

**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

- 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**

- 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.[1]
- the need to comply with existing obligations under international human rights law when considering, developing and applying national cybersecurity policies and legislation.[2]
- 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.[3]

**Ecuador**

- **Guidance** on norm 13.b (GGE 2015)[4]**:**
  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 and assess 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[5]:
  *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*

- 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.

**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]

- 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.

**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 activity that 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.*