Memorandum No. 34

Council for Security Cooperation in the Asia Pacific (CSCAP) Study Group on International Law and Cyberspace

September 2022

CSCAP MEMORANDUM NO.34
CSCAP Study Group on International Law and Cyberspace

Introduction

Countries in the Asia-Pacific are rapidly digitising at every level of society. The development of a vibrant digital economy holds immense potential for this region. Cybersecurity is critical to the development of a trustworthy and reliable digital economy, and is therefore a key enabler of economic progress and betterment of living standards across the region.[1] ASEAN supports ongoing work to promote practical, voluntary cyber norms of responsible state behaviour development of a rules-based cyberspace, confidence building measures (CBMs) in cyber and relevant application of international law to cyberspace. These discussions constitute efforts that lead to the eventual development of a rules-based cyberspace that undergirds a thriving and trusted digital economy in this region.[2]

ASEAN has made some progress on this issue with the issuing of the ASEAN Leaders' Statement on Cybersecurity Cooperation at the 32nd ASEAN Summit in April 2018 and from the third ASEAN Ministerial Conference on Cybersecurity (AMCC) in September 2018. Even as ASEAN Leaders have tasked relevant Ministers of all ASEAN Member States to make concrete progress on discussions pertaining to the adoption of practical, voluntary norms of State behaviour in cyberspace[3], taking reference from the recommendations set out in the 2015 UNGGE Report, and as the ARF Inter-Sessional Meeting on Security of and in the Use of ICTs consider proposals for robust confidence building measures, there is scope for a CSCAP Study Group to closely consider the vital issue of international law and cyberspace to help make these discussions more holistic and well-rounded for all ARF member states.[4]

Experts and policymakers are occupied with addressing immediate cyber security problems due to the unexpectedly rapid development and proliferation of technology. However, it is fundamentally important to consider the principles of solving cyber security issues. As the ASEAN-led, inclusive and security-oriented Track 2 forum, we believe that CSCAP has a significant role to discuss sharable principles of cyber security and international law based upon multiple existing mechanisms' work on the issue.

Objectives

The study group on International Law and Cyberspace was set up with three main objectives:

1. To consider various perspectives on the application of international law to cyberspace.

[1] CSCAP Russia asks for the term "Cybersecurity" to be replaced by "Security in the use of ICTs".
[2] CSCAP Russia asks for the term "rules-based cyberspace" to be replaced by "open, secure and stable ICT environment".
[3] CSCAP Russia asks for the term "cyberspace" to be replaced by "information space".
[4] CSCAP Russia asks for the term "international law and cyberspace" to be replaced by "security of and in the use of ICTs, and on how international law applies to the use of ICTs".

2. Identify specific areas of focus for ASEAN-led platforms for the discussion of international law.
3. Frame questions for further discussion.

Outcomes and Recommendations

The study group considered the various perspectives of international law and cyberspace including the norms agreed by the UNGGE and the Tallinn Manual that have been put forth on the application of international law to cyberspace, and considered the extent to which these perspectives apply to the regional context.

To this, the study group found that:

- Many cyber incidents can be dealt with by domestic legislation. For example, many forms of cyberattack are actions that breach domestic law in most jurisdictions.
- There is no binding agreement between states on international law for cyber operations. The Tallinn Manual is an academic effort to interpret international law to cyberspace and should not be seen as a prescriptive document.
- The recommendations made by the various United National Group of Governmental Experts (UNGGE) processes are not sources of international law. At the start of the CSCAP study group in February 2019, there was little buy-in for the recommendations of the 2015 UNGGE by states globally. Although the process has global representation, the resulting process is hampered by the need for loose language for consensus. The inability of the 2016/17 UNGGE to come to a consensus was largely because it attempted to address specificities in international law.[5]
- There are fundamental legal challenges to the application of international law in cyberspace. Among these challenges are: definitions over what constitutes a cyberattack or a cyber weapon; if data should be considered an object (and if it there is no effect on data is it against the law); the geographical challenges of neutrality or blockade; the nature of cyberspace (if it is a global commons or a defined international space can be carved out).
- States are still divided about how some concepts in international law applies in cyberspace, including sovereignty. Some states have published their positions on sovereignty without agreement on the concept being a principle or a rule. Most CSCAP member states have not put out positions on the various concepts of international law. The application of international law to cyberspace should be subject to further study as the concepts are updated and evolved.

[5] At the time of finalising the memorandum, the 6th UNGGE and first OEWG have concluded with consensus. Future discussions identified for discussions on international security in cyberspace include fostering common understandings of future threats, strengthening international cooperation and capacity building as well as identifying mechanisms that facilitate engagements for responsible state behaviour.

The study group further identified specific areas of focus for ASEAN-led platforms, considering closely the diverse needs and considerations of this region, and build upon the agreements made by ASEAN member states with regard to the 11 UNGGE norms at the ASEAN Ministerial Conference on Cybersecurity (AMCC).

In the course of the study, the study group focused its efforts on three main areas:

1) international law and participation from the private sector;
2) infrastructure protection and the application of international law and its principles; and,
3) developing a regional and international threshold for the use of force in cyberspace.

With regard to international law and participation from the private sector, the CSCAP study group recommends that:

- As the private sector is a primary driver in cyberspace, and given the State's limited jurisdiction in cyberspace, the private sector can play active roles in norm building. Thus, active involvement by the private sector could influence international norms to transform into international law.
- Future discussion could concentrate on means of reducing total dependence on specific tech companies for regulation.
- There should be international coordination either by a code of conduct or other forms of non-legally binding norms.

With regard to infrastructure protection and the application of international law and its principles, the group recommends that:

- Cyber norms building should start with critical infrastructure. In the group's discussion, there are three categories of critical infrastructure. The first is regional or agreed infrastructure, the second is domestic or infrastructure unique to the country, and the third are shared critical infrastructure such as the ASEAN Power Grid and fibre optic cables.
- The group also recommended using 'breach' instead of a 'cyber attack' for flexibility. An approach for the application of international law and its principles is to enhance penalty according to domestic legislation and yield on international law to prohibit breaches on the critical infrastructures.
- The group recommended that ASEAN Regional Forum should focus on protecting critical infrastructure from breaches and compromise on areas to be covered (whether regional, local or common) to prohibit breaches on these targets.

With regard to developing a regional and international threshold for the use of force in cyberspace, the group recommends that:

- Taking an implementation approach that is predominantly from a closed group of states would amount to fragmentation of international law and states should consider

factors and context on their own to assess definition under Article 2(4) of the UN Charter. The group raised that the use of force should be assessed by scale and effect where factors such as (i) severity, (ii) actual or intended effect (iii) nature of attacker and target and (iv) context can frame the definition.

- States can develop objective standards by providing or agreeing on similar examples that can be measured in the physical and non-physical sphere. For example, a physical effect can be the use of force that results in death and injury of people or damage and destruction of objects while, for non-physical, the examples are significant economic loss, widespread power outage, an attack against critical infrastructure and removal of data.
- The agreement for a definition of the use of force can lead to a future code of conduct for cyberspace.

Frame questions that can facilitate the region's discussion of international law and cyberspace in a way that contributes to and complements separate ongoing discussions at ASEAN-led platforms on norms and confidence building measures

ASEAN currently has several frameworks for cooperation. ASEAN is currently moving from the political commitment to broad principles toward the finding of practical ways forward to operationalise the norms recommended in UN General Assembly resolution 70/237 of 2015, signalling a change in the member states' posture towards the creation of a rules based international order.

The ARF ICT in ISM has a workplan with 14-15 items of which two items are on developing domestic legislation on cyber and on the protection of critical infrastructure.

The AMCC can also be developed into a framework for other cooperative measures. The 2020 AMCC has reiterated their collective commitment to take practical steps to enhance the cybersecurity of the region, in particular, the urgent need to protect national and cross-border Critical Information Infrastructure that serve as the backbone for regional communications trade, transportation, and logistics links. At the same time, Ministers and heads of delegations have also agreed to develop a long-term regional cybersecurity action plan to implement the norms of responsible state behaviour in cyberspace, taking into account the national priorities and cyber capacities of individual ASEAN member states.

Further CSCAP study groups can be formed on how norms of responsible state behaviour in cyberspace can be put into action in collaboration with other members of the ARF.

Refine the existing capacity building programmes being conducted for Asia-Pacific countries, in order to support awareness-raising and facilitate discussions on the application of international law to cyberspace

It was observed that ASEAN has thus far focused on confidence building measures. There are cooperative efforts in cyberspace, for instance those in lieu of the ASEAN power grid. However, ASEAN's response to cyber operations has been limited. The region can be disadvantaged technically which can hamper cooperative efforts. In addition, there is greater room for conversations on government and private sector collaboration in ASEAN. This also raised conversations of regimes where neutral third parties serve as investigation centres.

The study group discussed on increasing ASEAN's capacity to combat cybercrime. The proposals mentioned were the possibility of a Budapest Convention system in ASEAN and a cybercrime cooperation programme. For the former, steps forward can be built by tightening up loose coordination within ASEAN. For the latter, cooperation programmes can look into seeking cyber aid programmes for the improvement of capabilities, support technology and developing a cybercrime repository which would consist of a database on legislation, case-load database and electronic evidence as well as state practice.