BACKGROUND GUIDE—
Seniors Advanced

GIISMUN
TOKYO 2025
CHAPTER 5

Committee:

UNSC

United Nations Security Council

Agenda:

Reinforcing the Global Non-Proliferation Regime: Bridging Gaps in Existing Treaties and Addressing Emerging Nuclear Threats

Hosted by Global Indian International School Tokyo
18th July ~ 23rd July 2025

Committee Overview

The Senior Committee of the United Nations Security Council (UNSC-Senior) serves as the body's "think tank," charged with anticipating emerging threats to international peace and security and crafting forward-looking policy recommendations. Unlike the main Council, which addresses crises as they erupt, UNSC-Senior focuses on the root causes and underlying dynamics—such as digital inequality—that can fuel instability, marginalization, and conflict. Delegates will practice bridging technical solutions with the UNSC's mandate to maintain peace, exploring how unequal access to technology can translate into security vulnerabilities, state fragility, and threats to human rights.

History of the committee

Established by the UN Charter on 26 June 1945, the Security Council was charged with maintaining international peace and security through binding resolutions, peacekeeping, and sanctions. In response to more complex, transnational challenges in the early 21st century—cyber threats, pandemics, climate-driven resource conflicts—the Council formed its Senior Committee in 2012 as a specialized forum for horizon scanning and preventive diplomacy.

- Key Milestones
  - 2013: First Senior Committee report on "Cybersecurity and Sovereignty."
  - 2017: Adoption of annual "Emerging Threats" thematic reviews.
  - 2021: Integration of digital inequality as a standing item, recognizing its role in undermining social cohesion and fueling extremist recruitment.

Background Information

Digital inequality—stemming from gaps in infrastructure, affordability, skills, and local content—exposes communities to security risks at multiple levels:

- State Fragility: Governments unable to deliver e-services lose legitimacy, inviting unrest.
- Transnational Crime & Terrorism: Ungoverned digital spaces become havens for illicit finance, recruitment, and disinformation.
- Human Rights: Marginalized groups (rural, displaced, women, older persons) face barriers to accessing humanitarian aid, legal recourse, and social protection online.

The Senior Committee must assess how to incorporate digital development into early-warning systems, strengthen cyber resilience in vulnerable states, and ensure that technological progress bolsters—not undermines—international peace.

Key definitions

- **Digital Inequality:** The differentiated access to, use of, and benefits from digital technologies among individuals and communities, often driven by disparities in infrastructure, affordability, skills, and local content availability,
- **Digital Divide:** The gap between those with reliable Internet access—and the skills to use it—and those without, encompassing factors of access, affordability, quality, and relevance rather than a simple binary distinction.
- **Digital Inclusion**: The practice of ensuring all individuals and communities —especially the most disadvantaged—can access and effectively use digital technologies for education, employment, healthcare, and civic participation.
- **Digital Sovereignty**: A state's authority and control over the digital decisions, infrastructure, data flows, and services within its jurisdiction, balancing national governance with the need for cross-border harmonization on cybersecurity, privacy, and trade.
- **Digital Public Goods**: Open-source software, data standards, and content that adhere to privacy and interoperability standards, designed to accelerate progress toward the Sustainable Development Goals by lowering barriers for governments and communities.
- **Data Governance**: The coordinated management of data's availability, usability, integrity, and security across organizations or nations, requiring harmonized legal and technical frameworks to prevent fragmentation and uphold privacy and ethical use.
- **Platform Accountability**: The obligation of online intermediaries (e.g., social media and hosting providers) to moderate, remove, or label harmful or illegal content, balancing freedom of expression with the need to curb disinformation, hate speech, and other risks.
- **Cyber Resilience**: An organization's or state's capacity to anticipate, withstand, recover from, and adapt to adverse cyber events—ensuring continuity of critical functions despite attacks or failures.
- **Cyber Hygiene**: Routine security practices and behaviors—such as regular software updates, strong authentication, and secure backups—that individuals and organizations adopt to maintain system health and reduce vulnerability to cyber threats.
- **Preventive Diplomacy**: Diplomatic action aimed at preventing disputes from arising or escalating into violent conflicts, through early warning, confidence-building measures, and mediation efforts.

- **Hybrid Threats**: Coordinated campaigns that blend military and non-military, overt and covert tactics—such as disinformation, cyberattacks, economic coercion, and the use of irregular armed groups—to destabilize societies without triggering conventional war.

- **Algorithmic Bias:** Systematic and repeatable errors in software algorithms that produce unfair or discriminatory outcomes against certain groups, often reflecting biases in data or design choices.

- **Digital Literacy:** The confident and critical use of digital technologies for finding, evaluating, creating, and communicating information; it encompasses core ICT skills—retrieving, assessing, storing, producing, and exchanging content via networked devices.

- **Information Resilience:** The ability of communities and systems to filter, verify, and withstand disinformation and manipulative content online—protecting social cohesion and informed decision-making (concept often discussed alongside cyber resilience in UN studies).

- **Network Resilience:** The capacity of digital infrastructure (networks, servers, and endpoints) to maintain acceptable levels of service in the face of faults, attacks, or other disruptions, often through redundancy, segmentation, and real-time monitoring.

Agenda Overview

The agenda and the committee's aim/targets

Agenda: Reinforcing the Global Non-Proliferation Regime: Bridging Gaps in Existing Treaties and Addressing Emerging Nuclear Threats

As digital tools become integral to governance, commerce, and social interaction, disparities in digital access risk creating new fault lines. The Senior Committee will develop policy frameworks aimed at:

- Expanding affordable, secure connectivity in least-connected regions.
- Strengthening cyber resilience of critical infrastructure in fragile and conflict-affected states.
- Enhancing digital literacy and civic capacities to resist disinformation, recruit responsibly, and participate in governance.

Promoting equitable innovation ecosystems that empower local entrepreneurs and rebuild war-torn economies.

Dicussion Points

- **Infrastructure and Security**: How can the UNSC-Senior facilitate public-private partnerships to extend encrypted broadband into underserved areas without creating new vulnerabilities?
- **Cyber Resilience in Peacekeeping**: What standards and training should be adopted so UN peace operations can secure their digital platforms and also assist host governments in cyber capacity building?
- **Digital Literacy as Conflict Prevention:** In what ways can educational and civil society actors be mobilized to inoculate communities against online hate speech, extremist messaging, and rumor-driven violence?
- **Innovation for Reconciliation:** How can small grants, incubators, and hackathons be structured to support youth-led tech initiatives that foster social cohesion in post-conflict settings?

Issues Faced by the Committee

Financial Constraints
Limited UN and member-state budgets for digital infrastructure in fragile contexts.

Sovereignty Concerns
States wary of perceived external interference when the UNSC engages on digital governance.

Rapid Technological Change
Emerging tools—like AI-driven deep fakes—evolve faster than regulatory or peacekeeping responses.

Data Privacy vs. Security
Balancing individual rights with state needs to monitor and counter threats.

UN Response (Actions taken)

Digital Peacekeeping Framework (2022)
A pilot guideline for embedding cyber advisors in UN missions, now active in missions to the Central African Republic and Libya.

Digital Blue Helmets (2016)
Launched under the UN Office of Information and Communications Technology, the Digital Blue Helmets program creates an internal cyber-security "rapid response" platform for sharing threat intelligence across UN entities.

Global Connectivity Fund (2023)
Pooled contribution from five Permanent Members to subsidize satellite internet in UN-designated "digital deserts."

Information Integrity Task Force (2024)
Multi-stakeholder body issuing best practices on combating election-related disinformation in fragile environments.

Open-Ended Working Group on ICT Security (2021 – 2025)
Mandated by GA Resolution 75/240, this OEWG brings together all Member States to negotiate norms for responsible state behavior in cyberspace, confidence-building measures, and capacity-building roadmaps.

Global Digital Compact (2024)
Under the Pact for the Future, Member States adopted the Global Digital Compact to enshrine commitments on universal connectivity, digital inclusion, data privacy, AI ethics, and cyber norms.

Scope of Debate

Possible Caucus Questions:

- What incentives can the Security Council provide for tech companies to operate transparently and affordably in conflict-affected regions?
- What role should the Council play in helping small towns set up community mesh networks when big companies won't build there?|
- How might cyber norms negotiated at the UN level intersect with existing peace agreements and regional security pacts?
- In what ways can women's and youth-led digital cooperatives be empowered to bridge both economic and security gaps?
- How can the UNSC make sure that women and girls get equal digital training so they are not left behind?
- Should the UNSC consider mandating minimum cyber-security standards for countries contributing troops to UN missions?

- How can data-sharing frameworks be designed so that early-warning signals from local networks inform Security Council deliberations without compromising sources?
- How can the Security Council leverage lessons from the UN ICT Task Force (2001–2004) to structure effective public–private partnerships for closing the digital divide?
- How might UNSC resolutions require peacekeeping missions to check their own cyber-security and share best practices with host countries?
- What confidence-building measures can help countries share cyber-threat information without fearing political fallout?

Sources / Useful websites

- UN Security Council Official Website : Provides comprehensive information on the Security Council's structure, functions, resolutions, and subsidiary bodies, including committees addressing emerging threats. https://www.un.org/securitycouncil/
- UN Peacekeeping Cyber Guidelines: https://peacekeeping.un.org/en/cyber-support
- Broadband Commission for Sustainable Development : https://www.broadbandcommission.org
- TU Global Connectivity Report : https://www.itu.int/en/ITU-D/Statistics
- Council on Foreign Relations – UN Security Council Backgrounder : Offers a comprehensive overview of the Security Council's role, challenges, and discussions on reform, providing context for its approach to emerging threats. https://www.cfr.org/backgrounder/un-security-council
- UN Office for Disarmament Affairs – ICT Security : Focuses on international efforts to address information and communication technology (ICT) threats, including reports from Groups of Governmental Experts (GGEs) and Open-Ended Working Groups (OEWGs). https://disarmament.unoda.org/ict-security/