Endorsing the New Rules

Sherif Hashem, George Mason University, USA

Maarten Van Horenbeeck, Zendesk, USA

Cyber Norms

Normative processes

- Different groups organize normative processes, but the **Gold** standard is the **UN Group of Governmental Experts** .

- The **Open Ended Working Group** has been renewed up to 2025 to further support the implementation of UNGGE norms.


UNITED NATIONS
NATIONS UNIES

UN GGEs/UN OEWG: Past, Present, Future

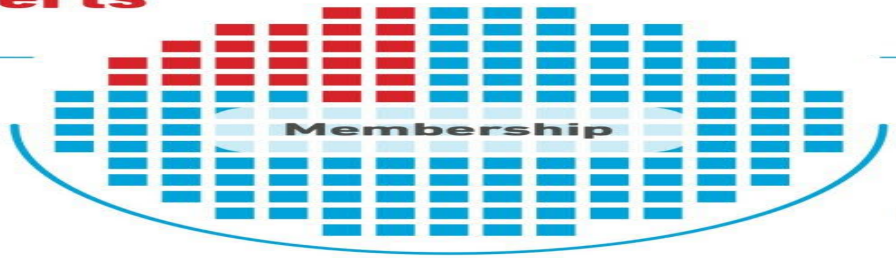
- In 2004, the UN General Assembly established the Group of Governmental Experts (GGE) to examine the impact of developments in ICT on national security and military affairs. **Six GGEs** have been convened – in 2004/2005, 2009/2010, 2012/2013, 2014/2015, 2016/2017, and 2019/2021. In addition, the UN General Assembly has also established the Open-Ended Working Group (OEWG) for 2019/2021 and 2021/2025.
- UN GGE and UN OEWG fall under the **UN First Committee** which deals with disarmament, global challenges and threats to peace that affect the international community and seeks out solutions to the challenges in the international security regime.

Comparative Survey

of the two UN-based processes on responsible behaviour in cyberspace

UN Group of Governmental Experts (2019–2021)

25 selected Member States



UN Open-Ended Working Group (2019–2021)

All interested UN Member States

Chair

Chair

Consultations

6 with Regional Organisations (AU, EU, OAS, OSCE, ARF, ASEAN Regional Forum), 2 with all Member States

Intersessional meetings with interested stakeholders (business, NGOs, and academia)

To address

- Norms, rules, and principles
- Confidence-building measures (CBMs) and capacity building
- How international law applies to cyberspace

UNGA A/RES/73/266

- (Further develop or change) Norms, rules and principles listed in A/RES/73/27 (par. 1)
- Confidence building measures (CBMs) and capacity building
- How international law applies to cyberspace
- Existing and potential threats
- Establishing regular institutional open-ended dialogue within the UN
- Relevant international concepts for securing global IT systems

UNGA A/RES/73/27

Reporting to

76th GA Session (2021), incl. annex with national contributions on how international law applies to cyberspace

76th GA Session (2021), on a consensus basis

Timeline

2019

- **3–4 June 2019:** Organisational meeting
- **9–13 September 2019:** 1st session
- **17–30 September 2019:** 74th GA
- **2–4 December 2019:** Multistakeholder informal consultation
- **5–6 December 2019:** Informal consultation for non-members
- **9–13 December 2019:** 1st session

2020

- **10–14 February 2020:** 2nd session
- **24–28 February 2020:** 2nd session
- **15–19 June 2020:** Informal virtual meetings
- **29 Sep–1 Oct 2020:** Informal virtual meetings
- **17–19 November 2020:** Informal virtual meetings
- **1–3 December 2020:** Informal virtual meetings
- **14–18 December 2020:** 3rd session

2021

- **January 2021:** Preparation of the Zero Draft
- **8–12 March 2021:** 3rd final session (A/75/816)
- **20–21 May 2021:** Informal consultations
- **24–29 May 2021:** 4th final session (A/76/135)

Geneva Internet Platform DigitalWatch

dig.watch/ungge

● UN GGE ● UN OEWG

Norms and Principles for Responsible State Behavior (UN GGE'15)

1. States should cooperate in developing and applying measures to increase stability and security in the use of Information and Communication Technologies (ICTs) and to prevent ICT practices that are acknowledged to be harmful or that may pose threats to international peace and security.
2. 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.
3. States should not knowingly allow their territory to be used for internationally wrongful acts using ICTs. 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.
4. 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.
5. States, in ensuring the secure use of ICTs, should respect the right to privacy in the digital age, to guarantee full respect for human rights, including the right to freedom of expression.

Norms and Principles for Responsible State Behavior (UN GGE'15)

6. 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.

7. States should take appropriate measures to protect their critical infrastructure from ICT threats, taking into account General Assembly Resolution 58/199 of 23 December 2003 on the creation of a global culture of cybersecurity and the protection of critical information infrastructures, and other relevant resolutions.

8. 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.

9. 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.

10. 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.

11. 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 CERTs or cybersecurity incident response teams CSIRTs**) of another State. A State should not use authorized emergency response teams to engage in malicious international activity.

Confidence-Building Measures To Strengthen International Peace And Security

- 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;
- 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;
- Encouraging, on a voluntary basis, transparency at the bilateral, sub-regional, regional, and multilateral levels, as appropriate, to increase confidence and inform future work.
- 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.
- 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;
- Enhance cooperation, including the development of focal points for the exchange of information on malicious ICT use and the provision of assistance in investigations;

Confidence Building Measures To Strengthen International Peace And Security

- 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;
- 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;
- 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.
- 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 behavior in information space with regard to their potential role;
- States to promote further, at multilateral levels, the consideration of existing and potential threats in the field of information security, as well as possible strategies to address the threats emerging in this field, consistent with the need to preserve the free flow of information

Additional Norms from the UN GGE 2021 Report

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:

- 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.

Additional Norms from the UN GGE 2021 Report

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.

- 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.
- 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.
- 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.
- 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.

Additional Quotations from the UN GGE 2021 Report

- Confidence Building Measures: 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).
- **International cooperation and assistance in ICT security and capacity-building:** Creating and enhancing the capacity of CERTs/CSIRTs and strengthening arrangements for CERT/CSIRT-to-CERT/CSIRT cooperation.


MAGIRUS

FIRST's input to these processes

- **Informal conversations** with participants in the UNGGE, promoting our perspectives
- **Formal participation in the UN Open Ended Working Group** consultation for civil society organizations
- **Formal contributions both directly and as part of civil society associations**

Our views: Norms Development

- Emphasize **partnership and inclusion**
- Double down on **Capacity Building**
- **Raise awareness** of Cyber Norms and CBMs
- **Ensure CERT/CSIRT status as incident responders**

Our views: Proposed Policy

- Adopt practical measures to clearly **distinguish roles and responsibilities** of their communities (e.g. EthicsfIRST)
- **Consider how policy may negatively affect the CSIRT community**, e.g. criminalization of technical expertise
- Request states to build narrow exemptions on sanctions and export controls to **permit sharing of defensive cybersecurity information**
- Encourage states to review norms from multi-stakeholder communities
- "Cybersecurity is a shared responsibility. Cybersecurity requires comprehensive, inclusive and integrated efforts from governments, international organizations, businesses, civil society, professionals, and citizens. Cooperation and partnerships are central to the success of such efforts."

Our views: Input to the UN OEWG in 2022

FIRST encourages the OEWG to work towards ensuring that:

- Incident responders can continue to collaborate globally, especially in the time of a crisis
- The good of all internet users and the global Internet safety and security must be taken into account
- An open and inclusive multi-stakeholder approach is essential for successful incident response and security efforts.

Our views: Input to the OEWG in 2022

- We highlighted that comprehensive sanctions, especially at the time of armed conflicts, force FIRST to exclude teams from involved countries. The 2015 UNGGE norms recommend that states must not attack incident response teams and that **CSIRTs must not participate in offensive operations**.
- The 2021 UNGGE consensus report underscores the importance of ***avoiding the politicization of CERTs/CSIRTs and respecting the independent character of their functions***. Following this logic, Incident response teams (CSIRTs and PSIRTs) should be exempt from such sanctions. FIRST brings together incident response teams and helps them build capacity, network, share knowledge, and most importantly build trust to work together and cooperate even during a crisis.

Thank you

Sherif Hashem

sherif.hashem@first.org

Maarten Van Horenbeeck

maarten@first.org