Report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security

Letter of transmittal

28 May 2021

I have the honour to submit herewith the consensus report of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security. The Group was established in 2018 pursuant to operative paragraph 3 of General Assembly resolution 73/266.

In this resolution, the General Assembly requested that a group of governmental experts be established in 2019 on the basis of equitable geographical distribution, proceeding from the assessments and recommendations contained in the consensus GGE reports of 2010, 2013 and 2015, to continue to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security, including norms, rules and principles of responsible behaviour of States, confidence-building measures and capacity-building, as well as how international law applies to the use of information and communications technologies by States. The Secretary-General was requested to submit a report on the results of the study to the Assembly at its seventieth-sixth session.

In accordance with the Group's mandate, an official compendium 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 in the original language of submission without translation [document symbol to be provided].

In accordance with the terms of the resolution, experts were appointed from 25 States: Australia, Brazil, China, Estonia, France, Germany, India, Indonesia, Japan, Jordan, Kazakhstan, Kenya, Mauritius, Mexico, Morocco, the Netherlands, Norway, Romania, the Russian Federation, Singapore, South Africa, Switzerland, the United Kingdom of Great Britain and Northern Ireland, the United States of America, and Uruguay. The list of experts is appended to the report.

The Group held four formal sessions: the first from 9-13 December 2019 at United Nations Headquarters, the second from 24-28 February 2020 in Geneva, the third in a virtual format from 5-9 April 2021 and the fourth in a virtual format from 24-28 May 2021. The third session of the Group was postponed pursuant to General Assembly decision 75/551 due to the COVID-19 pandemic. The Group nonetheless continued its work during this time through a series of several intersessional informal consultations. As per its mandate, a series of

consultations with relevant regional organizations and open-ended consultative meetings with Member States were also held in order to engage in interactive discussions and share views.

The Group wishes to express its appreciation for the contribution of the joint Support Team from the United Nations Office for Disarmament Affairs and the United Nations Institute for Disarmament Research.

I also take this opportunity to express my personal gratitude to the Government of Brazil for designating me and to the Group for the honour of the chairmanship. I also thank my fellow Experts, my Brazilian colleagues, members of the joint Support Team and the United Nations Secretariat, in particular the High Representative for Disarmament Affairs, for their support and for sharing their great expertise in a constructive spirit of engagement.

(Signed) Guilherme de Aguiar Patriota
Chair of the Group

I. Introduction

1. The present report reflects the outcome of discussions carried out by the Group of Governmental Experts pursuant to General Assembly resolution 73/266 on 'Advancing responsible State behaviour in cyberspace in the context of international security'. A key portion of the Group's work was conducted during the coronavirus disease (COVID-19) pandemic, which has highlighted the tremendous potential of digital technologies while accelerating the world's dependency on them, thereby further underscoring the importance of responsible behaviour in the use of ICTs in the context of international security.

2. The report builds upon and reaffirms the assessments and recommendations of the 2010, 2013 and 2015 consensus reports of the United Nations Groups of Governmental Experts (GGEs) on existing and emerging threats, norms, rules and principles of responsible State behaviour, international law, confidence-building and international cooperation and capacity-building, which together represent a cumulative and evolving framework for the responsible behaviour of States in their use of ICTs. The Group welcomes the adoption of the consensus report of the United Nations Open-ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, established pursuant to General Assembly resolution 73/27[1], which reaffirms and builds upon this framework.

3. The Group considered the matters under its mandate in light of their relevance to international peace and security. Furthermore, it sought to provide an additional layer of understanding to the assessments and recommendations of previous GGE reports, in order to provide guidance to support their implementation. This additional layer of understanding reaffirms the linkages between the different substantive elements of the Group's mandate and the importance of engaging other actors, including the private sector, civil society, academia and the technical community, where appropriate, in States' efforts to implement these recommendations.

4. The Group acknowledges the important role of regional and sub-regional bodies in taking forward the assessments and recommendations of the reports of the GGEs and in developing region-specific mechanisms and strengthening capacity-building efforts to support their implementation. In accordance with the Group's mandate, these and other relevant insights and experiences were shared with the Group during the informal consultative meetings of the Group with Member States held in New York and through a series of consultations held in collaboration with regional organizations.[2]

5. The Group reaffirms that an open, secure, stable, accessible and peaceful ICT environment is essential for all and requires effective cooperation among States to reduce risks to international peace and security. It is in the interest of all and vital to the common good to promote the use of ICTs for peaceful purposes. Respect for sovereignty and human rights and fundamental freedoms, as well as sustainable and digital development remain central to these efforts.

II. Existing and emerging threats

6. While ICTs and an increasingly digitalized and connected world provide immense opportunities for societies across the globe, the Group reaffirms that the serious ICT threats identified in previous reports persist. Incidents involving the malicious use of ICTs by States and non-State actors have

[1] A/75/816

[2] Reports of the different consultations are available at: https://www.un.org/disarmament/wp-content/uploads/2019/12/gge-chair-summary-informal-consultative-meeting-5-6-dec-20191.pdf and https://www.un.org/disarmament/wp-content/uploads/2019/12/collated-summaries-regional-gge-consultations-12-3-2019.pdf

increased in scope, scale, severity and sophistication. While ICT threats manifest themselves differently across regions, their effects can also be global.

7. The Group underlines the assessments of the 2015 report that a number of States are developing ICT capabilities for military purposes; and that the use of ICTs in future conflicts between States is becoming more likely.

8. Malicious ICT activity by persistent threat actors, including States and other actors, can pose a significant risk to international security and stability, economic and social development, as well as the safety and well-being of individuals.

9. In addition, States and other actors are actively using more complex and sophisticated ICT capabilities for political and other purposes. Furthermore, the Group notes a worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of another State. These uses undermine trust, are potentially escalatory and can threaten international peace and security. They may also pose direct and indirect harm to individuals.

10. Harmful ICT activity against critical infrastructure that provides services domestically, regionally or globally, which was discussed in earlier GGE reports, has become increasingly serious. Of specific concern is malicious ICT activity affecting critical information infrastructure, infrastructure providing essential services to the public, the technical infrastructure essential to the general availability or integrity of the Internet and health sector entities. The COVID-19 pandemic has demonstrated the risks and consequences of malicious ICT activities that seek to exploit vulnerabilities in times when our societies are under enormous strain.

11. New and emerging technologies are expanding development opportunities. Yet, their ever-evolving properties and characteristics also expand the attack surface, creating new vectors and vulnerabilities that can be exploited for malicious ICT activity. Ensuring that vulnerabilities in operational technology and in the interconnected computing devices, platforms, machines or objects that constitute the Internet of Things are not exploited for malicious purposes has become a serious challenge.

12. Capacities to secure information systems continue to differ worldwide, as do the capacities to develop resilience, protect critical information infrastructure, identify threats and respond to them in a timely manner. These differences in capacities and resources, as well as disparities in national law, regulation and practices related to the use of ICTs, and unequal awareness of and access to existing regional and global cooperative measures available to mitigate, investigate or recover from such incidents, increase vulnerabilities and risk for all States.

13. The Group reaffirms that the use of ICTs for terrorist purposes, beyond recruitment, financing, training and incitement, including for terrorist attacks against ICTs or ICT-dependent infrastructure, is an increasing possibility that, if left unaddressed, may threaten international peace and security.

14. The Group also reaffirms that the diversity of malicious non-State actors, including criminal groups and terrorists, their differing motives, the speed at which malicious ICT actions can occur and the difficulty of attributing the source of an ICT incident all increase risk.

III. Norms, Rules and Principles

15. The Group reaffirms with regard to the use of ICTs by States that voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. Norms and existing international law sit alongside each other. Norms do not seek to limit or prohibit action that is otherwise consistent with international law. They reflect the expectations of the international

community and set standards for responsible State behaviour. 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.

16. The Group also underscores the inter-relationship between norms, confidence-building measures, international cooperation and capacity-building. Given the unique attributes of ICTs, the Group reaffirms the observation of the 2015 report that additional norms could be developed over time, and, separately, notes the possibility of future elaboration of additional binding obligations, if appropriate.

17. In addition to work in the United Nations system, the Group acknowledges the valuable experiences on norms implementation emerging at the regional level, including those shared during the informal consultations held with Member States in New York and in collaboration with regional organizations in accordance with its mandate, noting that future work on ICTs in the context of international security should take these efforts into account. The Group also 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).

18. In consensus resolution 70/237, the General Assembly called upon Member States to be guided in their use of ICTs by the 2015 report of the GGE, which included eleven voluntary, non-binding norms of responsible State behaviour. In accordance with its mandate to advance responsible behaviour, the Group has developed an additional layer of understanding to these norms, underscoring their value with regard to the expected behaviour of States in their use of ICTs in the context of international peace and security and providing examples of the kinds of institutional arrangements that States can put in place at the national and regional levels to support their implementation. The Group reminds States that such efforts should be conducted in accordance with their obligations under the Charter of the United Nations and other international law, with a view to preserving an open, secure, stable, accessible and peaceful ICT environment. States are called upon to avoid and refrain from the use of ICTs not in line with the norms of responsible State behaviour.

Norm 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 acknowledged to be harmful or that may pose threats to international peace and security.

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 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.

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

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

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

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.

Norm 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.

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.

Norm 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.

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.

Norm 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.

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.

Norm 13 (g) States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly resolution 58/199.

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.

Norm 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 the critical infrastructure of another State emanating from their territory, taking into account due regard for sovereignty.

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.

[3] A/RES/58/199, which is part of a package of three including GA resolution A/RES/57/239 and A/RES/64/211.

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.

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

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.

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

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.

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

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.

IV. International law

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

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.

V. Confidence-Building Measures

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.

Cooperative measures

Points of Contact

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.

Dialogue and consultations

79. Dialogue through bilateral, sub-regional, regional and multilateral consultations and engagement can advance understanding between States, encourage greater trust and contribute to closer cooperation between States in mitigating ICT incidents, while reducing the risks of misperception and escalation. Other stakeholders such as the private sector, academia, civil society and the technical community can contribute significantly to facilitating such consultations and engagement.

80. Regional bodies have taken significant steps in developing and implementing CBMs that can reduce the risk of misperception, escalation and conflict that may stem from ICT incidents. Engagement in these groupings allows for focus on regional characteristics and concerns, while inter-regional exchanges allow for mutual learning between such organizations. States are encouraged to continue this work, as well as actively engage with those States not currently members of a relevant regional or sub-regional organization.

81. To continue strengthening cooperative measures relevant to national computer emergency response teams and other authorized bodies, States could encourage the sharing and dissemination of information and good practices on establishing and sustaining national CERTs/CSIRTs and on incident management through existing regional and global emergency response organizations and networks. Such encouragement and support for CERTs/CSIRTs would also serve to raise awareness among States of their commitments with regard to CERTs/CSIRTs and other related bodies under norm 13 (k).

Transparency measures

82. Exercising transparency on a voluntary basis through the exchange of national views and practices on ICT security incidents and other related threats and by making ICT security advice, guidance, evidence base and data supporting decisions publicly available is important for building trust and predictability, reducing the possibility of misinterpretation and escalation, and helping organizations and agencies make good risk management decisions.

83. To further advance transparency and predictability of State behaviour, provide exposure to a wider range of views and experiences and enhance State preparedness and early awareness of growing threats, States could consider using bilateral, sub-regional, regional and multilateral fora and informal consultations to voluntarily share: information and good practices, lessons or white papers on existing and emerging ICT security-related threats and incidents; national strategies and standards for vulnerability analysis of ICT products; and national and regional approaches to risk management and conflict prevention, including national approaches to classifying ICT incidents in terms of the scale and seriousness of the incident.

84. States can also avail of these existing fora to clarify positions and voluntarily exchange information on: national approaches to ICT security; data protection; the protection of ICT-enabled critical infrastructure; and ICT-security agency mission and functions, and ICT strategy at the national or organizational level, and the legal and oversight regimes under which they operate.

85. The recommendations on CBMs in previous GGE reports provide a cooperative basis for addressing growing threats to critical infrastructure-related challenges and for implementing the relevant norms. States are encouraged to continue raising awareness on the importance of critical infrastructure protection, promoting information sharing among critical infrastructure stakeholders and sharing of good practices and guidance. Where appropriate, they can use existing platforms and reporting modalities (see paragraph 86) to voluntarily share national views on the classification of critical national infrastructure and critical infrastructure providing essential services regionally or internationally, relevant national policies and legislation, and frameworks for risk assessment and for identifying, classifying and managing ICT incidents affecting critical infrastructure.

86. States could also use United Nations resources such as voluntary reporting to the Secretary-General, the Cyber Policy Portal of the United Nations Institute for Disarmament Research (UNIDIR), as well as the resources of other relevant international and regional organizations to consolidate information and good practices provided voluntarily by States on national strategies, policies, legislation and programmes that address ICT security issues relevant to international security and stability.

VI. International cooperation and assistance in ICT security and capacity-building

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.[4]

[4] OEWG Final Substantive Report para. 65.

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.[5]

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.

VII. Conclusions and Recommendations for Future Work

93. As States become increasingly dependent on ICTs, adhering to a common framework of responsible State behaviour in the use of ICTs in the context of international security is essential for all States to benefit from the technologies and protect against and respond to their misuse.

94. Focusing its efforts on promoting common understandings and effective implementation and building on the recommendations of previous reports, the Group identified and provided greater clarity and guidance on the approaches States can take to ensure that cooperative measures effectively address existing and potential threats in the sphere of ICT security. These approaches are clearly outlined in the report's sections on norms, rules and principles of responsible State behaviour; international law; confidence-building; and international cooperation and capacity-building, each of which takes forward the essential elements of responsible State behaviour developed in previous GGE reports.

95. The Group also identified potential areas for future work, which include but are not limited to:

(a) Increased cooperation at the bilateral, regional and multilateral levels to foster common understandings on existing and emerging threats and the potential risks to international peace and security posed by the malicious use of ICTs, and on the security of ICT-enabled infrastructure.

(b) Further sharing and exchanging of views on norms, rules and principles for responsible State behaviour and national and regional practices in norm and CBM implementation; and on how international law applies to the use of ICTs by States, including by identifying specific topics of international law for further in-depth discussion.

(c) Further strengthening international cooperation and capacity-building on the assessments and recommendations in this report in order to ensure all States can contribute to the maintenance of international peace and security, taking into consideration paragraph 90 above.

[5] OEWG Final Substantive Report para 56.

(d) Identifying mechanisms that facilitate the engagement of other essential stakeholders, including the private sector, academia, civil society and the technical community in efforts to implement the framework of responsible behaviour, where appropriate.

(e) Requesting UNIDIR, which serves all Member States, and encouraging other appropriate think-tanks and research institutions to undertake relevant studies on the topics discussed in this report.

96. The Group encourages the continuation of the inclusive and transparent negotiation process on ICTs in the context of international security under the auspices of the United Nations, including and acknowledging the Open-Ended Working Group on security in the use of information and communication technologies 2021-2025 established pursuant to General Assembly resolution 75/240. The group recommends future work builds upon the cumulative work of the GGEs and the OEWG.

97. The Group encourages States to continue efforts to further the framework of responsible State behaviour within the United Nations and other regional and multilateral forums to support regular dialogue, consultation and capacity-building in an inclusive, consensus-driven, action-oriented and transparent manner. In this regard, and congruent with the outcome of the OEWG, the Group notes a variety of proposals for advancing responsible State behaviour in ICTs, which would, *inter alia*, support the capacities of States in implementing commitments in their use of ICTs, in particular the Programme of Action. In considering these proposals, the concerns and interests of all States should be taken into account through equal State participation at the United Nations. In this regard, the Programme of Action should be further elaborated including at the Open-Ended Working Group process established pursuant to General Assembly resolution 75/240.

98. The Group recommends that Member States be guided by the assessments and recommendations of this report and those of previous GGEs, as well as the conclusions and recommendations of the final report of the OEWG (A/75/816), and consider how these might be further developed and implemented.

List of members of the Group of Governmental Experts on Advancing responsible State behaviour in cyberspace in the context of international security

Australia
Johanna Weaver
Special Adviser to Australia's Ambassador for Cyber Affairs
Department of Foreign Affairs and Trade

Brazil
Guilherme de Aguiar Patriota
Ambassador, Consul General of Brazil in Mumbai

China
Wang Lei
Coordinator for Cyber Affairs, Ministry of Foreign Affairs

Estonia
Heli Tiirmaa-Klaar
Ambassador at Large for Cyber Diplomacy, Director General, Cyber Diplomacy Department, Ministry of Foreign Affairs

France
Henri Verdier
Ambassador for Digital Affairs, Ministry for Europe and Foreign Affairs

Germany
Regine Grienberger (third and fourth session)
Ambassador for Cyber Foreign Policy, Federal Foreign Office

Wolfram von Heynitz (first and second session)
Head of International Cyber Policy Coordination Staff, Federal Foreign Office

India
S. Janakiraman
Joint Secretary and Head of the E-Governance & Information Technology and Cyber Diplomacy Divisions, Ministry of External Affairs

Indonesia
Rolliansyah Soemirat (third and fourth session)
Director for International Security and Disarmament, Ministry of Foreign Affairs

Harditya Suryawanto (second session)
Counsellor, CT & Cyber Issues, Directorate of International Security and Disarmament, Ministry of Foreign Affairs

Grata Endah Werdaningtyas (first session)
Director of International Security and Disarmament, Director for International Security and Disarmament, Ministry of Foreign Affairs

Japan
Takeshi Akahori
Ambassador for United Nations Affairs and Cyber Policy, Ministry of Foreign Affairs

Jordan
Feras Mohammad Abdallah Alzoubi
Chief of National Cyber Security Program Branch, Jordanian Armed Forces

Kazakhstan
Asset Nussupov
Head of Sector, Executive Office of the President of the Republic of Kazakhstan

Kenya
Katherine Getao
Chief Executive Officer, ICT Authority

Mauritius
Kaleem Ahmed Usmani
Head, Mauritius Computer Emergency Response Team (CERT-MU)

Mexico
Gerardo Isaac Morales Tenorio
Coordinator for Multidimensional Security, Ministry of Foreign Affairs

Morocco
Abdellah Boutrig
Colonel Major, Director of Assistance, Training, Control and Expertise, General Directorate of Information System Security, National Defense Administration

Netherlands
Carmen Gonsalves
Head, International Cyber Policy, Ministry of Foreign Affairs

Norway
Simen Ekblom (third and fourth session)
Cyber Policy Coordinator, Ministry of Foreign Affairs
Anniken Krutnes (first and second session)
Deputy Director-General, Department for Security Policy and the High North, Ministry of Foreign Affairs

Romania
Mihaela-Ionelia Popescu
Cyber policy coordinator, Ministry of Foreign Affairs

Russian Federation
Andrey Krutskikh
Special Representative of the President of the Russian Federation for International Cooperation in the Field of Information Security, Director, Department of International Information Security, Ministry of Foreign Affairs

Vladimir Shin (third and fourth session)
Deputy Director, Department of International Information Security, Ministry of Foreign Affairs

Singapore
David Koh
Chief Executive, Cyber Security Agency of Singapore and Commissioner of Cybersecurity

South Africa
Doc Mashabane
Director-General, Department of Justice and Constitutional Development

Moliehi Makumane (third session)
Special Advisor to South Africa's GGE representative

Switzerland
Nadine Olivieri Lozano
Ambassador, Head of International Security Division, Federal Department of Foreign Affairs

United Kingdom
Kathryn Jones
Head of International Cyber Governance, National Security Directorate, Foreign, Commonwealth and Development Office

Alexander Evans (first session)
Former Director Cyber, Foreign, Commonwealth and Development Office

United States
Michele Markoff
Acting Coordinator for Cyber Issues, United States Department of State

Uruguay
Noelia Martínez Franchi (third and fourth session)
Director of Multilateral Affairs, Ministry of Foreign Affairs
Alejandra Erramuspe (first and second session)
Senior Officer, Agency for e-Government and Information Society, Office of the President