Asia-Pacific and Views on the Resurrected UN Norms Process

MODERATOR: Bart Hogeveen
International Cyber Policy Centre
Australian Strategic Policy Institute
@BartHoogeveen @ASPI_ICPC

PANELISTS:

Grata Endah Werdaningtyas
Director of International Security and Disarmament, Indonesia Ministry of Foreign Affairs

David Koh
Chief Executive, Cyber Security Agency of Singapore

Johanna Weaver
Special Adviser to Australia’s Ambassador for Cyber Affairs, Australian Department of Foreign Affairs and Trade
Cyber Operations Tracker

The Digital and Cyberspace Policy program’s cyber operations tracker is a database of the publicly known state-sponsored incidents that have occurred since 2005. Know of an incident not listed in the tracker? Report it to us.
Developments in ICTs in the context of international security in Asia-Pacific

2019
- **Australia**: a sophisticated state actor breached the Australian parliament’s computer network and those of major political parties.

2019
- **Indonesia**: election committee alleges hacking attempts at voters’ database originating from Russian and Chinese IP addresses.

2019
- **Tonga**: cut in submarine cable forces Island country to fall back on satellite comms.

2018
- **Singapore**: sophisticated and well-planned hackers steal patient records from SingHealth, incl. those of the Prime Minister.

2018
- **Cambodia**: Chinese cyber espionage infiltrating government and media in advance of national election.

2019
- **Indonesia**: election committee alleges hacking attempts at voters’ database originating from Russian and Chinese IP addresses.

2018
- **ASEAN**: targeted phishing campaign by known APT using ASEAN official documents as pretext.

2018
- **Philippines**: Within hours of PCA advice on South China Sea, 68 government agencies suffer massive DDoS attack.

2014
- **Vietnam**: spear phishing campaign against government and military agencies, likely a network of intel agency was compromised.

2012
- **Philippines**: defacing campaign against academic and media outlets attempting to frustrate Being-Manilla talks.
No “international cyber arbiter”

- United Nations Security Council
- International Court of Justice
a common playbook ... 

... rules of the road 

NORMS, RULES AND PRINCIPLES FOR RESPONSIBLE BEHAVIOUR OF STATES
• Since 2004: five consecutive groups of governmental experts

• Developments in the field of ICT in the context of international security

• “[a] dramatic increase in incidents involving the malicious use of ICTs by State and non-State actors.”

→ Risks for all States, and may harm international peace and security

→ Certain States are developing military capabilities; use of ICT in future conflicts between States more likely
19. International law, and in particular the Charter of the United Nations, is applicable and is essential to maintaining peace and stability and promoting an open, secure, peaceful and accessible ICT environment.
2015 report

- 11 norms of responsible state behaviour in cyberspace
- Set of confidence-building measures
- Consideration of how international law applies
2 CONSIDER ALL RELEVANT INFORMATION
adopting and implementing, AMCC participants agreed to subscribe in-principle to the 11 voluntary, non-binding norms recommended in the 2015 Report of the United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), as well as to focus on regional capacity-building in implementing these norms.
First Committee Approves 27 Texts, Including 2 Proposing New Groups to Develop Rules for States on Responsible Cyberspace Conduct

Concluding its programme of work, the First Committee (Disarmament and International Security) today approved 27 draft resolutions and decisions, including two separate proposals to create working groups within the disarmament machinery to develop rules for States on responsible behaviour in cyberspace.

“Disarmament and international security are in your hands and your actions as Member States result in consequences which we must all face,” said Ion Jinga (Romania), Chair of the Committee, in his closing remarks. “The manner in which you approach the Committee is the way in which it can help us all reach our common goals.”
Cyber diplomacy agenda for 2019-2021

- Two United Nations cyber initiatives:
  - open-ended working group (OEWG)
  - group of governmental experts (UNGGE)

(... “to study, with a view to promoting common understandings and effective implementation, possible cooperative measures to address existing and potential threats in the sphere of information security (...”)
Asia-Pacific and Views on the Resurrected UN Norms Process
Kick off question

How would you assess the current international climate related to cyber/ICT security in the context of international/regional peace and security?

- **Peaceful**: states are working together on solutions to common challenges stemming from cyberspace
- **Contentious**: the political situation is tense, and states are more adversarial
- **Mixed**: while the political situation is tense, common solutions are nevertheless
- **Pre-crisis**: co-operation is breaking down, leading to unmanageable levels of distrust on cyber issues;
- **Crisis**: an international conflict stemming from the use of ICTs is a likely scenario.
Asia-Pacific and Views on the Resurrected UN Norms Process