*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.

* 1. 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)).
     1. 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.
     2. 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.
     3. Member States should be encouraged to compile and streamline the information that they present on their implementation of the accepted norms.
  2. 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)).
     1. 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
     2. Once those structures and processes are in place, States could develop ICT incident assessment or severity templates to evaluate and assess ICT incidents.
     3. 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.
     4. 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.
     5. 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.
     6. 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.
  3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (2015 ¶13(c)).
     1. 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.
     2. 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.
  4. 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)).

1. 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.
   1. 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))
2. 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.
   1. 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)).
3. 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.
4. States should consider the potentially harmful effects of their ICT activities on technical infrastructure essential to the general availability or integrity of the Internet.
   1. 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 shouldconsider, 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.
    1. 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.
    2. 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.
    3. 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.
    4. Efforts to protect critical information infrastructures should be undertaken with due regard for applicable national laws concerning privacy protection and other relevant legislation.
    5. 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.
    6. 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.
  1. 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)).

1. 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.
2. 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.

* 1. 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)).

1. 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.
  1. 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)).

1. 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;

1. 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.
   1. 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)).