NATIONAL SURVEY OF IMPLEMENTATION OF UNITED NATIONS RECOMMENDATIONS ON RESPONSIBLE USE OF ICTS BY STATES IN THE CONTEXT OF INTERNATIONAL SECURITY

Instructions

The Survey is set out in four parts, reflecting the four elements of the framework of responsible state behaviour in the use of ICTs:

- Part I - International law
- Part II - Norms, rules, and principles for the responsible behaviour of States
- Part III - Confidence building measures
- Part IV - Capacity-building

The Survey asks Member States to list measures taken consistent with the recommendations listed in the 2015 GGE report, as well as to identify challenges to implementation and/or specific gaps in capacity limiting implementation.

For context, relevant extracts from the 2015 GGE report, the 2021 OEWG Report, and the 2021 GGE report are included at the beginning of each part, and examples of implementation are also provided. However, it is recommended that the Survey is read alongside those reports in their entirety.

- Member States are invited to complete the survey at regular intervals, ideally no longer than every 12-24 months.
- An empty or partially- completed survey can be exported in PDF to facilitate internal coordination.
- Previous fully- or partially- completed surveys can be accessed via link generated on the last page of the survey.
- **There are no mandatory questions**, leaving Member States full control over which sections to fill in.
- The Survey includes both single and multiple select questions, with clear instructions marked as appropriate.
- Member States will be able to choose if information on national point(s) of contact will be included in the overall Survey response or saved separately. The difference between these options is further explained in the relevant section of the Survey.
- None of the information provided through the web interface will be automatically saved or used by UNIDIR or be visible to others.
- Member States willing to make their responses publicly available on UNIDIR's Cyber Policy Portal are invited to send by email the final PDF to cyberpolicyportal@un.org . More information on the submission process is available at the end of the Survey. UNIDIR will not edit or otherwise modify submissions by Member States before public release.

Please note that the submission of the completed Survey to UNIDIR for publication on the Cyber Policy Portal does not replace formal national submissions informing the Secretary General of their views and assessments on developments in the field of ICTs in the context of international security.

Note: The Survey may be expanded or updated in the event that the UNGA, by consensus, endorses and calls on Member States to implement the recommendations of a report of the OEWG, GGE or other UN mechanism or body mandated to study existing and potential threats in the sphere of information security and possible cooperative measures to address them.

Part One: International Law

Extract from 2015 GGE report

How international law applies to the use of ICTs (extracted from 2015 GGE Report)

24. The 2013 report stated that international law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. Pursuant to its mandate, the present Group considered how international law applies to the use of ICTs by States.

25. The adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs and to promote an open, secure, stable, accessible and peaceful ICT environment. These obligations are central to the examination of the application of international law to the use of ICTs by States.

26. In considering the application of international law to State use of ICTs, the Group identified as of central importance the commitments of States to the following principles of the Charter and other international law: 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.

27. State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

28. Building on the work of the previous Groups, and guided by the Charter and the mandate contained in General Assembly resolution 68/243, the present Group offers the following non-exhaustive views on how international law applies to the use of ICTs by States:

(a) States have jurisdiction over the ICT infrastructure located within their territory;

(b) In their use of ICTs, States must observe, among other principles of international law, State sovereignty, sovereign equality, the settlement of disputes by peaceful means and non-intervention in the internal affairs of other States. Existing obligations under international law are applicable to State use of ICTs. States must comply with their obligations under international law to respect and protect human rights and fundamental freedoms;

(c) Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the

Group noted the inherent right of States to take measures consistent with international law and as recognized in the Charter. The Group recognized the need for further study on this matter;
(d) The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;
(e) 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 to commit such acts;
(f) States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, 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. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.
29. The Group noted that common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment.

Extract from the 2021 OEWG report

International law (extracted from 2021 OEWG Report)
34. Recognizing General Assembly Resolution 70/237, and also acknowledging General Assembly resolution 73/27, which established the OEWG, States reaffirmed that international law, and in particular the Charter of the United Nations, is applicable and essential to maintaining peace and stability and promoting an open, secure, stable, accessible and peaceful ICT environment. In this regard, States were called upon to avoid and refrain from taking any measures not in accordance with international law, and in particular the Charter of the United Nations. States also concluded that further common understandings need to be developed on how international law applies to State use of ICTs.
35. States also reaffirmed that States shall seek the settlement of disputes by peaceful means such as negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, and resort to regional agencies or arrangements, or other peaceful means of their own choice.
36. States concluded that, given the unique attributes of the ICT environment, deepening common understandings on how international law applies to State use of ICTs, can be developed by exchanging views on the issue among States and by identifying specific topics of international
law for further in-depth discussion within the United Nations.
37. In order for all States to deepen their understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus and common understandings within the international community, States concluded that there was a need for additional neutral and objective efforts to build capacity in the areas of international law, national legislation and policy.
The OEWG recommends that
38. States, on a voluntary basis, continue to inform the Secretary-General of their national views and assessments on how international law applies to their use of ICTs in the context of

international security, and continue to voluntarily share such national views and practices through other avenues as appropriate.
39. States in a position to do so continue to support, in a neutral and objective manner, additional efforts to build capacity, in accordance with the principles contained in paragraph 56 of this report, in the areas of international law, national legislation and policy, in order for all States to contribute to building common understandings of how international law applies to the use of ICTs by States, and to contribute to building consensus within the international community.
40. States continue to study and undertake discussions within future UN processes on how international law applies to the use of ICTs by States as a key step to clarify and further develop common understandings on the issue.

Extract from the 2021 GGE report

International law (extracted from 2021 GGE Report)
69. International law is the basis for States' shared commitment to preventing conflict and maintaining international peace and security and is key to enhancing confidence among States. In its consideration of how international law applies to the use of ICTs by States, the Group reaffirms the assessments and recommendations on international law of the reports of previous Groups of Governmental Experts, notably that international law, and in particular the Charter of the United Nations is applicable and essential to maintaining peace and stability and for promoting an open, secure, stable, accessible and peaceful ICT environment. These assessments and recommendations, in conjunction with other substantive elements of previous reports, emphasize that adherence by States to international law, in particular their Charter obligations, is an essential framework for their actions in their use of ICTs.
70. In this respect, the Group reaffirmed the commitments of States to the following principles of the Charter and other international law: 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.
71. Adding to the work of previous GGEs and guided by the Charter and the mandate contained in resolution 73/266, the present Group offers an additional layer of understanding to the 2015 GGE report's assessments and recommendations of how international law applies to the use of ICTs by States, as follows:
(a) The Group notes that, in accordance with their obligations under Article 2(3) and Chapter VI of the Charter of the United Nations, States party to any international dispute, including those involving the use of ICTs, the continuance of which is likely to endanger the maintenance of ADVANCE COPY 14 international peace and security, shall, first of all, seek a solution by such means as described in Article 33 of the Charter, namely negotiation, enquiry, mediation, conciliation, arbitration, judicial settlement, resort to regional agencies or arrangements, or other peaceful means of their own choice. The Group also notes the importance of other Charter provisions relevant to the resolution of disputes by peaceful means.

(b) The Group reaffirms that State sovereignty and international norms and principles that flow from sovereignty apply to the conduct by States of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory. Existing obligations under international law are applicable to States' ICT-related activity. States exercise jurisdiction over the ICT infrastructure within their territory by, inter alia, setting policy and law and establishing the necessary mechanisms to protect ICT infrastructure on their territory from ICT-related threats.

(c) In accordance with the principle of non-intervention, States must not intervene directly or indirectly in the internal affairs of another State, including by means of ICTs.

(d) In their use of ICTs, and as per the Charter of the United Nations, States shall refrain 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.

(e) Underscoring the aspirations of the international community to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter applies in its entirety, the Group noted again the inherent right of States to take measures consistent with international law and as recognized in the Charter and the need for continued study on this matter.

(f) The Group noted that international humanitarian law applies only in situations of armed conflict. It recalls the established international legal principles including, where applicable, the principles of humanity, necessity, proportionality and distinction that were noted in the 2015 report. The Group recognised the need for further study on how and when these principles apply to the use of ICTs by States and underscored that recalling these principles by no means legitimizes or encourages conflict.

(g) The Group reaffirms that States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. It also reaffirms 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 to commit such acts. At the same time, the Group recalls 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 notes that accusations of organizing and implementing wrongful acts brought against States should be substantiated. The invocation of the responsibility of a State for an internationally wrongful act involves complex technical, legal and political considerations.

72. Without prejudice to existing international law and to the further development of international law in the future, the Group acknowledged that continued discussion and exchanges of views by States, collectively at the United Nations on how specific rules and principles of international law apply to the use of ICTs by States is essential for deepening common understandings, avoiding misunderstandings and increasing predictability and stability. Such discussions could be informed and supported by regional and bilateral exchanges of views between States.

73. In accordance with the Group's mandate, an official compendium [document symbol to be provided] of voluntary national contributions of participating governmental experts on the subject of how international law applies to the use of ICTs by States will be made available on the website of the United Nations Office for Disarmament Affairs. The Group encourages all States to continue sharing their national views and assessments voluntarily through the United Nations Secretary-General and other avenues as appropriate.

1.1 Has your government developed national position(s) on the application on international law to the use of ICTs by states? ☐ Yes | ☐ In progress | ☐ No

If response is yes, direct to question 1.2, If response is In progress, direct to question 1.3, if response is No, direct to question 1.4[1]

1.2 If yes, please extract text below and/or provide links to any public document(s).

Text box for positions (no word limit)

Box to provide URLs to public documents

1.3 If in progress, please specify the current status:

- ☐ Under consideration
- ☐ In active development
- ☐ Final stages of review or approval

[1] Examples could include, but are not limited to, developing national positions with respect to:

- The United Nations Charter and, the law on the use of force (jus ad bellum), including but not limited to
  - Sovereign equality and sovereignty
  - Settlement of disputes by peaceful means
  - Non-intervention in the internal affairs of other States
  - Prohibition on the use of force
  - Inherent right of self-defence, including "armed attack"
- International humanitarian law (jus in bello), including but not limited to
  - "attack" under IHL and the established legal principles of humanity, necessity, proportionality, and distinction
- International human rights law, including but not limited to privacy, freedom of expression, freedom of association

Please provide further details (not mandatory)

1.4 If no, please identify any challenges that inhibit the development of national position(s) on the application on international law to the use of ICTs by states. (Select all that apply)

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Please provide more details

Part Two: Norms, Rules and Principles for Responsible State Behaviour

Extract from the 2015 GGE report (chapeau)

Norms, Rules and Principles for Responsible State Behaviour (Chapeau text extracted from 2015 GGE Report)

[9] *The ICT environment offers both opportunities and challenges to the international community in determining how norms, rules and principles can apply to State conduct of ICT-related activities. One objective is to identify further voluntary, non-binding norms for responsible State behaviour and to strengthen common understandings to increase stability and security in the global ICT environment.*

[*10]* *Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Accordingly, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the expectations of*

the international community, set standards for responsible State behaviour and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

[11] *Previous reports of the Group reflected an emerging consensus on responsible State behaviour in the security and use of ICTs derived from existing international norms and commitments. The task before the present Group was to continue to study, with a view to promoting common understandings, norms of responsible State behaviour, determine where existing norms may be formulated for application to the ICT environment, encourage greater acceptance of norms and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed.*

[12] *The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an international code of conduct for information security (see A/69/723).*

[13] *Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the 2010 and 2013 reports of the previous Groups, the present Group offers the following recommendations for consideration by States for voluntary, non-binding norms, rules or principles of responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:*

Extract from the 2021 OEWG report (in full)

Norms, Rules and Principles for Responsible State Behaviour (text extracted from 2021 OEWG Report)

24. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict. States stressed that such norms reflect the expectations and standards of the international community regarding the behaviour of States in their use of ICTs and allow the international community to assess the activities of States. In accordance with General Assembly resolution 70/237, and acknowledging General Assembly resolution 73/27 States were called upon to avoid and refrain from use of ICTs not in line with the norms for responsible State behaviour.

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

26. While agreeing on the need to protect all critical infrastructure (CI) and critical information infrastructure (CII) supporting essential services to the public, along with endeavouring to ensure the general availability and integrity of the Internet, States further concluded that the COVID19 pandemic has accentuated the importance of protecting healthcare infrastructure including medical services and facilities through the implementation of norms addressing critical infrastructure. such as those affirmed by consensus through UN General Assembly resolution 70/237.

27. States affirmed the importance of supporting and furthering efforts to implement norms by which States have committed to be guided at the global, regional and national levels.

28. States, reaffirming General Assembly resolution 70/237 and acknowledging General Assembly resolution 73/27, should: take reasonable steps to ensure the integrity of the supply chain, including through the development of objective cooperative measures, so that end users can have confidence in the security of ICT products; seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions; and encourage the responsible reporting of vulnerabilities.
29. Given the unique attributes of ICTs, States reaffirmed that, taking into account the proposals on norms made at the OEWG, additional norms could continue to be developed over time. States also concluded that the further development of norms, and the implementation of existing norms were not mutually exclusive but could take place in parallel.
The OEWG recommends that
30. States, on a voluntary basis, survey their national efforts to implement norms, develop and share experience and good practice on norms implementation, and continue to inform the Secretary-General of their national views and assessments in this regard.
31. States should not conduct or knowingly support ICT activity contrary to their 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. Furthermore, States should continue to strengthen measures to protect of all critical infrastructure from ICT threats, and increase exchanges on best practices with regard to critical infrastructure protection.
32. States, in partnership with relevant organizations including the United Nations, further support the implementation and development of norms of responsible State behaviour by all States. States in a position to contribute expertise or resources be encouraged to do so.

Norm A

Norm text

A/70/174 13(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 agreed to be harmful or that may pose threats to international peace and security;*

2.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No
If response is yes or Under Consideration, proceed to question 2.2, If response is No, proceed to question 2.3 [2]

[2] **2021 GGE norm guidance**
19. The maintenance of international peace and security and international cooperation are among the founding purposes of the United Nations. This norm is a reminder that it is the common aspiration and in the interest of all States to cooperate and work together to promote the use of ICTs for peaceful purposes and prevent conflict arising from their misuse.
20. In this regard, and in furtherance of this norm, the Group encourages States to refrain from using ICTs and ICT networks to carry out activities that can threaten the maintenance of international peace and security.
21. The measures recommended by previous GGEs and the OEWG represent an initial framework for responsible State behaviour in the use of ICTs. As further guidance, and to facilitate such cooperation, the Group recommends that States put in place or strengthen existing mechanisms, structures and procedures at the national level such as relevant policy, legislation and corresponding review processes; mechanisms for crisis

2.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

and incident management; whole-of-government cooperative and partnership arrangements; and cooperative and dialogue arrangements with the private sector, academia, civil society and the technical community. States are also encouraged to compile and streamline the information they present on the implementation of the norms, including by voluntarily surveying their national efforts and sharing their experiences.

2.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm B

Norm text

A/70/174 13(b) *– In case of ICT incidents, States should consider all relevant information, including, inter alia, the larger context of the event, the challenges of attribution in the ICT environment, and the nature and extent of the consequences;*

3. 1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 3.2, If response is No, proceed to question 3.3[3]

[3] **2021 GGE norm guidance**

22. This norm acknowledges that attribution is a complex undertaking and that a broad range of factors should be considered before establishing the source of an ICT incident. In this regard, the *caution called for in paragraph 71 (g) of this report and in previous GGE reports can help avert misunderstandings and escalation of tensions between States.*

23. States that are subject to malicious ICT activity, and States from whose territory such malicious ICT activity is suspected to have originated, are encouraged to consult among relevant competent authorities.

24. A State that is victim of a malicious ICT incident should consider all aspects in its assessment of the incident. Such aspects, supported by substantiated facts, can include the incident's technical attributes; its scope, scale and impact; the wider context, including the incident's bearing on international peace and security; and the results of consultations between the States concerned.

25. An affected State's response to malicious ICT activity attributable to another State should be in accordance with its obligations under the Charter of the United Nations and other international law, including those relating to the settlement of disputes by peaceful means and internationally wrongful acts. States could also avail of the full range of diplomatic, legal and other consultative options available to them, as well as voluntary mechanisms and other political commitments that allow for the settlement of disagreements and disputes through consultation and other peaceful means.

26. To operationalize this norm at the national level and facilitate the investigation and resolution of ICT incidents involving other States, States can establish or strengthen relevant national structures, ICT-related policies, processes, legislative frameworks, coordination mechanisms, as well as partnerships and other forms of engagement with relevant stakeholders to assess the severity and replicability of an ICT incident.

27. Cooperation at the regional and international levels, including between national Computer Emergency Response Teams (CERTs)/Computer Security Incident Response Teams (CSIRTs), the ICT authorities of States and the diplomatic community, can strengthen the ability of States to detect and investigate malicious ICT incidents and to substantiate their concerns and findings before reaching a conclusion on an incident.

28. States can also use multilateral, regional, bilateral and multi-stakeholder platforms to exchange practices and share information on national approaches to attribution, including how they distinguish between different types of attribution, and on ICT threats and incidents. The Group also recommends that future work at the

3.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

United Nations could also consider how to foster common understandings and exchanges of practice on attribution.

3.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm C

Norm text

[13(c)] *– States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;*

4.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 4.2, If response is No, proceed to question 4.3[4]

4.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

---

[4] **2021 GGE norm guidance**

29. This norm reflects an expectation that if a State is aware of or is notified in good faith that an internationally wrongful act conducted using ICTs is emanating from or transiting through its territory it will take all appropriate and reasonably available and feasible steps to detect, investigate and address the situation. It conveys an understanding that a State should not permit another State or non-State actor to use ICTs within its territory to commit internationally wrongful acts.

30. When considering how to meet the objectives of this norm, States should bear in mind the following:

(a) The norm raises the expectation that a State will take reasonable steps within its capacity to end the ongoing activity in its territory through means that are proportionate, appropriate and effective and in a manner consistent with international and domestic law. Nonetheless, it is not expected that States could or should monitor all ICT activities within their territory.

(b) A State that is aware of but lacks the capacity to address internationally wrongful acts conducted using ICTs in its territory may consider seeking assistance from other States or the private sector in a manner consistent with international and domestic law. The establishment of corresponding structures and mechanisms to formulate and respond to requests for assistance may support implementation of this norm. States should act in good faith and in accordance with international law when providing assistance and not use the opportunity to conduct malicious activities against the State that is seeking the assistance or against a third State.

c) An affected State should notify the State from which the activity is emanating. The notified State should acknowledge receipt of the notification to facilitate cooperation and clarification and make every reasonable effort to assist in establishing whether an internationally wrongful act has been committed. Acknowledging the receipt of this notice does not indicate concurrence with the information contained therein.

(d) An ICT incident emanating from the territory or the infrastructure of a third State does not, of itself, imply responsibility of that State for the incident. Additionally, notifying a State that its territory is being used for a wrongful act does not, of itself, imply that it is responsible for the act itself.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

4.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)

☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
☐ Other implementation/development barrier (please specify):

Norm D

Norm text

A/70/174 13(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;*

5.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 5.2, If response is No, proceed to question 5.3[5]

5.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

[5] **2021 GGE norm guidance**

31. This norm reminds States of the importance of international cooperation to addressing the cross-border threats posed by criminal and terrorist use of the Internet and ICTs, including for recruitment, financing, training and incitement purposes, planning and coordinating attacks and promoting their ideas and actions, and other such purposes highlighted in this report. The norm recognizes that progress in responding to these and other such threats involving terrorist and criminal groups and individuals through existing and other measures can contribute to international peace and security.

32. Observance of this norm implies the existence of national policies, legislation, structures and mechanisms that facilitate cooperation across borders on technical, law enforcement, legal and diplomatic matters relevant to addressing criminal and terrorist use of ICTs.

33. States are encouraged to strengthen and further develop mechanisms that can facilitate exchanges of information and assistance between relevant national, regional and international organizations in order to raise ICT security awareness among States and reduce the operating space for online terrorist and criminal activities. Such mechanisms can strengthen the capacity of relevant organizations and agencies, while building trust between States and reinforcing responsible State behaviour. States are also encouraged to develop appropriate protocols and procedures for collecting, handling and storing online evidence relevant to criminal and terrorist use of ICTs and provide assistance in investigations in a timely manner, ensuring that such actions are taken in accordance with a State's obligations under international law.

34. Within the United Nations, a number of dedicated fora, processes and resolutions specifically address the threats posed by terrorist and criminal use of ICTs and the cooperative approaches required to address such threats. Relevant General Assembly resolutions include resolution 65/230 on the Twelfth United Nations Congress on Crime Prevention and Criminal Justice establishing an open-ended intergovernmental expert group (IEG) to conduct a comprehensive study of the problem of cybercrime; resolution 74/173 on promoting technical assistance and capacity-building to strengthen national measures and international cooperation to counter the use of ICTs for criminal purposes, including information sharing; and resolution 74/247 on countering the use of ICTs for criminal purposes.

35. States can also use existing processes, initiatives and legal instruments and consider additional procedures or communication channels to facilitate the exchange of information and assistance for addressing criminal and terrorist use of ICTs. In this regard, States are encouraged to continue strengthening efforts underway at the United Nations and at the regional level to respond to criminal and terrorist use of the Internet and ICTs, and develop cooperative partnerships with international organizations, industry actors, academia and civil society to this end.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

5.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)

☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
☐ Other implementation/development barrier (please specify):

Norm E

Norm text

A/70/174 13(e) – *States, in ensuring the secure use of ICTs, should respect Human Rights Council resolutions 20/8 and 26/13 on the promotion, protection and enjoyment of human rights on the Internet, as well as General Assembly resolutions 68/167 and 69/166 on the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression;*

6.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 6.2, If response is No, proceed to question 6.3[6]

[6] **2021 GGE norm guidance**

36. This norm reminds States to respect and protect human rights and fundamental freedoms, both online and offline in accordance with their respective obligations. Requiring special attention in this regard is the right to freedom of expression including the freedom to seek, receive and impart information regardless of frontiers and through any media, and other relevant provisions provided for in the International Covenant on Civil and Political Rights, the International Covenant on Economic, Social and Cultural Rights, and as set out in the Universal Declaration of Human Rights. Observance of this norm can also contribute to promoting non-discrimination and narrowing the digital divide, including with regard to gender.

37. Adoption of the resolutions referenced in this norm and others that have since been adopted is an acknowledgement of new challenges and dilemmas that have emerged around the use of ICTs by States and the corresponding need to address them. State practices such as arbitrary or unlawful mass surveillance may have particularly negative impacts on the exercise and enjoyment of human rights, particularly the right to privacy.

38. In implementing this norm, States should consider specific guidance contained in the cited resolutions. They should also take note of new resolutions adopted since the 2015 GGE report and contribute to new resolutions that may need to be advanced in light of ongoing developments.

39. Efforts by States to promote respect for and observance of human rights and ensure the responsible and secure use of ICTs should be complementary, mutually reinforcing and interdependent endeavours. Such an approach promotes an open, secure, stable, accessible and peaceful ICT environment. It can also contribute to the achievement of the Sustainable Development Goals (SDGs).

40. While recognizing the importance of technological innovation to all States, new and emerging technologies may also have important human rights and ICT security implications. To address this, States may consider investing in and advancing technical and legal measures to guide the development and use of ICTs in a manner that is more inclusive and accessible and does not negatively impact members of individual communities or groups.

41. The Group notes that within the United Nations a number of dedicated fora specifically address human rights issues. In addition, it acknowledges that a variety of stakeholders contribute in different ways to the protection and promotion of human rights and fundamental freedoms online and offline. Engaging these voices in policy-making processes relevant to ICT security can support efforts for the promotion, protection and enjoyment of human rights online and help clarify and minimize potential negative impacts of policies on people, including those in vulnerable situations.

6.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one
Title:
Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

6.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)

☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
☐ Other implementation/development barrier (please specify):

Norm F

Norm text

A/70/174 13(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;*

7.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No
If response is yes or Under Consideration, proceed to question 7.2, If response is No, proceed to question 7.3[7]

7.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

[7] *42. With regard to this norm, ICT activity that intentionally damages critical infrastructure or otherwise impairs the use and operation of critical infrastructure to provide services to the public can have cascading domestic, regional and global effects. It poses an elevated risk of harm to the population, and can be escalatory, possibly leading to conflict.*
43. This norm also points to the fundamental importance of critical infrastructure as a national asset since these infrastructures form the backbone of a society's vital functions, services and activities. If these were to be significantly impaired or damaged, the human costs as well as the impact on a State's economy, development, political and social functioning and national security could be substantial.
44. As noted in norm 13 (g), States should take appropriate measures to protect their critical infrastructure. In this regard, each State determines which infrastructures or sectors it deems critical within its jurisdiction, in accordance with national priorities and methods of categorization of critical infrastructure.
45. The COVID-19 pandemic heightened awareness of the critical importance of protecting health care and medical infrastructure and facilities, including through the implementation of the norms addressing critical infrastructure (such as this norm and norms (g) and (h)). Other examples of critical infrastructure sectors that provide essential services to the public can include energy, power generation, water and sanitation, education, commercial and financial services, transportation, telecommunications and electoral processes. Critical infrastructure may also refer to those infrastructures that provide services across several States such as the technical infrastructure essential to the general availability or integrity of the Internet. Such infrastructure can be critical to international trade, financial markets, global transport, communications, health or humanitarian action. 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 infrastructures that are not specified above.
46. To support implementation of the norm, in addition to consideration of the factors outlined above, States are encouraged to put in place relevant policy and legislative measures at the national level to ensure that ICT activities conducted or supported by a State and that may impact the critical infrastructure of or the delivery of essential public services in another State are consistent with this norm, used in accordance with their international legal obligations, and subject to comprehensive review and oversight.

Title:
Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

7.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)

☐ Other implementation/development barrier (please specify):

Norm G

Norm text

A/70/174 13(g) *– States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account, inter alia, General Assembly resolution 58/199 (2003) "Creation of a global culture of cybersecurity and the protection of critical information infrastructure", and other relevant resolutions;*

8.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 8.2, If response is No, proceed to question 8.3[8]

8.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

[8] **2021 GGE norm guidance**

47. This norm reaffirms the commitment of all States to protect critical infrastructure under their jurisdiction from ICT threats and the importance of international cooperation in this regard.

48. A State's designation of an infrastructure or sector as critical can be helpful for protecting said infrastructure or sector. In addition to determining the infrastructures or sectors of infrastructure it deems critical, each State determines the structural, technical, organizational, legislative and regulatory measures necessary to protect their critical infrastructure and restore functionality if an incident occurs. General Assembly resolution 58/199 on the Creation of a global culture of cybersecurity and the protection of critical information infrastructures and its accompanying annex 3 highlights actions that States can take at the national level to that end.

49. Some States serve as hosts of infrastructures that provide services regionally or internationally. ICT threats to such infrastructure could have destabilizing effects. States in such arrangements could encourage cross-border cooperation with relevant infrastructure owners and operators to enhance the ICT security measures accorded to such infrastructure and strengthen existing or develop complementary processes and procedures to detect and mitigate ICT incidents affecting such infrastructure.

50. Encouraging measures to ensure the safety and security of ICT products throughout their lifecycle or to classify ICT incidents in terms of their scale and seriousness would also contribute to the objective of this norm.

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

8.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm H

Norm Text

A/70/174 13(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 another State's critical infrastructure emanating from their territory, taking into account due regard for sovereignty;*

9.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 9.2, If response is No, proceed to question 9.3[9]

9.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

[9] **2021 GGE norm guidance**

51. This norm reminds States that international cooperation, dialogue, and due regard for the sovereignty of all States are central to responding to requests for assistance by another State whose critical infrastructure is subject to malicious ICT acts. The norm is particularly important when dealing with those acts that have the potential to threaten international peace and security.

52. Upon receiving a request for assistance, States should offer any assistance they have the capacity and resources to provide, and that is reasonably available and practicable in the circumstances. A State may choose to seek assistance bilaterally, or through regional or international arrangements. States may also seek the services of the private sector to assist in responding to requests for assistance.

53. Having the necessary national structures and mechanisms in place to detect and mitigate ICT incidents with the potential to threaten international peace and security enables the effective implementation of this norm. Such mechanisms complement existing mechanisms for day-to-day ICT incident management and resolution. For example, a State wishing to request assistance from another State would benefit from knowing who to contact and the appropriate communication channel to use. A State receiving a request for assistance needs to determine, in as transparent and timely a fashion as possible and respecting the urgency and sensitivity of the request, whether it has the capabilities, capacity and resources to provide the assistance requested. States from which the assistance is requested are not expected to ensure a particular result or outcome.

54. Common and transparent processes and procedures for requesting assistance from another State and for responding to requests for assistance can facilitate the cooperation described by this norm. In this regard, common templates for requesting assistance and responding to such requests can ensure that the State seeking assistance provides as complete and accurate information as possible to the State from which it seeks the assistance, thereby facilitating cooperation and timeliness of response. Such templates could be developed voluntarily at the bilateral, multilateral or regional level. A common template for responding to assistance requests could include elements that acknowledge receipt of the request and, if assistance is possible, an indication of the timeframe, nature, scope and terms of the assistance that could be provided.

55. Where the malicious activity is emanating from a particular State's territory, its offer to provide the requested assistance and the undertaking of such assistance may help minimize damage, avoid misperceptions, reduce the risk of escalation and help restore trust. Engaging in cooperative mechanisms that define the means and mode of crisis communications and of incident management and resolution can strengthen observance of this norm.

URL link to public documents, if any:

Describe more initiatives if needed:

9.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm I

Norm Text

A/70/174 13(i)] *– States should take reasonable steps to ensure the integrity of the supply chain, so 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;*

10.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 10.2, If response is No, proceed to question 10.3[10]

10.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

[10] **2021 GGE norm guidance**

56. This norm recognizes the need to promote end user confidence and trust in an ICT environment that is open, secure, stable, accessible and peaceful. Ensuring the integrity of the ICT supply chain and the security of ICT products, and preventing the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions are increasingly critical in that regard, as well as to international security, and digital and broader economic development.

57. Global ICT supply chains are extensive, increasingly complex and interdependent, and involve many different parties. Reasonable steps to promote openness and ensure the integrity, stability and security of the supply chain can include:

(a) Putting in place at the national level comprehensive, transparent, objective and impartial frameworks and mechanisms for supply chain risk management, consistent with a State's international obligations. Such frameworks may include risk assessments that take into account a variety of factors, including the benefits and risks of new technologies.

(b) Establishing policies and programmes to objectively promote the adoption of good practices by suppliers and vendors of ICT equipment and systems in order to build international confidence in the integrity and security of ICT products and services, enhance quality and promote choice.

(c) Increased attention in national policy and in dialogue with States and relevant actors at the United Nations and other fora on how to ensure all States can compete and innovate on an equal footing, so as to enable the full realization of ICTs to increase global social and economic development and contribute to the maintenance of international peace and security, while also safeguarding national security and the public interest.

(d) Cooperative measures such as exchanges of good practices at the bilateral, regional and multilateral levels on supply chain risk management; developing and implementing globally interoperable common rules and standards for supply chain security; and other approaches aimed at decreasing supply chain vulnerabilities.

58. To prevent the development and proliferation of malicious ICT tools and techniques and the use of harmful hidden functions, including backdoors, States can consider putting in place at the national level:

(a) Measures to enhance the integrity of the supply chain, including by requiring ICT vendors to incorporate safety and security in the design, development and throughout the lifecycle of ICT products. To this end, States may also consider establishing independent and impartial certification processes.

(b) Legislative and other safeguards that enhance the protection of data and privacy.

(c) Measures that prohibit the introduction of harmful hidden functions and the exploitation of vulnerabilities in ICT products that may compromise the confidentiality, integrity and availability of systems and networks, including in critical infrastructure.

59. In addition to the steps and measures outlined above, States should continue to encourage the private sector and civil society to play an appropriate role to improve the security of and in the use of ICTs, including supply chain security for ICT products, and thus contribute to meeting the objectives of this norm

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

10.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm J

Norm Text

A/70/174 13(j) *– States should encourage responsible reporting of ICT vulnerabilities and share associated information on available remedies to such vulnerabilities, in order to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure;*

11.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 11.2, If response is No, proceed to question 11.3[11]

11.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

[11] **2021 GGE norm guidance**

60. This norm reminds States of the importance of ensuring that ICT vulnerabilities are addressed quickly in order to reduce the possibility of exploitation by malicious actors. Timely discovery and responsible disclosure and reporting of ICT vulnerabilities can prevent harmful or threatening practices, increase trust and confidence, and reduce related threats to international security and stability.

61. Vulnerability disclosure policies and programmes, as well as related international cooperation, aim to provide a reliable and consistent process to routinize such disclosures. A coordinated vulnerability disclosure process can minimize the harm to society posed by vulnerable products and systematize the reporting of ICT vulnerabilities and requests for assistance between countries and emergency response teams. Such processes should be consistent with domestic legislation.

62. At the national, regional and international level, States could consider putting in place impartial legal frameworks, policies and programmes to guide decision-making on the handling of ICT vulnerabilities and curb their commercial distribution as a means to protect against any misuse that may pose a risk to international peace and security or human rights and fundamental freedoms. States could also consider putting in place legal protections for researchers and penetration testers.

63. In addition, and in consultation with relevant industry and other ICT security actors, States can develop guidance and incentives, consistent with relevant international technical standards, on the responsible reporting and management of vulnerabilities and the respective roles and responsibilities of different stakeholders in reporting processes; the types of technical information to be disclosed or publicly shared, including the sharing of technical information on ICT incidents that are severe; and how to handle sensitive data and ensure the security and confidentiality of information.

64. The recommendations on confidence-building and international cooperation, assistance and capacity-building of previous GGEs can be particularly helpful for developing a shared understanding of the mechanisms and processes that States can put in place for responsible vulnerability disclosure. States can consider using existing multilateral, regional and sub-regional bodies and other relevant channels and platforms involving different stakeholders to this end.

URL link to public documents, if any:

Describe more initiatives if needed:

11.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Norm K

Norm Text

A/70/174 13(k) *– States should not conduct or knowingly support activity to harm the information systems of another State's authorized emergency response teams (sometimes known as CERTS or CSIRTS). A State should not use authorized emergency response teams to engage in malicious international activity;*

12.1 Has your government taken actions consistent with this norm ☐ Yes | ☐ Under consideration | ☐ No

If response is yes or Under Consideration, proceed to question 12.2, If response is No, proceed to question 12.3[12]

12.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

[12] **2021 GGE norm guidance**

65. This norm reflects the fact that CERTs/CSIRTs or other authorized response bodies have unique responsibilities and functions in managing and resolving ICT incidents, and thereby play an important role in contributing to the maintenance of international peace and security. They are essential to effectively detecting and mitigating the immediate and long-term negative effects of ICT incidents. Harm to emergency response teams can undermine trust and hinder their ability to carry out their functions and can have wider, often unforeseen consequences across sectors and potentially for international peace and security. The Group underscores the importance of avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions.

66. In recognition of their critical role in protecting national security, the public and preventing economic loss deriving from ICT-related incidents, many States categorize CERTs/CSIRTs as part of their critical infrastructure.

67. In considering how their actions regarding emergency response teams can contribute to international peace and security, States could publicly declare or put in place measures affirming that they will not use authorized emergency response teams to engage in malicious international activity and acknowledge and respect the domains of operation and ethical principles that guide the work of authorized emergency response teams. The Group takes note of emerging initiatives in this regard.

68. States could also consider putting in place other measures such as a national ICT-security incident management framework with designated roles and responsibilities, including for CERTs/CSIRTs, to facilitate cooperation and coordination among CERTs/CSIRTs and other relevant security and technical bodies at the national, regional and international levels. Such a framework can include policies, regulatory measures or procedures that clarify the status, authority and mandates of CERTs/CSIRTs and that distinguish the unique functions of CERTs/CSIRTs from other functions of government.

URL link to public documents, if any:

Describe more initiatives if needed:

12.3 Please identify any challenges that inhibit the implementation of this norm.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)
- ☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
- ☐ Other implementation/development barrier (please specify):

Part Three: Confidence Building Measures

Extract from 2015 GGE report

Confidence-building Measures (extracted from 2015 GGE Report)

16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:

(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

(b) The development of and support for mechanisms and processes for bilateral, regional, subregional and multilateral consultations, as appropriate, to enhance inter-State confidence-building and to reduce the risk of misperception, escalation and conflict that may stem from ICT incidents;

(c) Encouraging, on a voluntary basis, transparency at the bilateral, subregional, regional and multilateral levels, as appropriate, to increase confidence and inform future work. This could include the voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs; vulnerabilities and identified harmful hidden functions in ICT products; best practices for ICT security; confidence-building measures developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;
(d) The voluntary provision by States of their national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national laws and policies for the protection of data and ICT-enabled infrastructure. States should seek to facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders. These measures could include:
(i) A repository of national laws and policies for the protection of data and ICT-enabled infrastructure and the publication of materials deemed appropriate for distribution on these national laws and policies;
(ii) The development of mechanisms and processes for bilateral, subregional, regional and multilateral consultations on the protection of ICT-enabled critical infrastructure;
(iii) The development on a bilateral, subregional, regional and multilateral basis of technical, legal and diplomatic mechanisms to address ICT-related requests;
(iv) The adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.
17. States should consider additional confidence-building measures that would strengthen cooperation on a bilateral, subregional, regional and multilateral basis. These could include voluntary agreements by States to:
(a) Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents and develop additional technical, legal and diplomatic mechanisms to address ICT infrastructure-related requests, including the consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;
(b) Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;
(c) Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role. States may wish to consider such bodies within their definition of critical infrastructure. States should support and facilitate the functioning of and cooperation among such national response teams and other authorized bodies;
(d) Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, as appropriate, such as information exchange about vulnerabilities, attack patterns and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents and enhancing regional and sector-based cooperation;
(e) Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.
18. The Group reiterates that, given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation. In this

regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums and other international organizations.

Extract from the 2021 OEWG report

Confidence Building Measures (extracted from 2021 OEWG Report)

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

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

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

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

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

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

47. As a specific measure, States concluded that establishing national Points of Contact (PoCs) is a CBM in itself, but is also a helpful measure for the implementation of many other

CBMs, and is invaluable in times of crisis. States may find it useful to have PoCs for, inter alia, diplomatic, policy, legal and technical exchanges, as well as incident reporting and response.

The OEWG recommends that

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

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

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

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

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

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

Extract from the 2021 GGE report

Confidence Building Measures (extracted from 2021 GGE Report)

74. The Group notes that by fostering trust, cooperation, transparency and predictability, confidence-building measures (CBMs) can promote stability and help to reduce the risk of misunderstanding, escalation and conflict. Building confidence is a long-term and progressive commitment requiring the sustained engagement of States. The support of the United Nations, regional and sub-regional bodies and other stakeholders can contribute to the effective operationalization and reinforcement of CBMs.

75. To underpin their efforts to build confidence and ensure a peaceful ICT environment, States are encouraged to publicly reiterate their commitment to, and act in accordance with, the framework for responsible State behaviour referred to in paragraph 2. States are also encouraged to take into consideration the Guidelines for Confidence-building Measures adopted by the United Nations Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H), as well as emerging practices at the regional and sub-regional levels relevant to CBMs and their operationalization.

13.1. Has your government taken actions consistent with the confidence building measures recommendations? ☐ Yes | ☐ Under Consideration | ☐ No

If response is No, proceed to question 13.3; if response is yes or Under Consideration, proceed to question 13.2

13.2 Please provide details below. In addition to listing specific measures, please provide links to any publicly available information.

Initiative one

Title:

Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed

Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

13.3 Please identify any challenges that inhibit the implementation of CBMs.

- ☐ Political barriers (e.g. the issue is not considered priority on the political agenda)
- ☐ Structural/Organizational barriers (e.g. unclear lines of responsibility or ownership of the issue)
- ☐ Personnel barriers (e.g. not sufficient human resources available)
- ☐ Knowledge barriers (e.g. lack of sufficient knowledge on the subject to develop a position – please specify areas requiring further development)

☐ Financial barriers (e.g. not sufficient financial resources available – please specify the impact of this issue)
☐ Other implementation/development barrier (please specify):

13.4 Would you like to nominate appropriate points of contact at the policy and technical levels to address serious ICT incidents ☐ Yes | ☐ No
If response is Yes, proceed to question 13.5; if response is no, proceed to question 14.

Points of Contacts

Points of Contact (extract from 2015 GGE Report)
16. Confidence-building measures strengthen international peace and security. They can increase interstate cooperation, transparency, predictability and stability. In their work to build confidence to ensure a peaceful ICT environment, States should take into consideration the Guidelines for Confidence-building Measures adopted by the Disarmament Commission in 1988 and endorsed by consensus by the General Assembly in resolution 43/78 (H). To enhance trust and cooperation and reduce the risk of conflict, the Group recommends that States consider the following voluntary confidence-building measures:
(a) The identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;
Points of Contact (extract from *2021 OEWG report)*
The OEWG recommends that
51. States, which have not yet done so, consider nominating a national Point of Contact, inter alia, at the technical, policy and diplomatic levels, taking into account differentiated capacities. States are also encouraged to continue to consider the modalities of establishing a directory of such Points of Contact at the global level
Points of Contact (extract from *2021 GGE report)*
76. The identification of appropriate Points of Contact (PoCs) at the policy and technical levels can facilitate secure and direct communications between States to help prevent and address serious ICT incidents and de-escalate tensions in situations of crisis. Communication between PoCs can help reduce tensions and prevent misunderstandings and misperceptions that may stem from ICT incidents, including those affecting critical infrastructure and that have national, regional or global impact. They can also increase information sharing and enable States to more effectively manage and resolve ICT incidents.
77. When establishing PoCs or engaging in PoC networks, States could consider:
(a) Appointing dedicated PoCs at the policy, diplomatic and technical levels and providing guidance on the specific attributes of the PoCs, including expected roles and responsibilities, coordination functions and readiness requirements.
(b) Creating inter- and intra-governmental procedures to ensure effective communication between PoCs during crises. Standardized templates can indicate the types of information required, including technical data and the nature of the request, but be flexible enough to allow for communication, even if some information is unavailable.
(c) Drawing lessons and good practices from regional PoC networks, including with regard to discussing, developing and implementing practical approaches to using PoC networks in national, regional and international contexts, including for early awareness of serious ICT incidents, with the aim of strengthening coordination and information sharing amongst designated PoCs.

78. Addressing global ICT security threats also requires global approaches that are both inclusive and universal. States could invite the United Nations Secretary-General to facilitate voluntary exchanges between all Member States on lessons, good practices and guidance relevant to PoC networks that are already in place at the regional and sub-regional levels. Such work could contribute to discussions relevant to the establishment of a directory of such PoCs at the global level.

Additional instructions:

Completion of this Survey provides an opportunity for countries to nominate (if they have not done so already) and share Points of Contact (POCs). UNIDIR will consolidate the information received and circulate an updated list to all nominated POCs twice a year. POC details will not be automatically included in survey responses, but will be available for download in a separate PDF that Member States can choose to submit to UNIDIR or not. POC details will not otherwise be shared or disseminated.

Once initiated, any communication initiated utilising the points of contact information, and any subsequent action, will proceed by mutual agreement.

13.5 Please provide details below as appropriate to your national circumstances (please select all that apply) [13]

☐ **Central Coordination Authority**

Name:

Email:

Phone number, include country code and area code:

[Languages spoken: drop down box, allow multiple sections]

24 hours ☐ | Business hours only ☐

☐ **Diplomatic**

Name:

Email:

Phone number, include country code and area code:

[Languages spoken: drop down box, allow multiple sections]

24 hours ☐ | Business hours only ☐

☐ **Technical POC (including CERT/CISIRT)**

Name:

Email:

Phone number, include country code and area code:

[Languages spoken: drop down box, allow multiple sections]

24 hours ☐ | Business hours only ☐

[13] Different countries organise themselves differently. Each country should therefore nominate respective point(s) of contact as appropriate to their domestic circumstances. Depending upon national arrangements, the nominated point(s) of contact could be an individual or organisation; countries may choose to provide a single coordination contact, and/or contacts for diplomatic, national security policy coordination, law enforcement and/or technical functions.

☐ **National Security**
Name:
Email:
Phone number, include country code and area code:
[Languages spoken: drop down box, allow multiple sections]
24 hours ☐ | Business hours only ☐
☐ **Law Enforcement**
Name:
Email:
Phone number, include country code and area code:
[Languages spoken: drop down box, allow multiple sections]
24 hours ☐ | Business hours only ☐
☐ **Other**
☐ Name:
☐ Email:
☐ Phone number, include country code and area code:
☐ [Languages spoken: drop down box, allow multiple sections]
☐ 24 hours ☐ | Business hours only ☐

For each set of details provided, confirm check box that requires acknowledgement and consent to the processes of updating and disseminating the list of POCs [a disclaimer will need to be included to ensure compliance with privacy requirements including GDPR)

Part Four: Capacity Building

Extract from 2015 GGE report

International cooperation and assistance in ICT security and capacity-building (extracted from 2015 GGE Report)
19. States bear primary responsibility for national security and the safety of their citizens, including in the ICT environment, but some States may lack sufficient capacity to protect their ICT networks. A lack of capacity can make the citizens and critical infrastructure of a State vulnerable or make it an unwitting haven for malicious actors. International cooperation and assistance can play an essential role in enabling States to secure ICTs and ensure their peaceful use. Providing assistance to build capacity in the area of ICT security is also essential for international security, by improving the capacity of States for cooperation and collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes.
20. The Group endorsed the recommendations on capacity-building in the 2010 and 2013 reports. The 2010 report recommended that States identify measures to support capacity-building in less developed countries. The 2013 report called upon the international community to work together in providing assistance to: improve the security of critical ICT infrastructure; develop technical skills and appropriate legislation, strategies and regulatory frameworks to fulfil their responsibilities; and bridge the divide in the security of ICTs and their use. The present Group also emphasized that capacity-building involves more than a

transfer of knowledge and skills from developed to developing States, as all States can learn from each other about the threats that they face and effective responses to those threats.
21. Continuing the work begun through previous United Nations resolutions and reports, including General Assembly resolution 64/211, entitled "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance:
(a) Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies;
(b) Provide assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchange legal and administrative best practices;
(c) Assist in providing access to technologies deemed essential for ICT security;
(d) Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;
(e) Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders;
(f) Develop strategies for sustainability in ICT security capacity-building efforts;
(g) Prioritize ICT security awareness and capacity-building in national plans and budgets, and assign it appropriate weight in development and assistance planning. This could include ICT security awareness programmes designed to educate and inform institutions and individual citizens. Such programmes could be carried out in conjunction with efforts by international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations;
(h) Encourage further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs.
22. The development of regional approaches to capacity-building would be beneficial, as they could take into account specific cultural, geographic, political, economic or social aspects and allow a tailored approach.
23. In the interest of ICT security capacity-building, States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations. Such initiatives would help to improve the environment for effective mutual assistance between States in their response to ICT incidents and could be further developed by competent international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations.

Extract from the 2021 OEWG report

Capacity Building (extracted from 2021 OEWG Report)

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

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

55. Ensuring an open, secure, stable, accessible and peaceful ICT environment requires effective cooperation among States to reduce risks to international peace and security. Capacity-building is an important aspect of such cooperation and a voluntary act of both the donor and the recipient.

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

Process and Purpose

- *Capacity-building should be a sustainable process, comprising specific activities by and for different actors.*
- *Specific activities should have a clear purpose and be results focused, while supporting the shared objective of an open, secure, stable, accessible and peaceful ICT environment.*
- *Capacity-building activities should be evidence-based, politically neutral, transparent, accountable, and without conditions.*
- *Capacity-building should be undertaken with full respect for the principle of State sovereignty.*
- *Access to relevant technologies may need to be facilitated.*

Partnerships

- *Capacity-building should be based on mutual trust, demand-driven, correspond to nationally identified needs and priorities, and be undertaken in full recognition of national ownership. Partners in capacity-building participate voluntarily.*
- *As capacity-building activities should be tailored to specific needs and contexts, all parties are active partners with shared but differentiated responsibilities, including to collaborate in the design, execution and monitoring and evaluation of capacity-building activities.*
- *The confidentiality of national policies and plans should be protected and respected by all partners.*

People

- *Capacity-building should respect human rights and fundamental freedoms, be gender sensitive and inclusive, universal and non-discriminatory.*
- *The confidentiality of sensitive information should be ensured.*

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

58. States concluded that capacity-building should contribute to transforming the digital divide into digital opportunities. In particular, it should be aimed at facilitating genuine involvement of developing countries in relevant discussions and fora and strengthening the resilience of developing countries in the ICT environment.

59. States concluded that capacity-building can help to foster an understanding of and address the systemic and other risks arising from a lack of ICT security, insufficient coordination between technical and policy capacities at the national level, and the related challenges of inequalities and digital divides. Capacity-building aimed at enabling States to identify and protect national critical infrastructure and to cooperatively safeguard critical

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

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

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

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

The OEWG recommends that

63. States be guided by the principles contained in paragraph 56 in their ICT-related capacity- building efforts in the field of international security, and other actors be encouraged to take these principles into consideration in their own capacity-building activities.

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

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

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

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

Extract from the 2021 GGE report

Capacity Building (extracted from 2021 GGE Report)

87. The Group underscores the importance of cooperation and assistance in the area of ICT security and capacity-building and their importance to all elements of the Group's mandate. Increased cooperation alongside more effective assistance and capacity-building in the area of ICT security involving other stakeholders such as the private sector, academia, civil society and the technical community can help States apply the framework for the responsible behaviour of States in their use of ICTs. They are critical to bridging existing divides within and between States on policy, legal and technical issues relevant to ICT security. They may also contribute to meeting other objectives of the international community such as the SDGs.

88. International cooperation and assistance in ICT security and capacity-building can strengthen States' capacity to detect, investigate and respond to threats and ensure that all States have the capacity to act responsibly in their use of ICTs. They can also help to ensure that all States achieve the necessary levels of protection and security of critical infrastructure, have adequate incident management capacities in place, and can request, or respond to calls for assistance in the event of malicious ICT activity emanating from or affecting their territory.

89. The Group recommends that international cooperation and assistance in ICT security and capacity-building be further strengthened to support States in the following areas:

(a) Developing and implementing national ICT policies, strategies and programmes.

(b) Creating and enhancing the capacity of CERTs/CSIRTs and strengthening arrangements for CERT/CSIRT-to-CERT/CSIRT cooperation.

(c) Improving the security, resilience and protection of critical infrastructure.

(d) Building or enhancing the technical, legal and policy capacities of States to detect, investigate and resolve ICT incidents, including through investment in the development of human resources, institutions, resilient technology and educational programmes.

(e) Deepening common understandings of how international law applies to the use of ICTs by States and promoting exchanges between States, including through discussions at the United Nations in this regard.

(f) Enhancing the technical and legal capacities of all States to investigate and resolve serious ICT incidents.

(g) Implementing agreed voluntary, non-binding norms of responsible State behaviour.

(h) To this end, and as a means to assess their own priorities, needs and resources, States are encouraged to use the voluntary Survey of National Implementation recommended by the United Nations OEWG.

90. In order to bridge digital divides and ensure all States benefit from these and other areas of assistance and capacity-building, States are encouraged to commit, where possible, financial resources as well as technical and policy expertise, and to support countries requesting assistance in their efforts to enhance ICT security.

91. In advancing international cooperation and assistance in ICT security and capacity-building, the Group underscores the voluntary, politically neutral, mutually beneficial and reciprocal nature of capacity-building. In this regard, the Group welcomes the capacity-building principles concerning process, purpose, partnerships and people recommended by the OEWG and encourages all States to be guided by these principles in their efforts to advance cooperation and assistance.

92. Promoting common understandings and mutual learning can also strengthen international cooperation and assistance in the area of ICT security and capacity-building. States should consider approaching cooperation in ICT security and capacity-building in a

manner that is multi-disciplinary, multi-stakeholder, modular and measurable. This can be achieved through working with the United Nations and other global, regional and sub-regional bodies and alongside other relevant stakeholders to facilitate the effective coordination and implementation of capacity-building programmes, and by encouraging transparency and information sharing on their effectiveness.

14.1 Has your government requested, provided, and/or received assistance in ICT security or capacity building during the reporting period in relation to any of the recommendations covered by this Survey? ☐ Yes | ☐ No
If response is No, proceed to question 14.2; if response is yes, proceed to question 15.

14.2 If yes, please provide details

A. Requested

Project one:
Title:
Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

B. Received

Project one:
Title:
Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

C. Provided

Project one:
Title:
Description (200 words max):

Status: ☐ in development; ☐ ongoing; ☐ completed
Lessons learned / comments upon completion; (200 words max):

URL link to public documents, if any:

Describe more initiatives if needed:

Finalization of the Survey

Would you like to submit now your Survey response, excluding information on national point(s) of contact, to UNIDIR for publication on the Cyber Policy Portal?

- ☐ Yes
- ☐ Not now, I will do it separately / at a later stage
- ☐ No

Please note that UNIDIR will publish submitted responses on the Cyber Policy Portal only after verifying the legitimacy of the sender through direct communication with the appropriate Permanent Mission to the United Nations or other relevant national authority. As such, there may be a delay from submission to publication.

Would you like to submit now information on national point(s) of contact, to UNIDIR?

- ☐ Yes
- ☐ Not now, I will do it separately / at a later stage
- ☐ No

☐ I understand that UNIDIR will release completed survey on the Cyber Policy Portal only if such surveys are submitted by email at cyberpolicyportal@un.org and if the sender can be verified.

☐ I understand that authorized representatives of Member States can at any time request that their completed survey is removed from the Cyber Policy Portal by sending an email at cyberpolicyportal@un.org.