Global Cyber Security – At last a "Permanent Mechanism" at the UN

By Paul Meyer, Senior Advisor, ICT4Peace
January 2026

Introduction

Cyber security as an international security issue has been steadily growing in salience during this century as states engage in ever more sophisticated offensive and defensive operations in cyberspace. Technological developments and the intensification of great-power rivalry have outpaced efforts at devising "norms of responsible state behaviour in cyberspace." This goal was brought closer on July 11 when a final report of a UN working group was adopted by consensus after four years of effort. A major outcome was agreement to establish for the first time a "permanent mechanism" at the UN to consider issues of international cyber security. After years of temporary ad hoc bodies a permanent forum (called the Global Mechanism) will be operational and serve as a venue for promotion of those "norms of responsible state behaviour" and an opportunity to call out violations of them. Canada was an active player from the beginning in the multilateral diplomacy of cyber security and can take some satisfaction that the outcome of the UN process broadly aligns with Canadian values and interests in a crucial domain for national security and well-being.

Background

The UN General Assembly via its First Committee on Disarmament and International Security has been studying the issue of cyber security (under the heading "Developments in the Field of Information and Telecommunications in the Context of International Security") for some 27 years. A Russian initiative at the origin, it rapidly gained wide support as states and stakeholders alike worried about the impact of malicious activity in cyberspace. The consideration has taken various forms, albeit with no sustained continuity, notably via Groups of Governmental Experts (GGE). These groups are formed by a limited number (15-20) government-nominated experts and normally undertake a study behind closed doors of a given problem over a couple of years culminating in a report if all can agree on one. These GGEs produced consensus reports each in 2010, 2013, 2015 and 2021, incrementally building up a body of common understandings and standards for state conduct. More recently, this work has been carried forward by more inclusive Open-Ended Working Groups (OEWG) in which any

interested UN member state can participate. An initial OEWG adopted its report in 2021 and a successor group has just adopted its final report on July 11 at the close of its eleventh week-long session.

A successful conclusion to a long diplomatic journey

The current OEWG, the formal if awkward title of which is "on the security of and in the use of Information and Communication Technologies (ICT)", has had eleven substantive sessions over the course of four years. These sessions have been supplemented by a series of informal consultations, several of which have allowed for the participation of other stakeholders (i.e., civil society and private sector entities with an interest in the subject matter but which normally have scant scope to input into inter-governmental processes such as those at the UN). The whole exercise has been skillfully steered along by its chair, Singaporean Ambassador Burhan Gafoor who methodically worked to find compromise solutions to points of contention and build a positive momentum in the group towards a substantial result. This was facilitated by his decision to issue successive "annual progress reports" to the General Assembly which built on each other in a manner that facilitated the adoption of the final report to the General Assembly. This report (the text of which is here) will provide the UN with authoritative guidance as to how responsible state behaviour in the use of ICTs should be achieved.

As the report notes the goal of the international effort is the creation of a "open, safe, secure, stable, accessible, peaceful and interoperable ICT environment". This cascade of adjectives reflects the varied features states wish to see in our networked cyberspace.

Key Themes

The report is structured along the six themes that have dominated the group's discussions: i) existing and potential threats; ii) norms of responsible state behaviour; iii) international law; iv) confidence building measures; v) capacity building and vi) regular institutional dialogue. To a large extent the language of the report reflects the usual wordsmithing and balancing required in order to gain universal acceptance for an official text. That effort, albeit painful at times, has the great benefit of universal support for the outcome.

Existing and Potential Threats

The increase in the frequency and scope of malicious cyber activity is a reality that any threat assessment must acknowledge, even if states are coy as to the nature of their own operations. The report strikes a mean which notes that "a number of States are developing ICT capabilities for military purposes" and that "the use of ICTs in conflicts between States is becoming more and more likely" while simultaneously calling on States "to use ICTs in a manner consistent with international law and promote their use for peaceful purposes". Beyond the direct military applications, the report flags "the worrying increase in States' malicious use of ICT-enabled covert information campaigns to influence the processes, systems and overall stability of other States". Other contemporary cyber threats such as those associated with compromised supply chains, exploitation of vulnerabilities in the Internet of Things, ransomware and the proliferation of "ICT-intrusive capabilities" all receive a brief acknowledgment.

Rules, Norms and Principles of Responsible State Behaviour

This section is the heart of the report in the sense of providing standards for state conduct. It refers to the chief output of the UN's past work on cyber security – the 2015 report of the GGE which enumerated 11 voluntary norms of responsible state behaviour in cyberspace (subsequently endorsed by a consensus UNGA resolution). These norms included such key constraints as the non-targeting of critical civilian infrastructure on which the public depends; a ban on attacks against Computer Emergency Response Teams (CERTs – the first responders to cyber incidents); foreswearing the use of proxies or allowing one's territory to be used for malicious cyber activity. Collectively these steps have become to be known as the "normative framework" ostensibly governing state behaviour.

The final report does not further extend this framework although it elaborates on how addressing certain outstanding issues can be linked to one or the other of the norms, thus reinforcing its authority. The report does emphasize the importance of the norms "reducing risks to international peace, security and stability and play an important role in increasing predictability and reducing risks of misperceptions, thus contributing to the prevention of conflict".

What role for International Law?

The extent to which states' conduct in cyberspace is subject to international law has been debated since the start of UN deliberations. The report reaffirms the emergent consensus that international law and specifically the UN Charter applies to cyberspace. While capturing this broad consensus the report essentially defers to the future a discussion that remains unresolved, namely how does international law apply to the actual use of ICTs? Given that cyber operations often inhabit a "grey zone" with respect to existing international humanitarian laws predicated on a state of "armed conflict"(or the UN Charter's terminology of "armed attack") it will be important for states to continue to exchange views on these specific cases in future.

Confidence-Building Measures (CBMs)

From the beginning it has been recognized that confidence-building measures would be desirable in this novel domain of international security action. The report trumpets one of the more tangible outcomes of the OEWG's work since its inception. This is the establishment as of May 2024 of a Points of Contact Directory by which states provide contact information for diplomatic officials and technical experts as to enable direct communication between states with respect to cyber incidents. A standard template for such communications has been developed and significantly modalities agreed for updating and periodically testing the operational status of the Directory to ensure it is an effective tool. In addition, a number of proposed global CBMs have been generated by the group although these like the norms retain their voluntary nature. In a display of immodesty becoming common with such UN groupings, the OEWG itself is proclaimed as a CBM as would be the future "permanent mechanism" overseeing the UN's work on cyber security.

Capacity building

In the UN, with its majority membership of developing states, it is not surprising that the need for capacity building is a refrain especially in contexts like that of cyberspace with a distinct "digital divide." The report duly prioritizes capacity-building a theme dear to the hearts of many member states which struggle to acquire the capabilities to fully participate in and benefit from cyber security proceedings. A dedicated ICT Capacity Building portal for identifying needs

and facilitating assistance is one specific recommendation of the report as is continuing the practice of holding regular Global Roundtables on the subject.

Regular Institutional Dialogue

While many facets of the cyber security challenge are addressed in the report, a crucial aspect concerns the principle of ensuring a Regular Institutional Dialogue at the UN going forward. This principle has been further refined during the OEWG's deliberations as requiring the establishment of a "permanent mechanism" (renamed in the report as the "Global Mechanism) for ongoing consideration of cyber security matters under UN auspices.

Under the careful supervision and encouragement of the Chair, the basic parameters of the permanent mechanism developed over the four annual progress reports are now in place. It would consist of "a single-track, State-led permanent mechanism" with the goal "to promote an open, secure, stable, accessible, peaceful and interoperable ICT environment".

The structure, scope, and schedule for this new institution was carefully elaborated and described in detail in the OEWG's third Annual Progress Report and endorsed in UNGA resolution A/RES/79/237). In particular, the mechanism is "to advance implementation of the cumulative and evolving framework for responsible state behaviour in the use of ICTs". This reference is to the 2015 normative framework discussed above with its 11 voluntary norms of responsible state behaviour. While the framework represents an important codification of norms of state conduct in cyberspace, it is also fair to say that they frequently have been honoured in the breach rather than in the observation. Consider the evidently wide-spread action of the placement of malware in elements of the critical civilian infrastructure of adversaries (e.g. power grids, transportation controls and water management systems). An on-going focus on state implementation as distinct from declaratory policy is thus widely seen as a crucial future function for the permanent mechanism.

The final report contains an annex outlining "additional elements for the Global Mechanism" that specifies the procedures and timetable that the permanent mechanism will follow. There is a lot of detail in this annex, but the Chair was evidently trying to stipulate as much as possible in the report rather than run the risk of leaving procedural gaps that could lead to disruptive disputes in the future.

The report sets out a five-year cycle of activity for the Global Mechanism with annual plenary sessions and a review conference to be held in the final year of the cycle. The report envisages the establishment of two thematic working groups. The first is to address "specific challenges in the sphere of ICT security" and the second is "to accelerate ICT capacity building". The groups will continue their work until the first Review Conference (provisionally set for 2031) which will decide on the number and scope of the dedicated thematic groups that are to be convened over the subsequent four years.

The new Global Mechanism will meet twice a year with one week for thematic groups and one week for the plenary session. It had been suggested that these group meetings will be convened immediately prior to or immediately following the annual substantive plenary sessions. This provision will yield the practical benefit of allowing delegates to cover both the groups and the plenary session in the same timeframe thus reducing extra travel and costs for participation (and facilitating the attendance of experts from capitals). It is noteworthy that this arrangement

proposed in the initial draft of the report was dropped in the final version leaving the question of scheduling open.

It is further specified that all meetings of the thematic groups will take place in a hybrid format. The possibility of establishing additional thematic groups is provided for although any such decision will require consensus agreement.

All of the above arrangements including agreeing dates for the sequence of meetings in the 2026-2031 timeframe are to be considered and approved by an organizational meeting to occur no later than March 2026 with the first plenary session of the new mechanism to be held no later than June 2026.

NGO involvement

The last issue the report grapples with is the troubled history of the participation of non-state actors in the work of the group. Since the inception of the OEWG there has been a battle over the modalities for such participation, with some states hiding behind the UN procedure whereby member states can veto the accreditation of a non state entity and do so anonymously and without having to disclose a reason. The OEWG had witnessed the rejection of private sector and civil society actors that would normally, given their expertise, have been welcomed into the group's deliberation. The Chair has engaged in a protracted effort to obtain a better deal for these stakeholders recognizing the importance of their inclusion for the credibility of the entire process and especially for the new mechanism going forward.

Despite his best efforts the modalities for inclusion of such stakeholders (i.e. businesses, NGOs and academia) are still rather contorted. Basically, a state objecting to the accreditation of any stakeholder is to communicate this decision to the Chair and disclose "on a voluntary basis" the basis for the objection. The Chair is then to disseminate this information to the rest of the member states and engage in "informal consultations for a period not exceeding three months regarding the concerns expressed with a view to facilitating accreditation wherever possible".

A more open approach to stakeholder inclusion was championed by Canada and Chile producing a working paper co-sponsored by 42 states. This paper proposed that any objection to the accreditation of a stakeholder would have to be put into writing with the rationale for that objection specified and the letter subsequently made public. It also advocated for a procedure by which if no consensus was achievable with respect to a particular stakeholder the matter should be settled by majority vote. This was a commendable expression of support for inclusivity, but in the end fell victim to the same resistance on the part of certain states to allowing non-state actors a greater say in this work that has been evident from the start. In the end, the formula contained in the final report while far from a guarantee of accreditation at least provides for a degree of transparency into the process which may act as a deterrent against arbitrary use of the veto prerogatives of member states.

Canada's role

Canada has been an active player from the start of UN work on international cyber security policy. It has been a vocal proponent of greater involvement of non-governmental entities in the UN processes (such as its joint working paper with Chile noted above). It has developed working papers on several themes including an influential guide on how states can

operationalize each of the agreed norms. Finally, Canada has espoused (and provided crucial funding) for action to promote gender equality in cyberspace and counter malicious activity that targets women. Overall Canada has demonstrated a refreshing initiative in helping to shape the contours of international cyber security policy rather than adopting a more passive posture. As a country that constantly refers to its support for the "international rules-based order" it was appropriate for Canada to exercise leadership in the multi-year effort to create a normative framework to govern this new and challenging domain of state action.

Conclusion

So more than a quarter of a century after the UN first addressed the issue of ICT use in the context of international security how are we to assess its latest outcome? On the plus side the OEWG's final report reaffirms and reinforces the core normative framework from 2015 and supplements it through several practical measures (e.g. the Points of Contact Directory; CBM proposals; a checklist for implementation of the eleven norms). Importantly it also establishes the first on-going institutional arrangement – the "permanent" now renamed "Global" mechanism – as a focal point for all future consideration of international cyber security at the UN. At the same time and as the report itself acknowledges malicious use of ICTs by state and non-state actors alike has continued to grow in a myriad of ways including means that pose major threats to civilian users (think of ransomware and the cyber compromise of critical infrastructure).

The effectiveness of the new Global mechanism has yet to be proven and the organizational meeting of next March could still witness a dilution of its authority. The fact however that a new UN forum dedicated to the security implications of this most universal of technologies will begin to operate next year should not be underestimated. Ideally the new mechanism will become more than a discussion forum and take on a peer review function as to how states implement their commitments. ICT4Peace, a Swiss-based NGO for which the author acts as an advisor has been an engaged stakeholder in the UN's work on cyber security from the start. It has proposed that a peer review mechanism based on the Periodic Review Mechanism of the Human Rights Council be instigated at the UN to help hold states to account for their behaviour in cyberspace. Declared adherence to norms of responsible state behaviour are all for the good, but in the absence of the transparency and accountability that comes with a review mechanism can we rely on improvements in the implementation record of states?

This text was first published by the Canadian Global Affairs Institute in January 2026.