

**COMMITTEE:** Cybersecurity

**QUESTION OF:** Countering State-Sponsored Cyberattacks on Critical Infrastructure

**SUBMITTED BY:** Ukraine

**CO-SUBMITTED BY:** Panama

**SIGNATORIES:** Azerbaijan, Afghanistan, Bangladesh, Italy, Finland, Estonia, United Kingdom, Canada, Israel, United States of America, South Korea, Nepal, France, Algeria

The General Assembly,

*Recalling* the purpose and the principles of the United Nations Charter, including the maintenance of international peace and security and the promotion of international cooperation,

*Fully aware* that the offensive-dominant nature of cyber warfare, difficulty of attribution and low entry barriers encourages both state and non-state actors to conduct large-scale disruption,

*Acknowledging* that operations conducted by state and state-backed groups include espionage, political manipulation and economic disruption,

*Recalling* its Resolution 70/237 of 23 December 2015, which endorsed the norms of responsible state behaviour in cyberspace and encouraged member states to protect their critical infrastructure from malicious ICT activities,

*Recognizing* the efforts of Member States to prioritize strengthening the security and resilience of critical infrastructure and enhancing national cyber readiness,

*Noting* with deep concern the growing incidence of state-sponsored and state-affiliated cyberattacks targeting critical infrastructure; that such attacks constitute threats to international peace and security; and the potential for such attacks to cause cascading humanitarian, economic and security effects,

*Affirming* that international law, including the UN Charter, the principles of sovereignty and non-intervention, the inherent right of Member States to self-defence and obligations arising under international human rights law and international humanitarian law, where applicable-applies to the use of ICTs and cyber operations,

*Acknowledging* that many critical infrastructure systems are privately owned or operated, and that public-private cooperation is essential for an effective response,

*Appreciating* the adoption by the General Assembly of the United Nations Convention against Cybercrime on 24 December 2024, following an inclusive and transparent intergovernmental process,

*Highlighting* the need to strengthen global cooperation and promote norms of responsible state behaviour in cyberspace,

Alarmed at the unprecedented increase in scam and phishing messages reported to the NCSC-FI (National Cyber Security Center), reportedly up 64% through the 3rd quarter of 2025, with bank-themed messages keeping prominence and threatening to undermine public trust,

Recognizing the importance of international cooperation, capacity-building, information-sharing, and technology transfer to reduce the global cybersecurity capability gap,

1. Calls upon Member States to affirm that malicious cyber-activities directed against critical infrastructure, whether by state or non-state actors, are unacceptable and undermine international peace and security;
2. Calls upon the United Nations system to recognise that cyber operations directed at critical civilian infrastructure of Member States and conducted in coordination with military actions may, depending on the circumstances, constitute certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes; as certain crimes committed by means of information and communications technology systems and for the sharing of evidence in electronic form of serious crimes.
3. Encourages states to adopt national legal and regulatory frameworks that require critical infrastructure operators to implement baseline cybersecurity measures, incident-reporting mechanisms and resilience planning;
4. Encourages public-private partnerships: states should promote cooperation between government agencies and private critical infrastructure operators to strengthen resilience, conduct joint exercises, incident-response drills, and share threat-intelligence;
5. Calls for Member States to develop resilience-enhancing measures in infrastructure design: network segmentation, redundant systems, supply-chain risk management,

recovery and continuity planning, and regular testing of government-controlled systems (ICS/SCADA) in critical sectors;

6. Requests the Secretary-General to convene, within twelve months, a single, global entity, a Cyber Emergency Response Team (CERT), under UN coordination, for threat-intelligence sharing, rapid technical assistance, and incident-response support; and with a focus on actionable attribution in the case of specific, high-intensity threats. This forum would bring together Member States, private-sector operators, civil society and international organisations;
7. Invites Member States to share information on malicious cyber-activity with the Open-ended Working Group on security of and in the use of ICTs (OEWG on ICTs);
8. Notes the special needs of states under active cyber-attack or emerging cyber-infrastructure threat and calls upon partner Member States and multilateral organisations to provide targeted capacity-building, cyber-education, technical assistance and resources to those states;
9. Urges Member States that have not yet done so to ratify the United Nations Convention against Cybercrime in accordance with their respective domestic legal frameworks and constitutional processes;
10. Further Requests all Member States to participate in a program in which they share best cybersecurity practices, learn from more prepared countries and co-develop defensive tools and policies to strengthen critical infrastructure resilience;
11. Calls upon developed and technologically advanced Member States, relevant UN bodies, and international organizations to provide targeted assistance to developing and under-resourced countries, including funding, training, technology transfer, and institutional support, to strengthen cybersecurity capacity and protect critical infrastructure;

12. Requests the establishment, under relevant UN bodies, of a Capacity-Building Initiative for Critical Infrastructure Protection focused on developing countries, which should:
- a. Provide technical training for government officials, regulators, and operators of essential services,
  - b. Support the creation or strengthening of national and sectoral Computer Emergency Response Teams in case of an emergency,
  - c. Assist in drafting or updating legal and regulatory frameworks for critical information infrastructure protection,
  - d. Promote secure-by-design principles in new infrastructure projects, especially in the energy, finance, and health sectors;
13. Invites donor states, international financial institutions, and private-sector partners to contribute funding, expertise, and technology to the CBI-CIP, ensuring that support is demand-driven and tailored to the needs of recipient developing countries;
14. Urges Member States to strengthen national cybersecurity frameworks to protect critical infrastructure, including energy grids, hospitals, transportation systems, and connected vehicles, against state-sponsored cyberattacks.