RSIS COMMENTARY

21 July 2025

Strengthening Multilateralism in Cyber and Information Domains

Eugene EG Tan

PONDER THE IMPROBABLE

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

Ponder the Improbable since 1996

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

RSIS COMMENTARY

www.rsis.edu.sg

No. 159 – 21 July 2025

Strengthening Multilateralism in Cyber and Information Domains

By Eugene EG Tan

SYNOPSIS

Multilateral cooperation in cyber and information domains is needed more than ever, especially at a time when geopolitical conflicts threaten to spiral out of control. The civilian sectors and armed forces of countries need to work together to agree on the operational boundaries of the latter and how best to share information and behave responsibly in the cyber and information domains.

COMMENTARY

The multilateral system that has underpinned interaction between states since World War II is under stress from the conflict and competition among states all over the world. The Russia-Ukraine war, the conflict between Israel and Iran, and the escalating rivalry between the United States and China, among other global tensions, have created a hostile environment for consensus-based decision-making among states. This shift towards a might-makes-right approach to international politics is dangerous for those, especially small states, which lack the capability to respond to threats from foreign powers.

However, some threats, including those from the cyber and information domains, do not respect the size or capacity of a state. It may be in the interest of states to cooperate with all stakeholders, including academia, the private sector, civil society, and one another, to ensure the security and stability of operational domains.

Maintaining cyber and information capabilities is costly, and even the best cannot claim immunity from cyber incidents or influence operations. Therefore, multilateralism and the multilateral dialogue mechanism should be strengthened to ensure a safer and more secure cyber domain.

Creation of Cyber Commands in ASEAN and Beyond

Militaries in the region and beyond are increasingly strengthening their capabilities due to the expanding threat landscape and its potential to affect national security adversely. As a result, they are enhancing their capabilities to address the threats emanating from these domains.

However, the lack of accountability regarding the who, what, when, where, and how militaries use these capabilities may destabilise operational domains that are inherently opaque. Having this discussion at a time when militaries in ASEAN are increasingly building their own cyber commands and operational capabilities has important implications for both the military and civilian sectors.

Among the questions that have current implications are: Under what conditions should militaries utilise their cyber and information capabilities; how should states balance their sovereignty with cooperation, especially with the various security partners that ASEAN member states have; how can they enhance their joint operational capabilities in the cyber and information domains; and, what areas should militaries prioritise when developing their cyber and information capabilities across different strategic environments.

The emergence of new technologies, such as artificial intelligence and autonomous systems, has also contributed to the uncertainties among states. Questions regarding the human element in decision-making and leadership considerations in cyber and information operations need to be discussed, with future developments in mind.

Responsible Military Behaviour in the Use of Information and Communication Technologies

These operational capabilities should also adhere to a multilateral framework that has a strong international agreement, as well as input and acceptance from stakeholders, on transparency and information-sharing measures. This will help build confidence among states and create an environment to tackle common cyber and information threats.

The good news is that discussions on responsible state behaviour in the use of information and communication technologies (ICTs) have been ongoing at various levels for a long time, including at the United Nations, ASEAN and other regional organisations. It should continue to address emerging threats or those that have yet to gain consensus.

ASEAN and its partners need to maintain constant dialogue on the norms or frameworks that militaries should adopt to ensure responsible state behaviour in cyberspace and how they will implement them, especially during peacetime competition below the threshold of armed conflict. For example, ASEAN member states have since 2018 pledged to be guided by the norms of responsible state behaviour in the use of ICTs laid out by the UN Group of Governmental Experts in 2015 and have published their Norms Implementation Checklist in February this year. Militaries need to weigh in on how the defence sector will abide by or be guided by these norms.

There is, however, little consensus on how state behaviour should be governed in the information domain, and even less so in military operations involving information. Societies are facing destabilising challenges from foreign influence and misinformation (FIMI) through the spread of false narratives that polarise politics, erode trust in institutions, fuel social unrest, undermine public institutions by manipulating opinions and deepening divisions, and pose serious challenges to security and social cohesion worldwide.

Militaries are taking note of the effects of FIMI and are increasingly playing a larger role in defending against disinformation. However, these actions by military institutions must uphold the principles of transparency, accountability, and public trust. Trust building within societies and with foreign partners is a necessary and fundamental part of information operations, especially when addressing the cognitive and psychological state of individuals in society and how these individuals perceive others outside their own.

Enhancing Information Sharing

The need for confidence-building measures also extends to cyber operations. The third Annual Progress Report of the UN Open-ended Working Group in 2024 had a list of eight voluntary confidence-building measures (CBMs) that states could undertake.

One of these CBMs was for states to share information, such as national ICT concept papers, national strategies, policies, programmes, legislation, and best practices, voluntarily on a bilateral, regional, or multilateral level. Another CBM called for states to share information and best practices on the protection of critical infrastructure (CI) and critical information infrastructure (CII).

As mentioned above, the cost and capability to fend off every cyberattack are astronomical, and states need to cooperate with each other, the private sector, and civil society as a form of self-help. States need to be deliberate in creating platforms where information can be shared in a manner that is comfortable for all parties.

To this end, the 2024 Annual Progress Report also calls on states to consider strengthening public-private partnerships and cooperation to leverage and widen the range of technical capabilities and knowledge to “detect, defend against and respond to ICT incidents”. Militaries need to figure out which modes of collaboration with the private sector have proven most effective in enhancing national and regional cyber resilience, and how they can be adapted across different jurisdictions. The level of information sharing and support provided by the private sector in times of crisis, both domestically and from abroad, is also something that all militaries need to consider.

Building Our Digital Frontiers Together

One thing is clear: As threats and challenges in the cyber and information domains become more common and complex, the potential solutions by militaries and other stakeholders can no longer be unilateral and follow a formula of best practices. A collaborative and multilateral approach that adheres to a commonly accepted framework of state behaviour is probably the best way small states can secure their digital future.

All states and their respective sectors – including the military and the private sector – should engage in dialogue with one another. Over the last decade, ASEAN has established a series of platforms for regional cooperation in cyberspace. ASEAN (and its plus mechanisms) are pivotal platforms for cyber cooperation, particularly in capacity-building and information and knowledge sharing.

In addition to the two centres dedicated to build capacity in the region – the ASEAN-Japan Cyber Capacity Building Centre based in Bangkok and the ASEAN-Singapore Cybersecurity Centre of Excellence based in Singapore – collaborative centres in different sectoral areas have also been set up to deepen collaboration, including the ASEAN Cyber Defence Network, the ADMM Cyber and Information Centre of Excellence (ACICE), and the ASEAN Regional CERT.

ASEAN itself is a confidence-building measure with its coordination role and dialogue mechanisms; what is lacking is the end product where there are actionable outcomes, such as the applicability of international law and addressing state-sponsored malicious cyber activity.

The Digital Defence Symposium, organised by the S. Rajaratnam School of International Studies (RSIS) and ACICE on 22-23 July 2025, is a small step in building information sharing and fostering trust and confidence among states, their private sector partners, and academia. But all journeys of a thousand miles begin with a single step. Now in its third edition, the symposium brings together perspectives from diverse sectors worldwide as a means to share information and enable states to collaborate on building their digital frontiers together.

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.

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