The Weaponization of Cyberspace and a New "Global Mechanism" at the UN

It is easy to be disillusioned over the current state of cyberspace. A promising realm for information exchange has become a treacherous environment, full of threats originating with state and non-state actors alike. It has become increasingly difficult for the average user to safely navigate the Internet, while even for states the volume and sophistication of offensive cyber operations pose major risks for their security.

By Amb. Paul Meyer, Senior Advisor, ICT4Peace

To date, some forty states have established cyber units within their armed forces, most of which are considered capable of "offensive" cyber operations. With the establishment of CAFCYBERCOM Canada has jettisoned the euphemistic "active cyber defence" terminology and now acknowledges it has developed "offensive cyber operations capabilities". Alongside the military there are also intelligence agencies who have invested heavily in cyber espionage. A challenge for victims of cyber intrusion is to determine whether the operation is intended to extract information or to destroy systems and disrupt operations. Unlike other forms of military action, offensive cyber operations are carried out covertly and states rarely acknowledge that they have been responsible for an attack on another state. Even the high profile Stuxnet attack in 2009 against Iranian nuclear facilities has never been officially claimed by the presumed perpetrators – the United States and Israel.

On a daily basis, we learn of state-conducted cyber operations that have exfiltrated tetra bytes of data or compromised critical infrastructure even

as those responsible hide behind a cloak of plausible deniability. China tops the list of adversarial cyber actors according to the latest threat assessment by the Canadian Government, stating that "Over the past four years, at least 20 networks associated with Government of Canada agencies and departments have been compromised by PRC cyber threat actors".

Alongside this real-world use – or abuse – of the Internet there have been efforts to subject this novel means for projecting power to some form of constraint. The weaponization of cyberspace can negate the societal and developmental benefits of this environment and "rules of the road" need to be agreed to curb destructive behaviour.

The United Nations has been a key venue in the effort to regulate state conduct in the quintessentially universal realm of cyber space. Since 1998, the UN General Assembly has had an agenda item on "Developments in the Field of Information and Communication Technologies in the context of International Security". Over 27 years, the UN has had a series of processes to consider state cyber conduct. The most significant output from this work was a 2015 document that enumerated eleven voluntary norms of "responsible state behaviour in cyberspace" that was subsequently endorsed by a consensus General Assembly resolution. Amongst these norms were agreement to refrain from cyber attacks directed at critical infrastructure on which the public depends, to prohibit attacks against Computer Emergency Response Teams (the "first responders" to cyber incidents) and to ban the use of proxies. This document is referred to as the "normative framework" and represents a high-water mark of international cooperation regarding state cyber behaviour.

The other major outcome of this lengthy process of diplomatic engagement was agreement this July on a final substantive report of an Open-Ended Working Group on cyber security after four years of proceedings. Importantly this report establishes a mechanism for on-going consideration at the UN of cyber security issues. This "Global Mechanism" would entail an annual plenary meeting alongside two thematic working groups: one on the spectrum of security issues encountered in cyberspace; and the other on capacity building programs

to help overcome the “digital divide” between developed and developing states. Provisions would be made for input from non-governmental stakeholders in civil society and the private sector given their critical role in cyberspace activity. The modalities for such participation by NGOs were a source of dispute throughout the group’s existence and the results, although far from ideal from a transparency perspective, do ensure a greater role for these non-governmental entities than had previously been the case.

The blueprint for the “Global Mechanism” will still have to receive final endorsement at an organizational meeting slated for March 2026, but the prospects seem good that finally the UN will have a permanent institutional home for consideration of cyber security issues.

The contrast between the norms of responsible state conduct and the incidents of offensive cyber operations that violate them points to a basic vulnerability of such accords. There is no real mechanism for the enforcement of these norms, and as we have seen in other areas, the UN Charter has a structural weakness in the veto rights granted to the five permanent members of the Security Council. These vetoes have protected permanent members from any action against their own culpability for violations of international law. The creation of a permanent UN body to address cyber security issues still suffers from an “accountability deficit” in its lack of a specific measure for holding states to account for their actions in cyberspace.

The NGO ICT4Peace, for which I am a Senior Advisor, proposed in 2020 the establishment of a “Cyber Peer Review” mechanism. Such a mechanism would be modeled on the Universal Periodic Review mechanism of the Human Rights Council. It would ensure a process whereby states could regularly be assessed on the degree of their compliance with the measures that they have agreed to. In the absence of a process for holding states to account, it is probable that some states will persist in conducting cyber operations in violation of the agreed normative framework of restraint. The future meetings of the “Global Mechanism” could be used to call out problematic behaviour by states. Such challenges in the opaque realm of offensive cyber operations may be difficult to sustain and would be vulnerable to being dismissed as just

disinformation by adversaries. It would be preferable if a form of systematic peer review could be instituted and provide an incentive for states to abide by the norms of responsible behaviour they have already agreed to.

ICT4Peace Foundation
Geneva, 27 October 2025

This blog post was published part of the "Canadian Security Interests and Trump 2.0" Conference.