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

RSIS COMMENTARY

www.rsis.edu.sg No. 042 – 28 March 2024

The UN Framework of Responsible State Behaviour for a Secure Cyber Environment

By Eugene EG Tan

SYNOPSIS

The security of cyberspace depends on how much and to what extent member states adhere to the UN framework of responsible state behaviour. The framework provides states with the tools and capacity to deal with malicious cyber activity. Mechanisms both inside and outside the United Nations can be leveraged to complement the framework in dealing with such threats.

COMMENTARY

Malicious activity in cyberspace seems to be occurring more frequently, in both scale and intensity. States have reported malicious activity targeted at their critical infrastructure, such as ransomware attacks on healthcare facilities, ports, and government apparatuses; wiper malware attacks; and even the pre-positioning of malware for exploitation in potential conflicts.

The framework of responsible state behaviour aims to reduce malicious activity by state and state-sponsored actors. This includes the strengthening of confidence-building measures among states and non-state stakeholders, implementation of the norms of responsible state behaviour agreed to by the United Nations Group of Government Experts (UNGGE) in 2015, and adherence to the principles of international law.

Some states have also stepped-up discussions on the implementation of the norms at the ongoing United Nations Open-ended Working Group for security in and of the use of Information and Communications Technology (ICT) 2021-2025 (OEWG).

Countering Malicious Activity

Having a framework of responsible state behaviour, or “rules of the road” so to speak, enables states and non-state stakeholders, including businesses, academia, civil society, and think tanks, to assess their respective risk appetites and potentially tailor the relationships they wish to have with one another. States need to adopt the 3Cs, namely, compliance, cooperation, and consequences, for a framework of responsible state behaviour to be effective.

Compliance

Much of the requirement to comply rests on how states accept the framework and how their policies and decisions align with it. States need to show their commitment to keep to the normative framework. The propensity for states to renege on the agreed framework of responsible state behaviour increases with every episode of non-compliance, and the effectiveness of the framework to prevent, disrupt, and mitigate malicious activity decreases.

Cooperation

The norms of responsible state behaviour require states to cooperate and not to act unilaterally. States and non-state stakeholders need to build bridges and mutual confidence. States can share resources for collective cybersecurity through joint advisories and joint operations to counter and disable malicious actors. Adhering to such a framework of cooperation also progresses the discussions at the OEWG and brings the community closer to a cyberspace that is safe to operate in and conducive to development of the cyber ecosystem.

Consequences

Irresponsible behaviour by states should not be ignored. When they occur, there should be consequences although these should not be framed as penalties. For example, a “consequence” may take the form of a decision not to operate in non-compliant countries, which is a business decision and not a political tool to deny them the development of ICT. The converse is also true where the more responsible a state is, the less risk there will be for business and, consequently, more investments for it.

Having these 3Cs in place will help to strengthen the framework of responsible state behaviour to prevent, disrupt and mitigate the effects of malicious cyber incidents as they provide clarity on what could happen if a malicious operation were to take place.

Weaknesses in the Framework of Responsible State Behaviour

However, the framework of responsible state behaviour has three major weaknesses in preventing malicious activity, namely, lack of capacity and confidence, reluctance among states to share information and non-reporting of vulnerabilities, and exploitation of the supply chain for malicious activity.

Lack of capacity and confidence

The importance of capacity to respond to malicious incidents and confidence to cooperate in addressing malicious activity cannot be overlooked, especially in cases where immediate cooperation against such activity is needed. The norms call for states to respond to appropriate requests for assistance by a state whose critical infrastructure is subject to malicious cyber acts emanating from their territories. However, there is no clarity as to what appropriate requests are. Furthermore, not all states have the capability or a mutual relationship to respond effectively or in a timely manner. Building capacity to respond to malicious incidents, which requires even more political will to implement, is therefore needed for states to react to appropriate requests for assistance.

Lack of information-sharing and non-reporting of vulnerabilities

The lack of information-sharing among member states and the non-reporting of vulnerabilities are also problems faced in the implementation of the framework on responsible state behaviour. The norms specifically commit states to report cyber vulnerabilities and to share information on remedies available to limit or eliminate potential threats to cyberspace and cyber-dependent infrastructure.

Information sharing is the antithesis of the non-reporting of vulnerabilities. The success of information sharing among states and non-state stakeholders contributes to the framework of responsible state behaviour, especially in cases of malicious activities that are insidious. Relatedly, the non-disclosure of vulnerabilities (having discovered them) detracts from the framework. Sharing information and reporting vulnerabilities is an effort that requires buy-in from different stakeholders.

Weaknesses in the supply chain

Malicious activity is penetrating deeper into the supply chain and targeting the vendors of critical information infrastructure themselves. The norms call on states to take reasonable steps to provide for the integrity of the supply chain so that end users will have confidence in the security of ICT products. They further call on states to prevent the proliferation of malicious ICT tools and techniques and the use of harmful hidden functions. There have also been calls by some states to ensure that operational technology remains secure and free from malicious activity.

Institutional Mechanisms to Enhance Responsible State Behaviour

As mentioned earlier, there is work at the OEWG to further implement and strengthen these norms. Unfortunately, the process to do this at the United Nations takes time whereas time is of the essence in tackling malicious activity in cyberspace.

Two main thrusts can be adopted to achieve responsible state behaviour: working with like-minded states and stakeholders to deal with threats and leaning on regional organisations.

Working with like-minded states and stakeholders

Like-minded states and stakeholders can work together, taking ad-hoc measures, to deal with malicious activity. For example, there is a group of states (including Singapore) that have made ransomware its focus. Many more issues can be dealt with on a cooperative basis, such as securing and strengthening supply chain integrity, and protection of operational technology.

Leaning on regional organisations

Regional organisations like ASEAN can be tapped into to strengthen the framework of responsible state behaviour. Things may move faster with regional organisations especially if there is political will to tackle the problem or to leverage ICTs as critical for development.

Some regional organisations have in fact taken common positions on elements in the framework of responsible state behaviour. These include the African Union taking a common international law position on the use of ICT in cyberspace in January 2024, and ASEAN choosing to be guided by the 11 norms of the framework in 2018.

This is a trend that is likely to continue where groups of states and stakeholders are convinced on the need to adopt a common position on what constitutes responsible behaviour.

Conclusion

Ultimately, the effective countering of malicious activity in cyberspace is contingent on the political will of states, and how they choose to work with each other and with non-state stakeholders. It also depends on how closely they adhere to the agreed framework of responsible state behaviour. The framework may not be perfect, but the principles that underpin it are sound and states and non-state stakeholders will do well to abide by it.

Eugene EG Tan is Associate Research Fellow at the Centre of Excellence for National Security (CENS), a constituent unit of the S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University (NTU), Singapore.

S. Rajaratnam School of International Studies, NTU Singapore
Block S4, Level B3, 50 Nanyang Avenue, Singapore 639798
T: +65 6790 6982 | E: rsispublications@ntu.edu.sg | W: www.rsis.edu.sg