16 April 2020

Open Ended Working Group Developments in the field of information and telecommunications in the context of international security

Joint Proposal: Argentina, Australia, Canada, Chile, Denmark, Estonia, France, Indonesia, Kenya, Mexico, the Netherlands, New Zealand, Pacific Island Forum member states, Poland, and South Africa. **Further co-sponsors are invited and welcomed.**

PROPOSED OEWG REPORT TEXT:

Recalling A/RES/70/237 "c*all[ed] upon Member States: to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts*"; and that A/70/74 recommended Member States "*give active consideration to the reports and assess how they might take up these recommendations for further development and implementation"*, this OEWG:

a. recommends the United Nations General Assembly (UNGA) invite Member States, on a voluntary basis, to survey their national implementation of UNGA resolution 70/237 as part of its invitation to Member States to continue to inform the Secretary-General of their views and assessments on the issue of developments in the field of ICTs in the context of international security;

b. recommends Member States be guided in their survey by the attached model "National Survey of Implementation of United Nations General Assembly Resolution 70/237" (the Survey), noting Member States could voluntary submit the Survey triennially, or could complete one part of the survey annually on a rotating basis;

c. requests the Secretary-General (through the UN Office of Disarmament Affairs) to compile national responses to the Survey as part of the annual report to the General Assembly with the views of Member States on the issue;

d. requests Member States to encourage regional organisations and other stakeholders to conduct analysis of the compilation of responses to the Survey with a view to developing targeted capacity building programmes which address any challenges to implementation or gaps in capacity so identified;

e. encourages development of capacity building programs, on the basis of the needs of requesting States, and in accordance with the national policies and priorities defined by Member States, with a view to assist Member States' completion of the Survey upon their request;

f. notes that 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.

16 April 2020

PROPOSED ATTACHMENT TO OEWG REPORT

National Survey of Implementation of United Nations General Assembly Resolution 70/237

Introduction

The cumulative reports of the 2010 (A/65/201), 2013 (A/68/98) and 2015 (A/70/174) *UN Group of Government Experts on Developments in the Field of Information and Communication Technologies in the Context of International Security* (GGE) made recommendations on responsible state behaviour, including with respect to the following four themes:

- How international law applies to the use of information and communication technologies (ICTs)
- Norms, rules and principles for the responsible behaviour of States
- Confidence building measures
- International cooperation and assistance in ICT security and capacity-building

The United Nations General Assembly (UNGA) considered and endorsed – by consensus – the 2010, 2013 and 2015 GGE reports (A/RES/65/41; A/RES/68/243; A/RES/70/237). Of particular relevance:

- the 2015 UNGA Resolution endorsing the 2015 GGE report "*call[ed] upon Member States: to be guided in their use of information and communications technologies by the 2015 report of the Group of Governmental Experts*" (A/RES/70/237 at [2(a)]); and
- the 2015 GGE report recommended Member States *give active consideration to the reports and assess how they might take up these recommendations for further development and implementation* (A/70/74 at [36]).

This *National Survey of Implementation of United Nations General Assembly Resolution A/RES/70/237* (the Survey) collates national take-up of the active recommendations from the 2015 GGE report, with a view to assisting assessment of their further development and implementation.

UN Member States are invited to voluntarily complete the Survey, on a triennial basis, as part of their response to the General Assembly's invitation to Member States to continue to inform the Secretary-General of their views and assessments on the issue of developments in the field of ICTs in the context of international security. Alternatively, Member States are invited to voluntarily complete one part of the Survey on a rolling annual basis.

The Secretary-General (through the UN Office of Disarmament Affairs) will compile national responses to the Survey as part of the annual report of the Secretary-General to the UNGA with the views of Member States on the issue. States, regional organisations, and other stakeholders can then use this compilation of responses to conduct analysis with a view to developing targeted capacity building programs which address any challenges to implementation or gaps in capacity identified.

The Survey is set out in four parts, reflecting the four key themes identified above. The Survey asks Member States to list measures taken consistent with the recommendations listed in the 2015 GGE report, as well as to identify barriers to implementation and/or specific gaps in capacity limiting implementation.

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.

For context, the chapeau paragraphs to the active recommendations from the 2015 GGE report are extracted. The Survey should, however, be read alongside the 2015 GGE report in its entirety.

Part one: how international law applies to the use of ICTs

A/70/174 [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.*

A/70/174 [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.*

A/70/174 [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.*

A/70/174 [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.*

A/70/174 [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/70/174 [28a] *States have jurisdiction over the ICT infrastructure located within their territory*

Question 1

a. Has your government developed a position on the issue(s) identified above?

b. If yes, please provide details including links to any public document(s).

c. If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [28b] *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;*

Question 2

a. Has your government developed a position on the issue(s) identified above?

b. If yes, please provide details including links to any public document(s).

c. If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [28c] *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;*

Question 3

a. Has your government developed a position on the issue(s) identified above?
b. If yes, please provide details including links to any public document(s).
c. If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [28d] *The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;*

Question 4

a. Has your government developed a position on the issue(s) identified above?
b. If yes, please provide details including links to any public document(s).
c. If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [28e] 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;

Question 5

a) Has your government developed a position on the issue(s) identified above?
b) If yes, please provide details including links to any public document(s).
c) If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [28f] 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.

Question 6

a) Has your government developed a position on the issue(s) identified above?
b) If yes, please provide details including links to any public document(s).
c) If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

A/70/174 [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.

Question 7

a. In addition to questions above, has your government developed any other positions that deepen common understandings on how international law applies to State use of ICTs?
b. If yes, please provide details including links to any public document(s).
c. If no, please identify any barriers and/or gaps in capacity that inhibit development of such a position.

Part two: norms, rules and principles for the responsible behaviour of States

A/70/174 [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.*

A/70/174 [*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.*

A/70/174 [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.*

A/70/174 [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).*

A/70/174 [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:*

Norm 1: 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;*

Question 1

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Norm 2: 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;*

Question 2

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***Norm 3: A/70/174 [13(c)]** – States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;*

Question 3

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibits implementation of this recommendation?

***Norm 4: 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;*

Question 4

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***Norm 5: 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;*

Question 5

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***Norm 6: 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;*

Question 6

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***Norm 7: 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;*

Question 7

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Norm 8: 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;*

Question 8

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Norm 9: 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;*

Question 9

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Norm 10: 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;*

Question 10

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Norm 11: 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;*

Question 11

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.
b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Part three: confidence building measures

A/70/174 [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/70/174 [16a] *– 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;*

Question 1

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [16(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;*

Question 2

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [16(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;*

Question 3

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [16(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.

Question 4

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [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/70/174 [17a] *– 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;*

Question 5

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [17b] *– Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;*

Question 6

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [17c] *– 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;*

Question 7

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [17d] *– 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;*

Question 8

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [17e] *– 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.*

Question 9

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [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.*

Question 10

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

Part four: capacity building

A//70/174 [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.*

A//70/174 [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.*

A//70/174 [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/70/174 [21a] – *Assist in strengthening cooperative mechanisms with national computer emergency response teams and other authorized bodies;*

Question 1

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [21b] – *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;*

Question 2

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [21c] – *Assist in providing access to technologies deemed essential for ICT security;*

Question 3

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [21d] –** Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;*

Question 4

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [21e] –** Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders;*

Question 5

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [21f] –** Develop strategies for sustainability in ICT security capacity-building efforts;*

Question 6

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [21g] –** 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;*

Question 7

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [21h] –** Encourage further work in capacity-building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs.*

Question 8

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

***A/70/174 [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.*

Question 9

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?

A/70/174 [23] *- 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.*

Question 10

a. What steps has your government taken consistent with this recommendation? In addition to listing specific measures, please provide links to any publicly available information.

b. Has your government identified any barriers and/or gaps in capacity that inhibit implementation of this recommendation?