FORUM: United Nations Security Council (UNSC)
QUESTION OF: Strengthening International Cybersecurity and Preventing State-Sponsored Cyber Attacks
SUBMITTED BY: France
CO-SUBMITTED BY: Japan, United Kingdom, & Netherlands

THE SECURITY COUNCIL,

Recalling its primary responsibility under the UN Charter for the maintenance of international peace and security,

Recognizing the increasing frequency, sophistication, and geopolitical impact of state-sponsored cyber operations targeting critical infrastructure, electoral processes, and national security systems,

Deeply concerned by the growing risk of cyber operations escalating into armed conflict under Article 51 of the UN Charter,

Noting with alarm that over 40% of global cyber incidents in the past decade involved direct or indirect state participation, as reported by the UN Office of Counter-Terrorism (UNOCT),

Emphasizing that cyberspace remains a shared international domain requiring collective responsibility, transparency, and cooperation,

Reaffirming that international humanitarian law, the principles of state sovereignty, and the prohibition of the use of force apply fully to cyberspace,

1. Establishes the *United Nations Cyber Stability and Response Taskforce* (UNCSRT), operating under the UN Office of Counter-Terrorism, mandated to:
    a. provide rapid technical assistance to Member States experiencing severe or ongoing cyber attacks,
    b. Investigate cross-border cyber incidents upon invitation of affected states,
    c. coordinate information-sharing between national cybersecurity agencies, INTERPOL, and regional organizations,
    d. issue non-binding public incident-assessment reports when attacks carry significant geopolitical consequences;

2. Calls upon all Member States to refrain from knowingly supporting, directing, or tolerating cyber operations that target:
    a. electoral systems,
    b. national power grids, water systems, or other critical civilian infrastructure,
    c. hospitals and medical networks,
    d. UN agencies and peacekeeping missions;

3. Encourages Member States to adopt national legislation that strengthens cyber defense capacity by:
    a. requiring timely reporting of major cyber intrusions to competent national authorities,
    b. establishing minimum cybersecurity standards for companies operating critical infrastructure,
    c. providing funding and technical support for domestic cyber-response teams;

4. Recommends the development of a *UN Cyber Norms Framework* to promote predictable state behavior in cyberspace, which would:
    a. outline prohibited actions, including cyber operations causing physical destruction, mass disruption of essential services, or threats to international peace,
    b. clarify thresholds at which cyber operations may constitute breaches of peace or acts of aggression,
    c. encourage transparency measures such as voluntary disclosure of national cyber doctrines;

5. Requests the Secretary-General to appoint a *Special Representative on Cyber Peace and Security* to:
    a. oversee UNCSRT,
    b. facilitate dialogue between technologically advanced and technologically developing nations,
    c. deliver annual briefings to the Council on emerging cyber threats;

6. Encourages regional organizations—including the EU, AU, ASEAN, and OAS—to expand cooperation on:
    a. joint cyber exercises,
    b. mutual incident-notification procedures,
    c. coordinated sanctions against state and non-state actors involved in major cyber intrusions;

7. Decides that any cyber operation determined by the Council to constitute a threat to international peace may trigger appropriate measures under Chapter VII of the UN Charter, including targeted sanctions against individuals, entities, or state agencies responsible;

8. Decides to remain actively seized of the matter.