Background Paper: Cybersecurity and the Foundation of Global Peace

Committee: United Nations Security Council (UNSC)
Topic B: Cybersecurity and the Foundation of Global Peace
chairs:

Introduction: Cybersecurity as a Threat to International Peace and Security

The digital age has introduced cyberspace as a fifth domain of warfare and conflict, directly challenging the foundational mission of the Security Council: the maintenance of international peace and security. Our position is that malicious cyber activity is a systemic security risk that poses a direct, escalating threat to global stability. Unlike traditional conflict, cyber threats are defined by the speed, ambiguity, and ease of escalation, necessitating immediate and decisive action from the UNSC to prevent digital incidents from triggering conventional warfare.

. Unique Characteristics and Threats to UNSC Mandate

Cyber operations possess characteristics that directly impede the Security Council's ability to act collectively and maintain peace:

The Risk of Escalation and Miscalculation

The difficulty of attribution determining the true source of a cyber attack—creates an environment of suspicion and distrust among states, often in the absence of hard evidence. This high level of ambiguity drastically increases the risk of miscalculation by one state leading to an unintended and disproportionate conventional or kinetic response by another. An attack could violate sovereignty without crossing the threshold of an "armed attack," yet still lead to a violent reaction that warrants UNSC intervention.

Targeting Critical Infrastructure (CNI) as a Threat to Peace

Attacks on Critical National Infrastructure (CNI) such as nuclear facilities, national power grids, financial systems, and essential communications networks—are not mere acts of espionage or crime. They are acts of aggression that can cause mass casualties, severe economic collapse, and humanitarian crises, meeting the definition of threats to international peace and security under the UN Charter. The UNSC must clarify that the deliberate, widespread targeting of CNI is a violation that may necessitate a collective response.

Erosion of Sovereignty and Political Stability

Cyber-enabled interference, including disinformation campaigns and election meddling, undermines the political stability and sovereignty of member states. When foreign actors utilize

cyberspace to destabilize a government or incite internal conflict, it creates conditions ripe for regional crises that demand the attention of the Security Council.

Current Legal and Normative Frameworks

The international legal framework confirms the applicability of international law to cyberspace, but clarity on enforcement is lacking:

Applicability of the UN Charter: Consensus has been established that the UN Charter, including Article 2(4) on the prohibition of the threat or use of force, and the inherent right of self-defense (Article 51), applies in cyberspace. However, the exact threshold for when a cyber operation constitutes a "use of force" or an "armed attack" remains a point of divergence among states.
Voluntary Norms: The UN has agreed upon non-binding norms of responsible state behavior, including the norm against deliberately damaging CNI. Crucially, these norms are voluntary and lack enforcement mechanisms, leading to a significant implementation gap where malicious activity continues unchecked.

Mandate and Action for the Security Council

Given its unique authority to mandate action, the Security Council must move beyond acknowledging the problem to establishing enforceable measures:

1. Clarify Legal Thresholds: The UNSC should work toward a resolution that clarifies its interpretation of the threshold for a "use of force" in cyberspace and determines when a major cyber incident constitutes a threat to international peace and security.
2. Institutionalize Confidence-Building Measures (CBMs): The Council should mandate the establishment of routine, secure cyber communication channels (hotlines) between member states especially those with known tensions to facilitate rapid de-escalation and information sharing during a crisis, thereby mitigating the risk of miscalculation.
3. Address Accountability: The UNSC should explore mechanisms for attribution and accountability for egregious violations of international law in cyberspace, particularly attacks on CNI that cause mass harm, which may include the consideration of sanctions against states responsible for such acts.
4. Promote Capacity Building: The Council must support capacity-building efforts to reduce the Digital Divide, as weak cyber defenses in any state create vulnerabilities that can be exploited globally, threatening collective security.

Conclusion

Cybersecurity is an existential challenge to the maintenance of international peace. The Security Council cannot wait until a catastrophic cyber incident triggers a conventional conflict to act. By clarifying legal applications, mandating CBMs, and establishing pathways for accountability, the UNSC can secure the digital domain and uphold its primary responsibility for global security.

cited works

Admin. 2022. “Background to UN Discussions on Responsible State Behaviour - Unidir.” Unidir (blog). March 11, 2022. https://nationalcybersurvey.cyberpolicyportal.org/background-to-un-discussions-on-responsible-state-behaviour/.

“UN GGE 2021 Report | Digital Watch Observatory.” n.d. Digital Watch Observatory. https://dig.watch/resource/un-gge-2021-report.