ICT for peace foundation

International Cyber Norms Roadmap

	OSCE[i]	GGE/*OEWG*[ii]	2016/2017 GGE Chairman's Impressions	Paris Call[iii]	The Kaljurand Commission[iv]
Upholding and developing the rule of law	Have in place modern and effective national legislation to facilitate exchange and cooperation #6	Establish/provide 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 (2015, ¶16 d i)		Promote the widespread acceptance and implementation of international norms of responsible behavior as well as confidence-building measures in cyberspace.	
		States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs (2015, ¶13 c)	An official notification from one State to another State should be regarded as providing the notified State with actual knowledge of the alleged activity. The notified State should acknowledge receipt of the request via the relevant national point of contact. When becoming aware of malicious ICT activities within or transiting through ICT systems located on their territory and that are likely to affect another State adversely, States should, in accordance with international and domestic law and within their capacity, take all reasonable steps, within their territory, to cause these activities to cease. A State that becomes aware of harmful ICT activities emanating from its territory but lacks the capacity to respond may choose to seek assistance from other States, including through standard assistance request templates. If the State knows the malicious ICT activity is transiting through its territory and is able to identify the State from which it is originating, it may choose to notify that State instead of, or in addition to, seeking assistance from other States. It is understood that notifying a State does not imply responsibility of the notified State for the incident.		
		States should respect resolutions on the promotion,	Experts underscored that States should recognize that personal data held on,		

		protection and enjoyment of human rights on the Internet (2015, ¶13 e)	transmitted through or processed by ICTs can have a profound impact on life and security. States should take appropriate steps to protect personal data, including its confidentiality, integrity, accessibility and authenticity, while respecting relevant international, legal human rights instruments.		
		States must meet their international obligations regarding internationally wrongful acts attributable to them under international law. However, the indication that an ICT activity was launched or otherwise originates from the territory or objects of the ICT infrastructure of a State may be insufficient in itself to attribute the activity to that State. Accusations of organizing and implementing wrongful acts brought against States should be substantiated (OEWG, 1.2)			
Cooperation and assistance		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 (2015, ¶13 a)	Managing and mitigating ICT-related incidents in an effective and timely manner requires cooperation among States and between States and other stakeholders, as well as the measures that enable it.	Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm.	
		States should consider how to best cooperate to exchange information, assist each other, prosecute terrorist and criminal use of ICTs and implement other cooperative measures to address such threats (2015, ¶13 d)	To support implementation of this norm, experts proposed that States support the work of the UN Commission on Crime Prevention and Criminal Justice and its on-going efforts to study, in a comprehensive manner, the problem of cybercrime.		
		States should intensify cooperation against criminal			

	and terrorist use of ICTs, harmonize legal approaches and strengthen practical collaboration between law enforcement and prosecutorial agencies (2013, ¶22)			
	Cooperate, in a manner consistent with national and international law, with requests from other States in investigating ICT-related crime or the use of ICTs for terrorist purposes or to mitigate malicious ICT activity emanating from their territory (2015, ¶17 e)			
	Enhanced mechanisms for law enforcement cooperation to reduce incidents that could otherwise be misinterpreted as hostile State actions (2013, ¶26 f)			
Facilitate cooperation between authorized authorities responsible for securing critical infrastructures #15	Increased cooperation to address incidents that could affect ICT or CI that rely on ICT-enabled industrial control systems, including guidelines and best practices among States against disruptions perpetrated by non-State actors (2013, ¶26 e)			
	States should respond to appropriate requests for assistance by another State whose CI is subject to malicious ICT acts (2015, ¶13 h)	Experts discussed that a State receiving an appropriate request for assistance following an ICT incident should: • acknowledge receipt of the request via the relevant national point of contact; • determine, in a timely fashion, whether it has the capacity and resources to provide the assistance requested and respond; • in its initial response, indicate the nature, scope and terms of the assistance that might be provided, including a timeframe for its delivery; and		

			• in the event that assistance is agreed upon, promptly provide the arranged assistance.		
		Establish focal points and cooperation for the provision of assistance in investigations (2015, ¶17 b)			
Exchange of views and information	National views of national and international threats #1	Voluntary sharing of national views and information on various aspects of national and transnational threats to and in the use of ICTs (2015, ¶16 c)			
	Information in relation with security of and in the use of ICTs #2	Voluntary sharing of national views and information on vulnerabilities and identified harmful functions in ICT products (2015, ¶16 c)	Publicly communicate elements of approaches to the use of ICT capabilities.		
	Measures that States have taken to ensure an open, interoperable, secure, and reliable Internet #4	Prevent practices that are acknowledged to be harmful or that may pose threats to international peace and security (2015, ¶13 a)	Experts suggested that States consider sharing information on best practices for protecting critical infrastructures, including on: baseline security requirements; Incident notification procedures; Incident handling tools and methodologies; Emergency resilience; and lessons learned from previous incidents.		
	Effective responses to threats to and in the use of ICTs #5	Establish focal points and cooperation for the exchange of information on malicious ICT use (2015, ¶17 b)			
	Best practices, awareness-raising, information on capacity-building #5	Voluntary sharing of national views and information on best practices for ICT security (2015, ¶16 c)	Experts felt States should be encouraged to raise awareness among senior decision makers across all branches of government as well as diplomatic personnel on the recommendations of the GGEs and the importance of CBMs to the maintenance of international peace and security. Results could be achieved by involving a wide variety of national representatives in activities that enhance practical understanding of the issues.		
	Information on national organization; strategies; policies and programmes – including on cooperation between the public and the private sector #7	Voluntary sharing of national views and information on national organizations, strategies, policies and programmes relevant to ICT security (2015, ¶16 c) (2013, ¶26 a)	Use existing mechanisms, including the UN Secretary-General's annual report on developments in the field of ICTs in the context of international security, other opportunities as well as relevant international and regional organizations and fora to report on national implementation of CBMs and to exchange information and experiences.		

	Provide a list of national terminology: terms and definitions or explanations #9				
	Exchanges in different formats: workshops, seminars, roundtables at regional and sub-regional level, to investigate further areas for cooperation #12	The creation of bilateral, regional and multilateral consultative frameworks for confidence-building, which could entail workshops, seminars and exercises to refine national deliberations on how to prevent disruptive incidents arising from State use of ICTs and how these incidents might develop and be managed (2013, ¶26 b)			
		Enhanced sharing of information on ICT security incidents, involving the more effective use of existing channels or the development of new channels and mechanisms to receive, collect, analyze and share information related to ICT incidents, for timely response, recovery and mitigation actions (2013, ¶26 c)	In order to facilitate notification and exchanges of information on incidents, and to support implementation of measures relating to the classification of ICT incidents, develop voluntary arrangements, such as standard incident severity schemas; encourage sharing of and participation in activities, including exercises relating to these and other voluntary incident classification arrangements, through appropriate international, regional, sub-regional and bilateral fora.		
	Consultations to reduce the risks of misperception, and possible emergence of pol-mil tension or conflict #3	The development of and support for mechanisms and processes for bilateral, regional, sub-regional and multilateral consultations to enhance inter-State confidence-building and reduce the risk of misperception, escalation and conflict that may stem from ICT incidents (2015, ¶16 b)			
Critical infrastructure	To protect critical national and international ICT infrastructures, including their integrity #3	A State should not conduct or knowingly support ICT activity contrary to its obligations under international law that intentionally damages CI or otherwise impairs the use and	There were recommendations that States consider the potentially harmful effects of their ICT activities on the general functionality of global ICT systems and the essential services that rely on them.	Prevent and recover from malicious cyber activities that threaten or cause significant, indiscriminate or systemic harm to individuals and critical infrastructure.	

		operations of CI to provide services to the public (13 f)			
		Voluntary provision of national views of categories of infrastructure that they consider critical and national efforts to protect them, including information on national-level laws and policies for the protection of data and ICT-enabled infrastructure (2015, ¶16 d)			
		States should seek to facilitate cross-border cooperation to address CI vulnerabilities that transcend national borders (2015, ¶16 d)			
		States should take appropriate measures to protect their CI from ICT threats (2015, ¶13 g)[1]	Experts also suggested that States should participate in voluntary risk assessment and business continuity (resilience, recovery and contingency) planning initiatives involving other stakeholders and aimed at enhancing the security and resilience of national and cross-border critical infrastructure against existing and emerging threats.		
		The development of technical, legal and diplomatic mechanisms to address ICT-related requests (2015, ¶16 d iii)			
		The adoption of 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 about incidents (2015, ¶16 d iv)			
		Consider categorizing CERT as critical infrastructure (2015, ¶17 c)			
Incident prevention and handling	Measures to ensure rapid communication at policy levels of authority, to permit concerns to be	In case of ICT incidents, States should consider all relevant information, including the larger context of the event the	States should give consideration to establishing the national structures, policies, processes and coordination mechanisms necessary to facilitate careful		

[1] UNGA resolutions

	raised at the national security level #8	challenges of attribution in the ICT environment and the nature and extent of the consequences (2015, ¶13b)	consideration of serious ICT incidents and to determine appropriate responses. Once those structures and processes are in place, States should develop JCT incident assessment or severity templates to evaluate and assess ICT incidents. Wherever possible, the templates should be in line with existing practices and avoid duplication.		
		Strengthen cooperative mechanisms between relevant agencies to address ICT security incidents (2015, ¶17 a)			
	Nominating contact points to facilitate communications and dialogue #8	States should respond to appropriate requests to mitigate malicious ICT activity aimed at the CI of another State emanating from their territory, taking into account due regard for sovereignty (2015, ¶13 h)	Given the varied and distributed nature of critical infrastructure ownership, experts felt that States should promote, in consultation with the relevant stakeholders, minimum standards for the security of critical infrastructures and promote cooperation with the private sector, academia and the technical community in critical infrastructure protection efforts.		
		The development or mechanisms and processes for consultations on the protection of ICT-enabled CI (2015, ¶16 d ii)			
Computer Emergency Response		Establish a national computer emergency response team and/or cybersecurity incident response team or officially designate an organization to fulfil this role (2015, ¶17 c)			
		Identify appropriate points of contact at the policy and technical levels to address serious ICT incidents (2015, ¶16 a)	Implement the measure relating to the identification of appropriate points of contact (2015 GGE report ¶16(a)) at both the policy and technical levels to address serious ICT incidents and create a directory of such contacts that can be shared bilaterally, regionally or at the global level. Systematize and exercise the use of such points of contact at both the policy and technical levels, and develop guidance on the expected roles and responsibilities of points of contact.		

		States should consider exchanging information on national points of contact, in order to expand and improve existing channels of communication for crisis management, and supporting the development of early warning mechanisms (2013, ¶26 c)			
	Provide and update contact data of national structures that manage ICT-related incidents and coordinate responses #8	Expand and support practices in computer emergency response team and cybersecurity incident response team cooperation, 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 (2015, ¶17 d)			
		States should not conduct or knowingly support activity to harm the information systems of authorized emergency response teams of another State. A State should not use authorized emergency response teams to engage in malicious international activity (2015, ¶13 k)			
		Exchanges of information and communication between national CERTs bilaterally, within CERT communities, and other forums, to support dialogue at political and policy levels (2013, ¶26 d)			
Integrity of the supply chain		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 (2015, ¶13 i)	Take steps, including through existing fora, to prevent the proliferation of malicious ICT tools and techniques. In doing so, States should encourage the legitimate activities of research communities, academia, industry, law enforcement, CERTs/ CSIRRTs and other ICT protection agencies	Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain.	State and non-state actors should not tamper with products and services in development and production, nor allow them to be tampered with, if doing so may substantially impair the stability of cyberspace.

			in ensuring the security of their ICT systems. Take steps to prevent non-State actors, including the private sector, from conducting malicious ICT activities for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory. Take steps to prevent non-state actors, including the private sector, from using harmful hidden functions for their own purposes or those of other non-State actors to the detriment of third parties including those located on another State's territory.		
		States should seek to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions (2015, ¶13 i 2)	Identify trust-building measures that can help allay concerns about harmful hidden functions in ICT products, encouraging the private sector and civil society to play an appropriate role to this end.		
Reporting of vulnerabilities	Responsible reporting of vulnerabilities affecting the security of and in the use of ICTs and sharing available measures, also with ICT business and industry #16	States should encourage responsible reporting of ICT vulnerabilities (2015, ¶13 j)	• Establish national structures that enable a responsible reporting and handling of ICT vulnerabilities; • Establish appropriate coordination mechanisms amongst public and private sector entities; • Engage in targeted capacity-building to support effective and responsible sharing of ICT vulnerabilities.		States should create procedurally transparent frameworks to assess whether and when to disclose not publicly known vulnerabilities or flaws they are aware of in information systems and technologies. The default presumption should be in favor of disclosure.
		States should share information about available remedies to vulnerabilities to limit and possibly eliminate potential threats to ICTs and ICT-dependent infrastructure (2015, ¶13 j 2)	In addition, and to avoid misunderstandings or misinterpretations, including those stemming from non-disclosure of information about potentially harmful ICT vulnerabilities, experts encouraged States to share, to the widest possible extent, technical information on serious JCT incidents. This information could include, inter alia, the indicators of attribution and compromise, the malware and method used and associated remedies. Experts felt that States should ensure that such information is handled responsibly and in coordination with other stakeholders, as appropriate.		Developers and producers of products and services on which the stability of cyberspace depends should prioritize security and stability, take reasonable steps to ensure that their products or services are free from significant vulnerabilities, take measures to timely mitigate vulnerabilities that are later discovered and to be transparent about their process. All actors have a duty to share information on

					vulnerabilities in order to help prevent or mitigate malicious cyber activity.
Role of the private sector, civil society and academia	Promote PPPs #14	States should encourage the private sector and civil society to play and appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services (24)	Encourage research on ICTs in the context of international peace and security, including on methodologies to enhance the technical attribution of ICT incidents.		
		State should consider how to best cooperate in implementing the above norms and principles, including the role that may be played by the private sector and civil society organizations (25)	Support policy-relevant and technical research on emerging JCT-related risks and threats.		
		States should encourage the private sector and civil society to play an appropriate role to improve security of and in the use of ICTs, including supply chain security for ICT products and services. States should cooperate with the private sector and the organizations of civil society in the sphere of implementation of rules of responsible behaviour in information space with regard to their potential role (OEWG, 1.13)			
Other				Prevent activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet.	Without prejudice to their rights and obligations, state and non-state actors should not conduct or knowingly allow activity that intentionally and substantially damages the general availability or integrity of the public core of the Internet, and therefore the stability of cyberspace.
				Strengthen our capacity to prevent malign interference by foreign actors aimed at undermining electoral processes	State and non-state actors should not pursue, support or allow cyber operations intended to disrupt the technical infrastructure

				through malicious cyber activities.	essential to elections, referenda or plebiscites.
				Prevent ICT-enabled theft of intellectual property, including trade secrets or other confidential business information, with the intent of providing competitive advantages to companies or commercial sector.	State and non-state actors should not commandeer others' ICT resources for use as botnets or for similar purposes.
				Support efforts to strengthen an advanced cyber hygiene for all Actors.	States should enact appropriate measures, including laws and regulations, to ensure basic cyber hygiene.
				Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.	
					Non-state actors should not engage in offensive cyber operations and state actors should prevent and respond to such activities if they occur.

[i] Decision No. 1202 OSCE Confidence-Building Measures to Reduce the Risks of Conflict Stemming from the Use of Information and Communication Technologies, PC.DEC/1202, 10 March 2016.
[ii] Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 24 June 2013, UN A/68/98), paras 22, 24, 25 and 26); Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security, 22 July 2015, UN A/70/174), paras 13, 16 and 17.
[iii] Paris Call for Trust and Security in Cyberspace, https://www.diplomatie.gouv.fr/IMG/pdf/paris_call_text_-_en_cle06f918.pdf
[iv] https://cyberstability.org