Cumulative Recommendations in the UN GGE Reports (2010-2015)[1]

	2010[2]	2013[3]	2015[4]
Goal	To study both threats in the sphere of information security and relevant international concepts and to suggest possible cooperative measures that could strengthen the security of global information and communication systems.	To offer recommendations to promote peace and stability in State use of ICTs.	To consider the application of international law to the State use of ICTs. 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.
Threats, risks and vulnerabilities	Motives for disruption emanate from: a. Demonstrating technical prowess; b. Theft of money or information; c. Extension of State conflict Sources of threats: a. Non-state actors (criminals, terrorists) b. States Objectives: ICT can be used to damage information resources and infrastructures Dual-use of ICTs and growing sophistication Examples of threats: 1. Terrorist use of ICTs (communication, collecting information, recruitment, organisation, promoting their ideas and actions, soliciting funding) 2. ICTs as instruments of warfare and intelligence, also for political purposes 3. Attribution issues	ICTs as dual-use technologies that can be used for legitimate (1) and malicious (2) purposes. The combination of a. Global connectivity b. Vulnerable technologies c. Anonymity, facilitates the use of ICTs for disruptive activities. Threats have grown more acute and incidents more damaging. Sources of threats: a. Non-state actors b. States Threats: 1. Use of proxies 2. Development and the spread of sophisticated malicious tools and techniques 3. Attribution problems persists, malicious use of ICTs can be easily concealed, allowing for increasingly	Sources of threats: a. Non-state actors b. States Misuse of ICTs may harm international peace and security. Threats: 1. Developing ICT capabilities for military purposes. Use of ICTs in future conflicts. 2. Attacks against a State's critical infrastructure and associated information systems 3. Use of ICTs for terrorist purposes (beyond recruitment, financing, training, incitement) and for terrorist attacks against ICTs or ICT-dependent infrastructure 4. Attribution problem 5. Destabilising misperceptions, the potential for conflict and the possibility of harm to citizens, property or economy. 6. Diversity of malicious non-state actors (criminal groups and terrorists) 7. The speed at which malicious ICT actions can occur

[1] This table is courtesy of Liisi Adamson (l.adamson@fgga.leidenuniv.nl) / Cyber Policy Institute (CPI, www.cpi.ee). When text is blue this is to indicate that the wording is not a reiteration of statements from previous reports, but added in the respective year of each report.
[2] 2010 07 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/65/201)
[3] 2013 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/68/98*)
[4] 2015 09 UN Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (A/70/174)

	2010[2]	2013[3]	2015[4]
	4. Use of proxies 5. Protection of critical infrastructures 6. ICT supply chain security 7. ICT capacity and security differences among States	sophisticated exploits. Mistaken attribution is a risk. 4. Terrorist use of ICTs (communication, collecting information, recruitment, organisation, planning and coordinating attacks, promoting their ideas and actions, soliciting funding) 5. Supply chain security and embedded harmful hidden functions 6. Protection of critical infrastructures and industrial control systems 7. ICT security capacity differences among different States	8. ICT security capacity differences among different States.
Norms, rules and principles of responsible State behaviour (voluntary, non-binding)	–	GGE noted the International Code of Conduct proposed by SCO. Intensified cooperation against criminal or terrorist use of ICTs was called for. States should harmonise legal approaches and strengthen practical collaboration between law enforcement and prosecutorial agencies. GGE called for encouraging the private sector and civil society to play a role to improve security of and in the use of ICTs, including supply chain security.	Voluntary, non-binding norms of responsible State behaviour: 1. Can reduce risks to international peace and security 2. Do not seek to limit or prohibit action that is otherwise consistent with international law 3. Reflect international community's expectations 4. Set standards for responsible State behaviour 5. Allow international community to assess the activities and intentions of States 6. Can help to prevent conflict in the ICT environment and contribute to its peaceful use. GGE noted the International Code of Conduct proposed by SCO.
			Proposed 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. 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

2010[2]	2013[3]	2015[4]
		b. In case of ICT incidents, States should consider all relevant information, including the larger context of the event, challenges of attribution 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. e. State should 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. Protecting of critical infrastructure from ICT threats, taking into account UNGA Resolution 58/199 (2003) 'Creation of a global culture of cybersecurity and the protection of critical information infrastructure' 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. Ensuring the integrity of the supply chain. States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions j. Encourage responsible reporting of ICT vulnerabilities and sharing associated information k. States should not conduct or knowingly support activity to harm the information systems of another State's authorized

	2010[2]	2013[3]	2015[4]
			emergency response teams (CERT). A State should not use authorized emergency response teams to engage in malicious international activity. 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.
International Law Applicable to the use of ICTs	–	International law and the UN Charter applies and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment. State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities. States have jurisdiction over ICT infrastructure within their territory. Addressing the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments. States must meet their international obligations arising from internationally wrongful acts attributable to them. States must not use proxies to commit internationally wrongful acts and should seek to ensure that their territories are not used by non-state actors for unlawful use of ICTs.	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. GGE proposed non-exhaustive list of principles of international law that apply to the use of ICTs by States: a. States have jurisdiction overt 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. States have the inherent right to take measures consistent with international law and as recognised in the UN Charter. d. Established international legal principles, including, where applicable, the principles of humanity, necessity, proportionality and distinction, apply. 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

	2010[2]	2013[3]	2015[4]
			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.
Confidence-building measures	–	Voluntary confidence-building measures (CBM) can promote trust and assurance among States and help reduce the risk of conflict by increasing predictability and reducing misperception. CBM-s help increase: a. Transparency b. Predictability c. Cooperation Proposed CBMs: (a) Voluntary exchange of views and information (national strategies and policies, best practices, decision-making process, relevant national organisations and measures to improve international cooperation (b) Creation of consultative frameworks for confidence-building (workshops, seminars, exercises) (c) Enhanced sharing of information on ICT security incidents. Exchanging information on national points of contact (d) Exchanges of information and communications between national CERTs (e) Increased cooperation to address incidents that could affect ICT or critical infrastructure that rely upon ICT-enabled industrial control systems (including guidelines and best practices against disruptions perpetrated by non-state actors)	CBMs strengthen international peace and security and can increase interstate cooperation, transparency, predictability and stability. Proposed voluntary CBMs: a. Identification of appropriate points of contact at policy and technical levels b. Development and support for mechanisms and processes for consultations to enhance interstate confidence-building and to reduce the risk of misperception, escalation, and conflict that may stem from ICT incidents c. Encouraging transparency via 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. Voluntary provision of States' 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 (e.g. a repository of national laws and policies; development of mechanisms and processes for consultations on the protection of ICT-enabled critical

	2010[2]	2013[3]	2015[4]
		(f) Enhanced mechanisms for law enforcement cooperation States should promote complementarity of measures and facilitate the dissemination of best practices. There's a need to enhance common understandings and intensify practical cooperation.	infrastructures; development of mechanisms to address ICT related requests; adoption of voluntary national system to classify ICT incidents in terms of their scale and seriousness for the purpose of facilitating the exchange of information on incidents) Additional voluntary CBMs 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 and 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. Encouraging the establishment of computer emergency response teams d. Expand and support practices between computer emergency response teams e. Cooperate 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
Cooperative measures	Risks require concerted responses in order to: a. Combat the criminal misuse of information technology; b. Create a global culture of CS; c. Promote other essential measures that can reduce risk. International efforts to combat the threat of cybercrime have been conducted. Importance of minimising the misperception resulting from a lack of	Need for cooperative action to promote a peaceful, secure, open and cooperative ICT environment. Cooperative measures should be considered, which could enhance international peace, stability and security (including the common understandings on the application of relevant international law and derived norms, rules, and principles of responsible State behaviour). States must lead in addressing the challenges, but effective cooperation	Effective international cooperation would benefit from private sector, academia and civil society organisation's participation. The UN should play a leading role in promoting the dialogue.

	2010[2]	2013[3]	2015[4]
	shared understanding regarding international norms pertaining to State use of ICTs. Calls for elaboration of measures designed to enhance cooperation where possible. E.g.: 1. Sharing best practices 2. Managing incidents 3. Building confidence 4. Reducing risk 5. Enhancing transparency and stability Collective action needed to address the threats. Collaboration among and between the States, the private sector and civil society is held important.	would benefit from the appropriate participation of the private sector and civil society. The UN should play a leading role in promoting the dialogue. Efforts made by international organisation and regional entities must be taken into account (wider than just cybercrime as was stated in GGE 2010 report).	
Capacity building	Capacity building needed to bridge the current divide in ICT security and appropriate assistance where needed. States need to identify measures to support capacity-building in less developed countries.	Some States may require assistance to: 1. Improve security of critical ICT infrastructure 2. Develop technical skill and appropriate legislation 3. Strategies and regulatory frameworks to fulfil their responsibilities 4. Bridge the divide in the security of ICTs and their use Assistance means technical and other assistance. Measures to be considered: (a) Supporting international capacity-building efforts to secure ICT use and ICT infrastructures; to strengthen national legal frameworks, law enforcement capabilities and strategies; to combat the use of ICTs for criminal and terrorist purposes; to assist in the identification and dissemination of best practices. (b) Creating and strengthening incident response capabilities (CERTs) (c) Supporting the development and use of e-learning, training and	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 and effective responses to them. Measures to be considered: 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;

	2010[2]	2013[3]	2015[4]
		awareness-raising to help overcome the digital divide (d) Increasing cooperation and transfer of knowledge and technology for managing ICT security incidents (e) Further analysis and study by research institutes and universities	g. Prioritise 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 organisations, including by the UN 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. Development of regional approaches would be beneficial to capacity-building. States may consider forming bilateral and multilateral cooperation initiatives that would build on established partnership relations.
Recommendations	(i) Further dialogue among States to discuss norms pertaining to State use of ICTs, to reduce collective risk and protect critical national and international infrastructure; (ii) Confidence-building, stability and risk reduction measures to address the implications of State use of ICTs, including exchanges of national views on the use of ICTs in conflict; (iii) Information exchanges on national legislation and national information and communications technologies security strategies and technologies, policies and best practices; (iv) Identification of measures to support capacity-building in less developed countries; (v) Finding possibilities to elaborate common terms and definitions relevant to General Assembly resolution 64/25.		Recommendations for future work: 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. 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.