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

RSIS COMMENTARY

www.rsis.edu.sg No. 137 – 9 September 2021

A More Secure Cyberspace: Can UN Lead the Way?

By Sithuraj Ponraj

SYNOPSIS

The successful conclusion of the recent UN discussions on cybersecurity was a significant achievement. This signals a renewed political commitment by the international community to ensure a secure and stable international cyberspace.

COMMENTARY

THE RECENT UN Security Council (UNSC) debate in June on "maintaining international peace and security in cyberspace" was a significant political moment. Proposed by Estonia as part of its one-month long rotating presidency, the debate was the first formal UNSC discussion on the subject.

As speakers noted during the debate, cyber-attacks ─ whether State-sponsored or otherwise ─ have developed in intent and sophistication to a point where they could deeply destabilise entire societies and the international system. Cyber-attacks disrupt the delivery of basic critical and essential services; cripple supply chains; bring economies to a stand-still; and affect the integrity of electoral and political processes and public institutions.

Needed: UN's Decisive Role

The expectation from many quarters is that the United Nations — and specifically the UNSC — should play a decisive role in addressing the issue, given that any one of these factors could serve as a flashpoint for a nasty geopolitical conflict and a breakdown of the international rules-based order.

The UN has a strong foundation on which to build this effort. Six Groups of

Governmental Experts (GGE) have met since 2004 to develop rules, norms and principles of State behaviour in cyberspace. The most recent GGE and a newly set-up Open-Ended Working Group (OEWG) working on the same issues concluded their work in March and May this year.

There were substantial consensus reports that affirmed the importance of implementing an effective framework of responsible State behaviour in cyberspace. The UN Third Committee, one of six main committees of the UN General Assembly, has also been pursuing discussions on the topic of cybercrime.

The UNSC itself has had several informal discussions on cybersecurity at the initiative of its members referred to as “Arria-formula” discussions since 2016.

However, these discussions continue to be dogged by geopolitical disagreements and significant differences of opinion. These differences are on which international laws should apply to cyberspace, how they should be applied ─ and perhaps just as importantly, if new norms should be developed and what happens if these laws and norms are violated. Then, there is the tricky problem of attribution.

Urgent Need to Build Trust

The splintering of countries into various blocs seeking to impose their own technical standards and costs will not only have a detrimental impact on the international multilateral rules-based order. It will also cause a bifurcation of the Internet and embolden cybercriminals who depend on such a fracture to thrive.

None of these outcomes can be in the interests of the international community ─ especially small and developing States who would most likely be caught in the middle.

UN cybersecurity discussions need to find a workable framework to maintain the relevance of multilateralism in such a fraught environment. It must find a way to seize the political moment offered by the successful conclusion of the recent OEWG as well as the 6th GGE.

This must be taken together with the commitment expressed by all the speakers at this first formal debate to successfully forge an open and inclusive platform for addressing cybersecurity issues and potential geopolitical conflict.

There is an urgent need to build trust and confidence in international cyberspace. Small and developing states may have an important role to play in this process by providing perspectives that will focus the discussions on immediate issues and practical solutions beyond continuing strong partisan pressures.

Calling Out Bad Behaviour

In this regard, it is crucial that the next set of UN cyber discussions develop a long-term institutional mechanism that builds transparency and accountability into all efforts to implement rules, norms and confidence-building measures (CBMs). Also urgently needed are capacity building programmes, together with a strong reference to those agreed by consensus at previous GGEs and OEWGs.

But implementation is only one side of the equation. While discussions on how and when international law and agreed norms apply in cyberspace continue to be useful, such a mechanism could also seek to encourage States to voluntarily report on their implementation status.

At the same time, the UN membership — whether through this mechanism or UNSC — could consider mainstreaming cyber diplomacy and itself clearly call out bad behaviour. For example, such statements could call out cyber-attacks that target critical infrastructure and disrupt the delivery of basic and critical services to the public, such as the 2017 WannaCry and NotPetya attacks.

Technical, operational and political complexities could mean that most cases of attribution to a specific actor or actors will always remain a national prerogative. Calling out bad behaviour (even without attributing it to an actor) serves two purposes:

First, it signals clearly that the international community finds such behaviour unacceptable; second, it allows small and developing countries and regional groupings to add their voice to a larger, non-partisan statement. Statements calling out bad behaviour should specifically link the behaviour to the norms being breached, to anchor the relevancy of previous UN outcomes.

Can the UN Anchor Its Continued Relevance?

In this regard, it is important that UN cyber discussions also urgently identify ways to foster appropriate and meaningful engagement on cyber issues with private stakeholders including industry, academia, civil society groups and NGOs at the UN.

These players often possess significant levers and can bring resources to the continued development of a trusted and secure cyberspace, through technical expertise, thought leadership and capacity building resources.

The beginning of a new five-year OEWG discussion process from 2021-2025 represents an opportunity for the UN to anchor its continued *multilateral* relevance for cybersecurity discussions. It is important that small and developing nations and regional organisations strongly support this effort.

Sithuraj Ponraj is Senior Visiting Fellow at the Centre of Excellence for National Security (CENS) at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore. He was previously Director of the International Cyber Policy Office in the Cyber Security Agency, where he played a key role in developing Singapore's international cybersecurity strategy.