Report of the Group of Governmental Experts  
On Developments in the Field of Information and Telecommunications  
In the Context of International Security

Introduction

1. Pursuant to General Assembly resolution 68/243 (2013) "Developments in the field of information and telecommunications in the context of international security", the Secretary-General, on the basis of equitable geographical distribution, established a group of governmental experts to continue to study, with a view to promoting common understandings, existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles for responsible behaviour of States and confidence-building measures, the issues of the use of information and communications technologies in conflicts and how international law applies to the use of information and communications technologies by States, as well as relevant international concepts aimed at strengthening the security of global information and telecommunications systems.

2. An open, secure, stable, accessible and peaceful ICT (Information and Communications Technology) environment is essential for all, and requires effective cooperation among States to reduce risks to international peace and security. The present report reflects the recommendations of the Group of Governmental Experts (GGE) and builds upon the work of previous GGEs.¹ The Group examined relevant international concepts and possible cooperative measures pertinent to its mandate. They reaffirmed that it is in the interest of all States to promote the use of ICTs for peaceful purposes and to prevent conflict arising from their use.

Existing and Emerging Threats

3. ICTs provide immense opportunities for social and economic development and continue to grow in importance for the international community. There are, however, disturbing trends in the global ICT environment, including a dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors. These trends create risks for all States, and the misuse of ICTs may harm international peace and security.

4. A number of States are developing ICT capabilities for military purposes. The use of ICTs in future conflicts between States is becoming more likely.

5. The most harmful attacks using ICTs include those targeted against a State’s critical infrastructure and associated information systems. The risk of harmful ICT attacks

¹ United Nations documents A/65/201 and A/68/98.
against critical infrastructure is both real and serious.

6. 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, which if left unaddressed may threaten international peace and security.

7. 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. States are rightfully concerned about the danger of destabilizing misperceptions, the potential for conflict, and the possibility of harm to their citizens, property and economy.

8. Different levels of capacity for ICT security among States can increase vulnerability in an interconnected world.

Norms, Rules, and Principles for the Responsible Behaviour of States

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 in order to increase stability and security in the global ICT environment.

10. Voluntary, non-binding norms of responsible State behaviour can reduce risks to international peace, security and stability. As such, norms do not seek to limit or prohibit action that is otherwise consistent with international law. Norms reflect the international community’s expectations, set standards for responsible State behaviour, and allow the international community to assess the activities and intentions of States. Norms can help to prevent conflict in the ICT environment and contribute to its peaceful use to enable the full realization of ICTs to increase global social and economic development.

11. Previous GGE reports 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 this Group was to continue to study, with a view towards promoting common understandings, norms of responsible State behaviour; determine where existing norms may be elaborated for application to the ICT environment; encourage greater acceptance of norms; and identify where additional norms that take into account the complexity and unique attributes of ICTs may need to be developed.
12. The Group noted the proposal of China, Kazakhstan, Kyrgyzstan, the Russian Federation, Tajikistan and Uzbekistan for an International Code of Conduct for Information Security, circulated by the Secretary-General as UN document A/69/723.

13. Taking into account existing and emerging threats, risks and vulnerabilities, and building upon the assessments and recommendations contained in the July 2010 and June 2013 GGE Reports, the Group offers the following recommendations for States’ consideration for voluntary, non-binding norms, rules, or principles for the responsible behaviour of States aimed at promoting an open, secure, stable, accessible and peaceful ICT environment:

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;

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;

c. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs;

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;

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

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;

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;

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;

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;

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;

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.

14. The Group observed that, while such measures may be essential in promoting an open, secure, stable, accessible and peaceful ICT environment, their implementation may not immediately be possible, particularly for developing countries, until they acquire adequate capacity.

15. Given the unique attributes of ICTs, additional norms could be developed over time.

Confidence-Building Measures

16. Confidence-Building Measures (CBMs) 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 UN 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 CBMs:
a. Identification of appropriate points of contact at the policy and technical levels to address serious ICT incidents and the creation of a directory of such contacts;

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

c. Encouraging, on a voluntary basis, transparency at the bilateral, sub-regional, 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; CBMs developed in regional and multilateral forums; and national organizations, strategies, policies and programmes relevant to ICT security;

d. The voluntary provision by States of their national views of categories of infrastructure 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, sub-regional, regional, and multilateral consultations on the protection of ICT-enabled critical infrastructures;
   iii. The development on a bilateral, sub-regional, regional and multilateral basis of technical, legal, and diplomatic mechanisms to address ICT-related requests;
   iv. Adoption of voluntary national arrangements to classify ICT incidents in terms of the scale and seriousness of the incident, for the purpose of facilitating the exchange of information on incidents.

17. States should consider additional confidence-building measures that would strengthen cooperation at a bilateral, sub-regional, regional and multilateral basis. These could include voluntary agreement by States to:
a. Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents, and develop additional technical, legal, and diplomatic mechanisms to address ICT infrastructure-related requests, including consideration of exchanges of personnel in areas such as incident response and law enforcement, as appropriate, and encouraging exchanges between research and academic institutions;

b. Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;

c. States are encouraged to establish a national Computer Emergency Response Teams (CERT), Computer Security Incident Response Team (CSIRT) or to 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 national CERTs, CSIRTs, and other authorized bodies;

d. Expand and support practices in CERT and CSIRT cooperation as appropriate, such as information exchange about vulnerabilities, attack patterns, and best practices for mitigating attacks, including coordinating responses, organizing exercises, supporting the handling of ICT-related incidents, and enhancing regional and sector-based cooperation;

e. Cooperate, in a manner consistent with domestic and international law, with requests from other States in investigating ICT-related crime or use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory.

18 The Group reiterates that, given the pace of ICT development and the scope of the threat, there is a need to enhance common understandings and intensify cooperation. In this regard, the Group recommends regular institutional dialogue with broad participation under the auspices of the United Nations, as well as regular dialogue through bilateral, regional and multilateral forums, and other international organizations.

**International Cooperation and Assistance in ICT Security and Capacity-Building**

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 a State’s citizens and critical infrastructure vulnerable, or make a State 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. Assistance to build capacity in ICT security is also essential for international security, by improving States’ capacity for cooperation and
collective action. The Group agreed that capacity-building measures should seek to promote the use of ICTs for peaceful purposes.

20. The Group endorsed the 2010 and 2013 reports’ recommendations on capacity building. The 2010 Report recommended that States identify measures to support capacity-building in less developed countries. The 2013 GGE 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 current 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 they face and effective responses to them.

21. Continuing the work begun through previous United Nations resolutions and reports, including General Assembly resolution 64/211 "Creation of a global culture of cybersecurity and taking stock of national efforts to protect critical information infrastructures", States should consider the following voluntary measures to provide technical and other assistance to build capacity in securing ICTs in countries requiring and requesting assistance:

a. Assist in strengthening cooperative mechanisms with national CERTs and other authorized bodies;

b. Provide assistance and training to developing countries to improve security in the use of ICTs, including critical infrastructure, and exchange legal and administrative best practices;

c. Assist in providing access to technologies deemed essential for ICT security;

d. Create procedures for mutual assistance in responding to incidents and addressing short-term problems in securing networks, including procedures for expedited assistance;

e. Facilitate cross-border cooperation to address critical infrastructure vulnerabilities that transcend national borders;

f. Develop strategies for sustainability in ICT security capacity-building efforts;

g. Prioritize ICT security awareness and capacity building in national plans and budgets and assign it appropriate weight in development and assistance planning. This could include ICT security awareness programmes designed to educate and inform
institutions and individual citizens. Such programmes could be carried out in conjunction with efforts by international organizations, including by the United Nations and its agencies, the private sector, academia and civil society organizations;

h. Encourage further work in capacity building, such as on forensics or on cooperative measures to address the criminal or terrorist use of ICTs.

22. The development of regional approaches to capacity-building would be beneficial as they could take into account specific cultural, geographic, political, economic, or social aspects, and allow a tailored approach.

23. In the interest of ICT security capacity building, States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations. Such initiatives would help improve the environment for effective mutual assistance between States in their response to ICT incidents and could be further developed by competent international organizations, including the United Nations and its agencies, the private sector, academia and civil society organizations.

How International Law Applies to the Use of ICTs

24. The 2013 GGE Report on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98) 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, this Group considered how international law applies to the use of ICTs by States.

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

26. In considering the application of international law to State use of ICTs, the Group identified as of central importance States’ commitments to the following principles of the UN Charter and other international law: sovereign equality; the settlement of international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered; refraining in their international relations from the threat or use of force against the territorial integrity or political independence of any State, or in any other manner inconsistent with the purposes of the United Nations; respect for human rights and fundamental freedoms; and non-intervention in the internal affairs of other States.
27. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities and to their jurisdiction over ICT infrastructure within their territory.

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

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

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

c. Underscoring the international community’s aspirations to the peaceful use of ICTs for the common good of mankind, and recalling that the Charter of the United Nations applies in its entirety, the Group noted the inherent right of states to take measures consistent with international law and as recognized in the UN Charter. The Group recognized the need for further study on this matter;

d. The Group notes the established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction;

e. States must not use proxies to commit internationally wrongful acts using ICTs, and should seek to ensure that their territory is not used by non-State actors to commit such acts;

f. States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from a State’s territory or from its ICT infrastructure may be insufficient in itself to attribute the activity to that State. The Group noted that the accusations of organizing and implementing wrongful acts brought against States should be substantiated.

29. The Group noted that common understandings on how international law applies to State use of ICTs are important for promoting an open, secure, stable, accessible and peaceful ICT environment.
Conclusions and Recommendations for Future Work

30. There has been significant progress in recognizing the risks to international peace and security from the malicious use of ICTs. Recognizing that ICTs can be a driving force in accelerating progress towards development, and consistent with the need to preserve global connectivity and the free and secure flow of information, the Group considered it useful to identify possible measures for future work which include, but are not limited to, the following:

   a. Further development by States collectively and individually of concepts for international peace and security in the use of ICTs at the legal, technical and policy levels; and

   b. Increased cooperation at regional and multilateral levels to foster common understandings on the potential risks to international peace and the security posed by the malicious use of ICTs, and on the security of ICT-enabled critical infrastructure.

31. While States have a primary responsibility for maintaining a secure and peaceful ICT environment, effective international cooperation would benefit from identifying mechanisms for the participation, as appropriate, of the private sector, academia and civil society organizations.

32. Areas where further research and study could be useful include, inter alia, concepts relevant to State use of ICTs. UNIDIR, as a UN research institute serving all Member States, is one such entity that could be requested to undertake relevant studies, as could other relevant think tanks and research organizations.

33. The United Nations should play a leading role in promoting dialogue on the security of ICTs in their use by States, and developing common understandings on the application of international law and norms, rules and principles for responsible State behaviour. Further work could consider initiatives for international dialogue and exchange on ICT security issues. These efforts should not duplicate ongoing work by other international organizations and forums addressing issues such as criminal and terrorist use of ICTs, human rights, and internet governance.

34. The Group noted the importance for the UN General Assembly to consider the convening of a new Group of Governmental Experts on Developments in the Field of Information and Telecommunications in 2016 to continue to study with a view to promote common understandings on existing and potential threats in the sphere of information security, and possible cooperative measures to address them, as well as how international law applies
to the use of ICTs by States, including norms, rules, and principles of responsible behaviour of States, confidence-building measures, and capacity building.

35. The Group acknowledges the valuable efforts in ICT security made by international organizations and regional groups. Work among States on security in the use of ICTs should take these efforts into account, and Member States should, when appropriate, encourage the establishment of new bilateral, regional, and multilateral platforms for dialogue, consultation, and capacity-building.

36. The Group recommends that Member States give active consideration to the recommendations contained in this Report on how to help build an open, secure, stable, accessible and peaceful ICT environment, and assess how they might be taken up for further development and implementation.