CPI
CYBER POLICY
INSTITUTE

ICTs and International Security:
The Third Way

Eneken Tikk and Mika Kerttunen

The second substantive session of the Open-ended Working Group on developments in the field of information and telecommunications in the context of international security (OEWG) will meet multiple and partially irreconcilable views on how information and communication technologies (ICTs) should be addressed in the context of international security.

The OEWG differs from the previous format in which this issue has been addressed, the UN Group of Governmental Experts (GGE), in several important ways. The GGE is unwilling and unable to meet the expectations of transparency and inclusiveness. It is explicitly focused on strategic cybersecurity concerns – primarily those of interest to the Russian Federation and the United States of America. This makes the OEWG the only venue with the potential of hearing and accommodating all interested voices.

This potentially accommodating role of the OEWG cannot, however, be taken for granted. Like all GGEs before it, the OEWG is jealously guarded by the USA and Russia, both determined to control and direct the international discussion according to their visions and ambitions. Their positions are built on the shared goal of preventing an unwanted [nuclear] confrontation between them. Around these two poles gather groups of states anchored in one or the other's positions. It therefore falls upon other governments to seize the full potential of the OEWG by carving out a shared path.

The need for a more constructive dialogue was evident way before the OEWG was established. Over the past two decades, states have shared hundreds of pages of views with the Secretary-General. Many of their thoughts have never been addressed in the GGE. The quest for change is also apparent in the statements and contributions that industry and the civil society have made during the OEWG process. This *third way* is characterized by calls for less securitized and more human-centric dialogue, shared conviction that states' actions in cyberspace [as in any other domain] must be guided and governed by international law, a genuinely open mind to possible gaps in international law and ways to overcome them, demands for transparency and inclusiveness of the process, a sense of shared responsibility, exercise of restraint, and due focus on the benefits of digitalization and the role of ICTs in sustainable development and peace.

Although the OEWG derives from, and must acknowledge, the achievements of the GGE, renewing international cybersecurity talks requires critical assessment of its premises and conclusions. Not all states consider the work of the GGEs as cumulative. We are yet to assess the full consequences of the 2016—2017 GGE's lack of consensus. The very resolution underpinning the OEWG has set the precedent of re-wording GGE's earlier texts. Moscow's and Washington's tacit agreement on succession and coherence between the two processes could be contingent in an attempt to figure out how to best moderate their next steps.

Building its discussions on the structure and language of the work of previous expert groups risks making the OEWG hostage to the boundaries dictated and accepted by the GGE. Simply inviting additional views on threats, applicable international law, possible non-binding norms for responsible state behavior, confidence and capacity building could impose on OEWG discussions the many hidden assumptions and faulty logic of the earlier outcomes and no-outcomes of the GGEs. Following the structure and premises of the earlier conversation makes it easier for the USA and Russia to moderate progress or no-progress in both venues, thereby preventing an alternative approach to issues of ICTs and international security.

To effectively tackle issues of international cybersecurity, the OEWG must independently identify and link problems and solutions. This requires embarking on questions thus far not asked or answered. What actual concerns does the international community have about state uses of ICTs? What causes and enables irresponsible behavior? What role do gaps in national capacity play in the threat picture? Which of these issues, if any, constitute a threat to international peace and security? Which of these should the OEWG prioritize? What experience can countries exchange in overcoming identified and shared concerns? Where should cybersecurity rank among other security and stability problems that the world is facing?

An independent discussion of threats and shared concerns is necessary to address the question of applicability of international law. Without agreeing on issues to which international law, rather than, for instance, diplomacy, technology, markets, or increased awareness, is expected to provide answers, it is impossible to detect gaps in existing law. Where gaps become visible, overcoming them can be simply a matter of interpretation, or it may require negotiating new rules, which is hardly a real option in a heavily polarized international community. National statements and submissions are a good starting point for revisiting the question how international law applies.

The OEWG should avoid the GGE's shortcuts. A serious fallacy in the 2015 GGE report is that it downgrades well-established concepts of international law, duly followed by most states, to voluntary and non-binding norms – a tenet that, if taken as a basis of the OEWG discussions, could seriously undermine international law. Should voluntarism as an approach be adopted by the OEWG? Without commonly perceived and prioritized issues, it becomes next to impossible to decide what, if any, effective remedy can come from the strictly voluntary and non-binding norms, rules and principles, or how they are to be implemented.

Similarly, confidence-building measures (CBMs), and their effectiveness, are directly related to a shared reading of threats, their perceived severity and acuteness as well as relations between the states concerned. Different regions have different assessments of issues as well as types of measures to address them. Comparing these views and the chosen measures can be a good starting point for deciding which, [if any,] of these measures would be useful in the UN setting. Notably, both OSCE and the GGE have adopted a particular approach to CBMs, setting transparency and cooperation as a precondition to discussing restraint. This way, the need for restraint, including, and especially, by the relatively few states repeatedly implicated in using ICTs in power projection, has not been addressed, or assessed, in the international discussions so far. However, transparency and cooperation are unlikely in the conditions of perceived enmity, whereas effective measures of mutual restraint might satisfy both sides, while providing predictability and security to others.

The OEWG presents the international community with an unprecedented opportunity to conduct a transparent, inclusive and effective international cybersecurity discussion. Basing the work of the OEWG on the premises and logic of the GGEs risks subjecting this new process to the entrenched expert dialogue's limitations and [no-]outcomes. Free from these limitations, the work of the OEWG has the potential of confirming or counterbalancing the currently established views.

***

Eneken Tikk and Mika Kerttunen are independent experts who have participated in numerous global, regional and national cybersecurity discussions. Eneken advised the Estonian expert in the 2012—2013, 2014—2015 and 2016—2017 GGEs. Mika was part of the Finnish GGE delegation in 2016—2017. From 2014 to 2019 Eneken was the course director of ICT4Peace Foundation's international cybersecurity capacity building program. As of 2020, the Cyber Policy Institute runs its own International Cybersecurity Masterclass.

Please contact us:

tikk@cpi.ee
+372 507 22 70
www.cpi.ee