RSIS COMMENTARY

27 March 2026

Unpacking the Upcoming Global Mechanism on ICTs in the Context of International Security and the Role of Non-state Stakeholders

Eugene EG Tan and Benjamin Ang

PONDER THE IMPROBABLE

RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS 30

RSIS | S. RAJARATNAM SCHOOL OF INTERNATIONAL STUDIES
Nanyang Technological University, Singapore

RSIS COMMENTARY

www.rsis.edu.sg

No. 063 – 27 March 2026

Unpacking the Upcoming Global Mechanism on ICTs in the Context of International Security and the Role of Non-state Stakeholders

By Eugene EG Tan and Benjamin Ang

SYNOPSIS

The United Nations "Global Mechanism on developments in the field of ICTs in the context of international security and advancing responsible State behaviour in the use of ICTs" (Global Mechanism) begins this month with its organisational meeting to set up permanent discussions at the United Nations. Non-state stakeholders have an essential role in these discussions but face opposition from some states. This commentary suggests how they can still contribute.

COMMENTARY

For over twenty years, discussions at the United Nations among states have grappled with rules for the use of information and communications technology (ICT), and for the past ten years, the framework for responsible state behaviour in cyberspace. With geopolitical tensions spiralling into open conflict around the world and states' use of offensive cyber capabilities in conflict, there is an understandable sense of concern about the efficiency and efficacy of this framework, and whether it can create a peaceful and stable cyberspace for all states.

Continuing negotiations on the rules of the road for cyberspace is not impossible. The United Nations Open-ended Working Group on Peace and Security in the use of ICTs 2021-2025 (UN OEWG 2021-2025) passed four annual progress reports by consensus despite the furore over Russia's invasion of Ukraine. States worked to ensure that the conversation over rules for the use of ICTs continues in a more sustained and permanent manner through the Global Mechanism.

What is the Global Mechanism?

The Global Mechanism was born out of the OEWG 2021-25 negotiations and was set up to continue its work.

States recognised that the outstanding issues among themselves regarding the use of ICTs will not be overcome anytime soon. The permanent nature of the Global Mechanism reflects this impasse among states, but also recognises the importance of reaching consensus and a lasting agreement.

Based on the OEWG 2021-2025 experience, we anticipate that progress at the Global Mechanism will be painfully incremental, if any, especially in international law and norms. The use of offensive cyber operations in conflicts from Ukraine to Venezuela and Iran shows that states are unlikely to curb their military use of cyber capabilities, even in violation of international law. This is not unique to the cyber domain but part of some states' broader violation of existing international law regarding sovereignty and use of force.

Focusing on Capacity Building and Confidence Building Measures

The areas where the Global Mechanism can make meaningful progress are in the application and implementation of agreed norms through capacity-building and confidence-building measures. Many states remain willing and interested in capacity- and confidence-building measures with one another. During the OEWG 2021-2025, capacity building was the most achievable pillar to advance the framework for responsible state behaviour in cyberspace, given the uneven cyber maturity among states. States have been called to convene regular Global Roundtables on ICT security capacity-building to facilitate capacity-building technical-level discussions among capacity-building practitioners, representatives of interested states, and other interested parties and stakeholders, including businesses, non-governmental organisations, and academia.

The OEWG 2021-2025 reports also listed eight confidence-building measures for cooperation and incident resolution. States are invited to share a variety of information, including best practices in critical information protection and national strategies to strengthen public-private partnerships and cooperation on cybersecurity.

Even though non-state stakeholders do not seek a vote, which is reserved for states, most states recognise that discussions on ICT greatly benefit from, and should include, input from non-state stakeholders, especially those with the expertise, experience, and ownership of key ICTs. Non-state stakeholders, in turn, recognise that the states need their support to ensure the peace and security of cyberspace.

Potential Role of Stakeholders in the Global Mechanism

Unfortunately, while states are called on to partner and cooperate with non-state stakeholders, a small number of states seem to insist these stakeholders are not welcome because the Global Mechanism is an inter-state process. During the OEWG

2021-2025, these states vetoed the participation of many key stakeholders who could have contributed valuable technical or legal input to the discussions.

As an accredited non-state stakeholder, we appreciated that input was recorded, but we were disappointed that many states were absent during our brief time for interventions. Non-state stakeholders will face the same challenges in the upcoming Global Mechanism.

But the tail does not need to wag the dog. Non-state stakeholders have other ways to build conditions for better discussions at the Global Mechanism. At the final substantive meeting of the OEWG 2021-2025, we proposed a parallel process for non-state stakeholders to meet, share expertise, discuss complex technical and legal issues, and subsequently present consolidated reports to key Global Mechanism meetings. This track 2 process, which could also be track 1.5 to welcome input from interested states, will avoid the politicised accreditation veto system, provide adequate time for non-state stakeholders to dive deep into issues, and provide the Global Mechanism with digestible, relevant, and useful inputs. The proposal has received positive feedback, but will need support from national, regional, and international entities to move forward.

Non-state stakeholders also have more work to do on capacity and confidence building at the national, regional, and international levels, especially on issues such as ransomware, the protection of critical information infrastructure, and the security implications of emerging technologies. In the ASEAN region, non-state stakeholders should continue to actively contribute to the work of the ASEAN-Singapore Cybersecurity Centre of Excellence (in Singapore), the ASEAN-Japan Cyber Capacity Building Centre (in Bangkok), and the ADMM Cybersecurity and Information Centre of Excellence (ACICE), including through annual programmes like the UN-Singapore Cyber Fellowship and the Digital Defence Symposium.

Accreditation is not the sole measure of influence. Non-state stakeholders can advance the objectives of the Global Mechanism by continuing to build capacity, strengthen confidence, and translate technical expertise into actionable cooperation. If there is support for the separate stakeholder process, they can also synthesise and provide deep expertise to the Global Mechanism. By doing so, they help sustain progress even when formal processes stall. Practical engagement, not procedural access, will ultimately determine whether the Global Mechanism delivers meaningful outcomes.

Benjamin Ang is Head of the Centre of Excellence for National Security (CENS) and Future Issues and Technology (FIT) at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. Eugene EG Tan is Associate Research Fellow at CENS.

Please share this publication with your friends. They can subscribe to RSIS publications by scanning the QR Code below.