Council for Security Cooperation in the Asia Pacific

1st Meeting of the CSCAP Study Group on International Law and Cyberspace

February 26-27, 2019
Singapore

DRAFT PROCEEDINGS

The first CSCAP Study Group Meeting on International Law and Cyberspace in Singapore from 26 to 27 February 2019. This CSCAP Study Group is co-chaired by CSCAP Singapore, CSCAP Malaysia and CSCAP Japan, mirroring the co-chairs of the ASEAN Regional Forum Inter-Sessional Meeting on Security of and in the Use of Information and Communications Technology (ARF ISM-ICT). This Study Group also seeks to build on the work done in 2012 by a prior CSCAP Study Group on Cyber Security.

The meeting was attended by over 20 participants, who included experts from various CSCAP member countries and Singapore-based experts on international law and cyberspace. The CSCAP members present were: Australia, China, European Union, Indonesia, Japan, Malaysia, New Zealand, Philippines, Republic of Korea, Singapore, and Vietnam. The meeting focused on three main questions: (i) why international law matters in cyberspace and what does international law mean for cyberspace; (ii) why/how is international law in cyberspace relevant to ASEAN and ASEAN member states; and (iii) what are the global challenges to implementing international law in cyberspace.

KEYNOTE SPEECH

Air Commodore Bill Boothby (Retd) spoke at length on the sources of international law, how international law can apply to cyberspace, the current global movements in the formation of international law with regard to cyberspace, and the legal challenges to applying international law in cyberspace.

- There have been no global treaties with regard to cyberspace. the Budapest Convention with regard to cybercrime only has 61 parties to the treaty, and has been rejected by Russia and Brazil because it largely takes into account the European view.
- Many cyber incidents can be dealt with by domestic legislation. For example, many forms of cyber attack are actions that breach domestic law in most jurisdictions. However, there is no 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 reports from United National Group of Governmental Experts (UNGGE) process are not sources of international law. The recommendations made by the UNGGE have low buy-in 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.
- There are fundamental legal challenges to the application of international law in cyberspace. Among these challenges are: definitions over what constitutes a cyber attack 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).

- There are differences in views on sovereignty in cyberspace between the USA / EU and China. The Chinese view of how sovereignty can apply in cyberspace may not be wrong if it can demonstrably show how information can be allowed or blocked. China is increasingly becoming a world leader in cyber technology, especially in the area of cyber surveillance – an area where the state is sovereign.

PANEL 1: INTRODUCTION TO INTERNATIONAL LAW IN CYBERSPACE

Xu Longdi (CSCAP China) emphasised the uniqueness of cyberspace and the need for rules in cyberspace.

- States are cooperating on many fronts to work on the rules that apply to cyberspace, especially at the United Nations. The first committee (Disarmament and International Security Committee) is not the only committee at the United Nations looking at international law in cyberspace, with the other committees cooperating at other issues such as online fraud.
- Universal application of international law may not be compatible with regional cyber security situations. Seeking a regional consensus in international law may contribute towards norm formation.
- Pragmatic cooperation can be sought with the private sector. Consultations can take place with other private sector companies like Huawei, Tencent, ABB, and NEC above those who have had a say on international law matters.

Melanie Broder (CSCAP Australia) noted that existing international law is a good starting point to discuss how it applies to cyberspace, and that there is a lot of scope for disagreement. However, the means of delivery – cyber – should not change the understanding of what international law means in cyberspace.

- Seeing how existing international law applies in cyberspace is a good starting point for discussion. There is a lot of ground for disagreement in how international law applies in cyberspace.
- There is nothing inherently special about cyberspace, and the thinking about cyber issues does not need to be special either.
- Existing strategic theory can advise on the development of international law in cyberspace by looking at the potential outcomes of governing state behaviour.

Professor Park Nohyoung (CSCAP Korea) said that an integrated approach is needed to effectively discuss international law in cyberspace. International law in cyberspace also needs to be universal in scope.

- There are many efforts to develop international law at different levels – at intergovernmental, regional, national, private sector and academic levels.
- Processes developing international law do not have to be seen as alternate, competing platforms. Intergovernmental discussions take place at more forums that just the UNGGE, which is constituted under the first committee. The first, second, and third committees all are discussing elements of international law with regard to cyberspace.

- International law can be discussed by international jurists on the 6th committee of the United Nations. There is precedence for this, the 1970 Declaration on Principles of International Law concerning Friendly Relations.

Discussion

Issue: There is a divergence between the Russian/Chinese view and the Western (US/Europe) view on International Law with regard to cyberspace.

There was a call for a specific set of international law to govern the use of cyberspace, citing past precedent that there have been conventions on other types of weapons. There was also a discussion around the Russian and Chinese call for an International Code of Conduct, commenting that the text was actually largely similar to the western position. To this, participants noted that there are serious differences in philosophy between the Russian or Chinese view and the Western (US/Europe) view.

Issue: It is difficult to obtain a common understanding of International Law in cyberspace.

Participants were also not opposed to having a specific set of international law for cyberspace, but the differences between the western (US/Europe) and Russian/Chinese views were too great to have a common understanding on international law. There have been other parallel efforts to develop international law in the other committees of the UN, but most publicity and effort has been concentrated on the first committee and its processes, e.g. the UNGGE and the upcoming Open-ended Working Group.

Issue: There is a need to define what cyberspace means.

There was discussion on what cyberspace actually constitutes and what international law in cyberspace is meant to regulate. Participants had different views of whether cyberspace is purely a technical issue or whether it includes influences the information space as well.

Issue: There is a need to define sovereignty in sources of law or through official documents. In addition, there has to be an in depth discussion on concepts of international law and cyberspace.

There was discussion on the definition of sovereignty and possible sources to define sovereignty. An example was made on possible sources of China's Cyber Sovereignty coming from President Xi Jinping's speeches which articulates several rights of the state, among them are the right to develop ICT, the right to policymaking in ICT, the right to jurisdictions, the right to engage in international cooperation and the right to choose their own development model. There were also discussions which focused on certain concepts of international law and cyberspace such as state responsibility in regards to attribution, responsibilities of a state for non-state actors using their infrastructure or criminal usage of cyberspace.

Issue: The Tallinn Manual is an academic effort, and is not meant to be seen as a definitive document on international law in cyberspace.

There were questions over the continued use of the Tallinn Manual as a reference for international law, saying that it is akin a bible for international law. This view was refuted by participants commenting that the framers of the manual never intended for it to be a bible, but was guided by an academic view of how existing international law could apply in cyberspace. There was also a suggestion that the Tallinn Manual could serve as the starting point of discussions where states discuss the key points of contention in the Tallinn Manual.

PANEL 2: ASEAN PERSPECTIVES ON INTERNATIONAL LAW IN CYBERSPACE

Nguyen Huu Phu (CSCAP Vietnam) spoke about Vietnam's efforts in cyberspace and its perspective on how its cyber laws are compatible with international law.

- Vietnam has identified certain areas of cyber risk that it wishes to address: disinformation threats, attack on critical information infrastructures, cybercrime, the lack of standardised infrastructure, government safety and security, and, the lack of global consensus for a 'clean' cyberspace.
- Vietnam sees international cooperation fulfilling its cybersecurity needs in three major ways: research and analysis of cyber incidents, the prevention of cybercrime, and, ensuring security and safety through international arrangements and treaties.
- ASEAN should endeavour to participate in norms discussion internationally in a meaningful way, in line with the ASEAN Leaders' Statement on Cybersecurity.

Andrew Mantong (CSCAP Indonesia) spoke about Indonesia's experience with regard to cyberspace, and how it has grappled with legislation domestically.

- Indonesia is concerned about issues arising from the development of the internet, including the fourth industrial revolution and freedom of expression. It is not in favour of the information control model proposed by Russia and China.
- Indonesia practices a defensive doctrine in cyberspace. The state does not restrict investment by other states, instead plays a part in facilitating such investment for domestic development. Indonesia emphasises development in its digital economy, cyber awareness, cooperation with other states, the development of civil society, and the development of good cyber norms.
- At a regional level, Indonesia advocates that norms should be developed at a pace comfortable to all states in the region. Norm development should also be done in line with the ASEAN spirit of non-intervention.

Discussion

Issue: There is a need to broaden the conversation on norms to encompass economic growth.

The messaging surrounding norm formation globally has largely been in the language of international security and prohibiting certain state behaviours. The ASEAN Leaders' Vision for a Resilient and Innovative ASEAN and the ASEAN Smart Cities Concept Note suggest that ASEAN is moving towards the use of smart technologies as a growth lever. Likewise, the conversation on norms should be broadened to discuss the economic growth angle, rather than be fixated on international security.

Issue: There is a possibility for regional consensus on International Law in ASEAN.

ASEAN needs to build on its own terms a stable and prosperous cyberspace governed by rules and norms in trust-based environment, and all stakeholders have a role to play in ensuring this. ASEAN should try to find what member states can agree upon, so as to reduce disagreements with each other.

Issue: ASEAN needs to contribute more to the international law discussions with regard to cyberspace.

A participant noted that there is currently no ASEAN input into the interpretation of international law with regard to cyberspace. ASEAN member states should actively participate in the Open-ended Working Group and the UNGGE to make the ASEAN voice heard on the international stage.

PANEL 3: GLOBAL PERSPECTIVES ON INTERNATIONAL LAW IN CYBERSPACE

Ben Creet (CSCAP New Zealand) described governance of the internet as a complex and difficult problem, and there are challenges to formulate and implement international law in cyberspace.

- There are limits to how human rights apply to cyberspace. For example, despite New Zealand placing great importance on the freedom of expression, the New Zealand Harmful Digital Communication Act places certain restrictions on the content that individuals post online.
- Among these challenges is the divide between multilateral and multi-stakeholder approaches to the discussions of international law. Some private corporations have been proactively providing input on interpretations of international law, while some states have steadfastly held on to a view that international law should be done by states.
- Every state should have a doctrine that actively discloses and patches cybersecurity vulnerabilities to ensure the security and stability of cyberspace. Instead, states are exploiting vulnerabilities to get on each other's' networks. This increases the risk of malicious actors exploiting these vulnerabilities to wreak havoc in cyberspace.

Benjamin Ang (CSCAP Singapore) concluded the day's proceedings by questioning participants again what cyberspace and international law means, and identified the challenges to implementing international law.

- There were six challenges identified in the implementation of international law: (1) definition of cyberspace; (2) the concept of sovereignty; (3) the concept of due diligence; (4) the concept of state responsibility; (5) espionage; and (6) what constitutes use of force.
- There were questions raised about the ideological and cultural differences between the 'East' and 'West', and how other stakeholders were involved in the process of framing international law for cyberspace.
- There is also a challenge on how states can regulate non-state actors, who are not covered by international law, but form a large part of the cybersecurity ecosystem.

Discussion

Issue: There needs to be more discussion over the definitions for concepts in International Law.

A participant noted that current discussions were taking place with vague conceptions of what international law means without providing the details. It was suggested that discussions over international law globally should involve more granularity and how these concepts apply to cyberspace.

Issue: There is a need to discuss more about voluntary norms rather than international law.

International law in cyberspace currently deals with issues arising from armed conflict, but the likelihood of cyber warfare is low because most cyber incidents are below the threshold of armed attack. The difficulty of international law discussions mainly lies with its application in peacetime, and not in times of war. It is observed that states are reluctant to be bound by international law in

cyberspace, and that the norms that were agreed at the UNGGE were more closely aligned to confidence and capacity building measures.

Issue: Sovereignty may have been made practicable by Russia.

Russia's announcement to cut off internet connection with the outside world may serve as a template on how the concept of sovereignty can be made practicable. By cutting off internet access to the rest of the world, Russia may be able to claim jurisdiction over what happens within the state.

Issue: Supply chain vulnerabilities are becoming increasingly important in the international law conversation.

It was observed that states have done little to secure supply chains for hardware (security of vulnerable components) and software (security of vulnerable sub-applications). It was suggested that there might be an international process where applications are white listed to address these issues.

PANEL 4: NEXT STEPS IN STUDYING INTERNATIONAL LAW FOR CYBERSPACE

Farlina Said (CSCAP Malaysia) recapped the issues that transpired over the course of the study group, and laid out the potential areas for discussion for the next study group.

- The discussions regarding international law in cyberspace often does not address threats on the ground. There should be further discussion over how international law governing Information and Communication Technologies can be applied to such threats.
- There are some salient critiques over the processes used to frame international law. First, there was criticism over processes like the UNGGE not being fully representative, and there are states that were not involved in the process. Second, there may be a prevailing bloc mentality over the discussions of international law for cyberspace that pits those interested to apply existing sets of international law to cyberspace against those who wish to write new laws. Third, not all states are equipped to deal with international law, especially developing countries that are more concerned with domestic circumstances.
- There is work to be done on the discourse around international law in cyberspace. This work involves the development of a common lexicon, mapping out the concerns from states and approaches to international law, and identifying the priority areas where international law should be addressed.

Patryk Pawlak, Joanna Kulesza, and Francois Delarue (CSCAP EU) presented a paper on the applicability of international law in cyberspace, outlining the avenues for future cooperation in advancing international law.

- International law in cyberspace is increasingly becoming an important issue for the European Union. Only a few states were interested in the topic of international law in cyberspace when it was first mooted, but this has changed. The appointment of an EU Cyber Ambassador signals the involvement of all EU member states, and the importance placed on the issue of international law. The EU aims to push the conversation in a pragmatic manner, and is concerned mainly at securing the future of a free, open, and secure Internet.
- While there are different interpretations of international law, states generally agree that international law is relevant. However, international law is not a panacea for all cyber issues. There are no collective countermeasures that states can take to address cyber issues.

- The EU proposes three ways to advance the conversation on the applicability of international law to cyberspace: (1) the creation of a transparency framework for states to publically disclose their approach regarding the application of international law applicable to cyberspace; (2) build legal capacity among states to build stability in cyberspace by reducing overreactions from states, improving understanding of existing obligations and commitments, and improve a state's capacity to formulate a more effective response; and, (3) to map and share states' best practices and lessons to contribute toward the application of international law.

FUTURE EVENTS AND NEXT STEPS

The co-chairs of the CSCAP Study Group on International Law and Cyberspace agreed that the second meeting of the study group will be hosted by CSCAP Malaysia in Malaysia later this year.

The study group agreed to garner views from all CSCAP members on the six areas - (1) definition of cyberspace; (2) the concept of sovereignty; (3) the concept of due diligence; (4) the concept of state responsibility; (5) espionage; and (6) what constitutes use of force - identified by the study group.

The inputs from various CSCAP member committees will be submitted to CSCAP Malaysia for compilation in preparation for the second study group meeting. The compiled inputs will serve as the basis for discussion at the second study group meeting.