CSCAP General Conference

Session 4
Building a Secure and Open Cyberspace through Cooperation

Elaine Korzak
Cybersecurity Fellow
Center for International Security and Cooperation
Stanford University

Focus

Significance of norms (in particular international law) for building a secure and open cyberspace through cooperation

“In the place of today´s cyber free-for-all, we need understood rules of the road …. Behaviour that is unacceptable offline is also unacceptable online, whether it is carried out by individuals or by governments.”

UK Foreign Secretary William Hague at
the London Conference on Cyberspace 2011

"It is of great significance that the common challenges in the sphere of information security should be dealt with through international cooperation … with the aim of achieving the earliest possible consensus on international norms and rules guiding the behaviour of States in the information space."

"To that end, China, Russia, Tajikistan and Uzbekistan have jointly elaborated … an international code of conduct for information security …"

Letter from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the UN Secretary-General, 12 September 2011 (A/66/359)

Argument

There is consensus on the need for norms in cyberspace

"Rules of the Road"

But the challenge is to agree on the type and content of norms

International law: existing norms, new norms, mix?

Key development in 2013: UN GGE Report

Norms

- Norms: Shared expectations of how individuals or organisations will act; In other words standards of behavior

- facilitate cooperation

- different shapes and forms (formal/informal, binding/non-binding, etc)

Norms in Cyberspace

- Examples of ongoing initiatives and processes
  - United Nations
  - ITU
  - London Process
  - European Union
  - Shanghai Cooperation Organization
  - OSCE

+ civil society
+ business (including technical communities)

- Plethora of activities

- regional vs global?

Developments in the UN – 1st COM of GA

- Since 1998 UN GA Resolution “Developments in the field of information and telecommunications in the context of international security” (A/RES/53/70)
- Three Groups of Governmental Experts (GGE)

- Most recent GGE 2012/2013:

15 Member States (Argentina, Australia [Chair], Belarus, Canada, China, Egypt, Estonia, France, Germany, India, Indonesia, Japan, Russia, UK, USA)

2013 GGE Report

- **Mandate:**

"… to study existing and potential threats in the sphere of information security and possible cooperative measures to address them, including norms, rules or principles of responsible behaviour of States and confidence-building measures with regard to information space …"
(A/RES/66/24)

2013 GGE Report

- **Key recommendations:**

Para 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.

Para 20: State sovereignty and international norms and principles that flow from sovereignty apply to State conduct of ICT-related activities, and to their jurisdiction over ICT infrastructure within their territory.

Para 21: State efforts to address the security of ICTs must go hand-in-hand with respect for human rights and fundamental freedoms set forth in the Universal Declaration of Human Rights and other international instruments.

Recognition of existing legal frameworks
= significant development

What´s next?

- New GGE for 2014/2015; mandate to elaborate how exactly international law applies to states´ use

Moving forward:

- Don’t backtrack on commitment made – applicability of international law is starting point
- Next step: application of particular norms
- Importance of track 2 discussions – Tallinn Manual as exampleAmend existing law rather than replace it wholesale
- Danger of fragmentation