ASEAN: International Law on Cybersecurity

Kriangsak Kittichaisaree

Centre for International Law/ NUS

August 2018

Chairman's Statement of the 32nd ASEAN Summit, Singapore, 28 April 2018

ASEAN Political-Security Community

6. To identify a concrete list of voluntary, practical norms of State behavior in cyberspace for ASEAN to adopt & implement, and to strengthen cooperation on personal data protection in cyberspace

ASEAN Leaders' Statement on Cybersecurity Cooperation

- **Int'l law, esp. UN Charter, applies and is essential to maintaining peace & stability & promoting an open, secure, stable, accessible and peaceful ICT environment;**
- **State sovereignty & consequential int'l norms and principles apply to ICT-related activities;**
- **Entrust relevant Ministers etc. to identify a concrete list of voluntary, practical norms of State behavior in cyberspace for ASEAN to adopt and implement, taking reference from the voluntary norms recommended in UNGGE's 2015 report.**

UN GGE

Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security

UN GGE

Memberships fluctuated from year to year

- **15 in 2004 – 2013**
- **20 in 2014/15 (with Malaysia)**
- **25 in 2016/17 (with P5/UNSC + India, Indonesia, Japan and ROK, etc.)**

2 reports in 2013 and 2015

2013 Report

- **International law applies in cyberspace.**

  UN Charter, sovereignty, jurisdiction over ICT infrastructure within State territory, non-intervention in the internal affairs of other States

2015 Report

- **11 voluntary, non-binding norms of responsible State behavior**

(a)To coop. to increase stability & security in the use of ICTs and to prevent harmful ICT practices;

(b)To consider all relevant info in case of ICT incidents;

(c)To not knowingly allow one's territory to be used for IWA using ICTs;

(d)To increase exchange of info and assistance to prosecute terrorist and criminal use of ICTs;

(e)To respect human rights and fundamental freedoms;

(f)To not conduct or knowingly support ICT activity contrary to int'l law obligations;

2015 Report (cont.)

(g) To protect critical infrastructure from ICT threats;

(h) To assist another State whose critical infrastructure is subject to malicious ICT acts

(i) To prevent the proliferation of malicious ICT tools and techniques;

(j) To report ICT vulnerabilities and share associated info on available remedies

(k) To not conduct of knowingly support activity to harm the info systems of CERTs

2015 Report (cont.)

- Private sector and civil society should self-regulate and self-police.
- CBMs to increase int'l coop and reduce risk of conflict
- Private sector, academia, and civil society could play important roles in supporting States.
- Capacity building is essential for int'l cooperation.
- Additional norms could be developed over time.

UNGA Resolution 237 (Dec 2015)

UN Member States to "be guided in their use of information and communications technologies by the [UN GGE's] 2015 Report.

2017 (no) Report

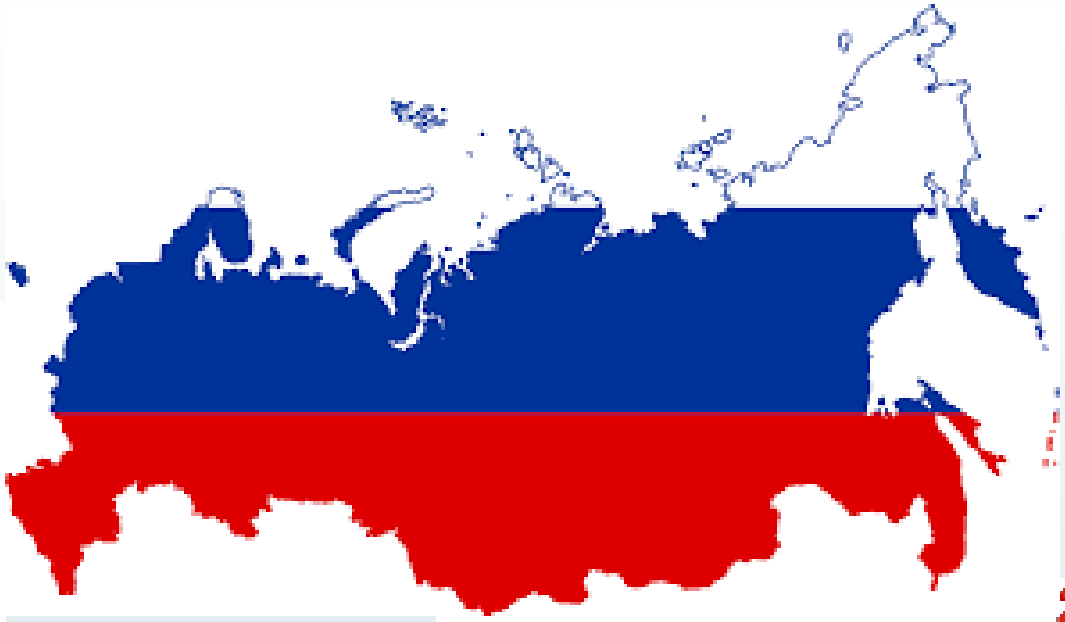
- **Failed to submit its 3rd report due to deadlock**

  - No real desire to compromise?

  - Countries are divided by their existing or potential capacity to utilize ICTs.

  - The dividing lines were mostly political and hardly legal.

Key Players



USA

- Fundamental freedoms of expression and association
- Respect for intellectual property rights
- Protection from arbitrary or unlawful interference with Internet users' privacy
- Protection from cybercrimes
- Inherent right to self-defence consistent with the UN Charter

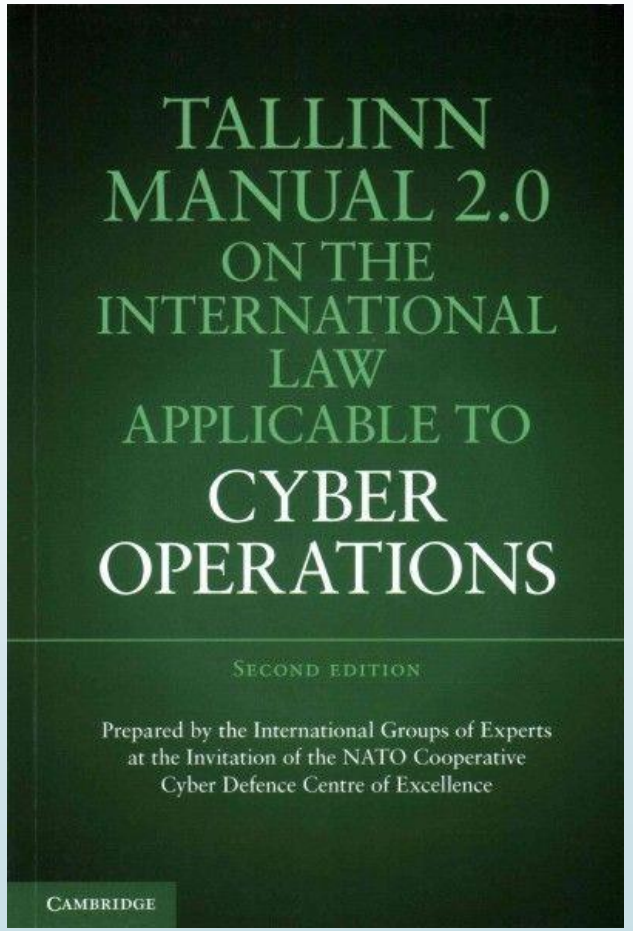
China

- Universal respect of ‘national cyber sovereignty’
- International law to regulate transnational cybercrimes
- Internet freedom and regulation to balance between “cyber sovereignty” and “cyber freedom”

Russia

- *Cyber warfare is part of "information warfare"*
- **Cf. US and most NATO Member States' military doctrine –** ***cyber warfare is a subset of information operations/warfare***

Tallinn Manual 2.0



Tallinn Manual

- **By int'l law experts chosen by NATO Cooperative Cyber Defense Center of Excellence**
- **Meant to state the law as it existed in June 2016**
- **4 parts:** (1) general int'l law & cyberspace
  (2) specialized regimes of int'l law & cyberspace
  (3) int'l peace and security & cyber activities
  (4) law of cyber armed conflict

Sovereignty

- **“The Principle of Sovereignty applies in cyberspace.”**
- **“A State must not conduct cyber operations that violate the sovereignty of another State.”** (e.g. an agent using USB drive to introduce malware into cyber infrastructure in another State)
- **But, cyber espionage : passive v. offensive intelligence gathering activity; govt v. industrial/commercial targets**
- **Peace time cyber espionage not *per se* regulated by IL**

Due Diligence

- "A State must exercise due diligence in not allowing its territory, or territory or cyber infrastructure under its govt. control, to be used for cyber operations that affect the rights of, and produce serious adverse consequences for, other States."
- The State must have actual or constructive knowledge of the harm.
- Where a State knows of the transboundary harm, it must take "all measures that are feasible in the circumstances to put an end to the cyber operations."
- Cf. UN GGE : States "should" exercise due diligence.

Jurisdiction

- **Sometimes unclear in which State data or other digital evidence resides.**
- **Territorial jurisdiction** e.g. E-data widely available on the internet, but hosted on servers in another State
- **Extraterritorial enforcement jurisdiction** e.g. Data accessible via the internet but not intended to be available to individuals in the concerned State

Non-Intervention

- Banning intervention involving ‘coercion’ by cyber means in internal/external affairs of another State
- “The premises of a diplomatic mission or consular post may not be used to engage in cyber activities that are incompatible with diplomatic or consular functions.”
- Diplomatic agents/consular officials may not engage in cyber activities that interfere in the internal affairs of the receiving State or are incompatible with the laws.”
- Conducting cyber espionage by diplomatic/consular missions would not be allowed.

Law of Int'l Responsibility

- **The most difficult legal questions re: attribution = non-State actors working as proxies for a State or in some way on behalf of a State w/o clear legal authority**
- **"Effective control"**
- **Aiding and assisting**
- **Countermeasures are only available against States.**
- **Cyber countermeasures -** need not target the specific organ of the State/ can be used to respond to a non-cyber violation

Cyberwarfare

US and NATO

- **Whether cyberattack = use of force (Art 2(4) UN Charter) depends on test of 'scale and effect' [of physical damage, not mere economic loss] giving rise to countermeasures or, if = 'armed attack', self-defence under Art 51 UN Charter.**
- **If 'armed conflict', then no longer law enforcement matters but IHL / law of armed conflict applies.**

Cyberwarfare (cont.)

Russia, China and others:

- **Problems regarding attribution + high burden of proof of 'clear and compelling' evidence, not mere 'speculation'**
- **Different attribution standards by intelligence agencies *v.* law enforcement agencies?**
- **Cyberattack is better subject to domestic law enforcement, not UN law or IHL/LOAC.**

Cyber terrorism

- 2010 Beijing Convention & Protocol on aviation security = 1st to specifically mention perpetration by "any technological means" to commit terrorist acts.
- Yet the other existing sectoral conventions can also be interpreted to suppress cyber terrorism in various ways.
- But 1963 Tokyo Convention allows inaction regarding offences of a political nature, while the other conventions/protocols up to 1997 are silent on the "political exception".

Cyber terrorism (cont.)

- 1997 Terrorist Bombing Convention & subsequent conventions: proscribed criminal acts ‘are under no circumstances justifiable by considerations of a political, philosophical, ideological, racial, ethnic, religious or other similar nature …’
- Beijing Protocol (Sep 2010) amending 1970 Hague Convention: offences not to be considered as ‘political offences’

Cybercrimes

2001 Council of Europe's Budapest Convention on Cybercrime

58 State Parties =

➨ **All CoE members** except Russia, Ireland, San Marino, and Sweden; plus

➨**15 non-CoE Members:** Australia, Canada, Chile, Costa Rica, Dominican Republic, **Israel, Japan,** Mauritius, Panama, **Philippines**, Senegal, **Sri Lanka, Tonga,** USA, and, as of 1 Oct 2018, Argentina

Cybercrimes (cont.)

- **Russia and China oppose** Budapest Convention, esp. Art. 32(b) allowing transborder access to stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the **person** who has the lawful authority to disclose the data to the Party through that computer system.
- **ROK : Budapest Convention is already out of date.**

Russia' Draft UN Convention on Cooperation in Combating Information Crimes

- Emphasizes territorial sovereignty
- Territorial jurisdiction of States
- Non-intervention in the domestic affairs of other States

List of offences under Budapest Convention

- **Offences against the confidentiality, integrity and availability of computer data and systems:** illegal access, illegal interception, data interference, system interference, and misuse of devices
- **Computer-related offences:** forgery, fraud
- **Content-related offences:** child pornography
- **Offences related to infringements of copyrights and related rights**

List of offences under Russian Draft Convention

Similar to Budapest Convention, but more detailed + novelty

- Unauthorized impact on data: intentional unauthorized copying of electronic information
- Offences related to **State secret** protected by domestic law
- **Use of ICT to commit acts established as offences by the int'l law** as provided in conventions against terrorism, corruption, drug trafficking, transnational organized crimes.
- **Preparation** for committing an offence is punishable.

List of offences under Russian Draft (cont.)

- Transfer of criminal proceedings for purposes of criminal prosecution in the interests of the proper administration of justice, esp where several jurisdictions are involved to ensure combining of criminal cases.
- Conference of State Parties to improve the capacity & coop & to promote and review the implementation
- Int'l Technical Commission on Combating ICT Crime (ITC)

  - Permanent body, to assist the States in reviewing the implementation of the Convention.

  - 23 members elected for a 5-year term and may be re-elected, 2/3 of whom elected by the Conference+1/3 by the governing bodies of the ITU.

  - Experts in diplomacy, int'l law, communication technologies or relevant research developments.

Tallinn 2.0: Int'l Human Rights Law

- **Right to privacy " encompasses the confidentiality of communications."**
- **"The obligations to respect and protect int'l human rights,** with the exception of absolute rights**, remain subject to certain limitations that are necessary to achieve a legitimate purpose, non-discriminatory, and authorized by law."**
- **States may also derogate from certain human rights obligations** if provided by the specific provisions of the applicable treaty**.**

Privacy, freedom of expression/speech v. law and order

- **1966 Int'l Covenant on Civil and Political Rights (ICCPR)**

117 State Parties (in ASEAN: Brunei, Malaysia, Myanmar & Singapore not party)

Q: What is the universal standard?

ICCPR *Article 19*

Right to hold opinions + freedom of expression subject to restrictions provided by law and necessary:

(a) For respect of the rights or reputations of others;

(b)For the protection of national security/public order/public health or morals.

ICCPR *Article 20*

Prohibiting by law:

- Any propaganda for war or advocacy or national, racial or religious hatred that constitutes

  - incitement to discrimination, hostility or violence.

Similar provisions in Article 12, American Convention on Human Rights

Article 10 European Convention on Human Rights

➨ restrictions prescribed by law and necessary in a democratic society

European Charter on Human Rights' jurisprudence: 3-part cumulative test: legality; legitimacy; necessary & proportionate in a democratic society (meeting a 'pressing social need')

- PLUS 'margin of appreciation' to the government.

African Charter on Human & Peoples' Rights: no comparable yardstick re the restrictions

Q: Punishing online services providers?

Cyber terrorism and freedom of speech/expression

- **European Court of Human Rights in *Leroy v France* and *Sürek v Turkey (No 3)***
- **S. 21 UK Terrorism Act 2000 and *Anjem Choudary* case**
- **S. 23(c)(1) US Communications Decency Act 1996 and *Twitter***

The Americas

- **The OAS adopted 12 principles in the Statement of Principles for Privacy and Personal Data Protection in the Americas** (31 March 2015).

  i.e., lawful and fair purposes; clarity and consent; relevant and necessary; limited use and retention; duty of confidentiality; protection and security; accuracy of data; access and correction; sensitive personal data; accountability; trans-border flow of data and accountability; and disclosing exceptions

Africa

- **The AU started drafting a *Convention on the confidence and security in cyberspace* to establish a legal framework for cybersecurity in Africa** through organization of e-transactions, protection of personal data, promotion of cybersecurity, e-governance, and combating cybercrime (2011).
- **The AU adopted the *African Union Convention on Cyber Security and Personal Data Protection*** (27 June 2014).

AIs

Individual criminal responsibility

- **AIs making soldiers wage cyber war against a remote target according to AIs' programmed judgement**
- **The cyber warrior = a *de facto* 'humanoid robot' who cannot (?) be reasonably held responsible for his action.**
- **Cf. US Military Tribunal/Nuremberg in *Einsatzgruppen*: a soldier is not an automaton, but a reasoning agent who is bound only to obey the lawful orders.**

AIs (cont.)

State responsibility for lethal AIs (LAIs): *Lex lata =? De lege ferenda =?*

- **GGE on Lethal Autonomous Weapons (LAWS), 1st meeting in Nov 2017, under Convention on Certain Conventional Weapons (CCW) 'to explore and agree on possible recommendations on options related to emerging technologies in the area of LAWS'.**
- **GGE: IHL applies to all weapons, & responsibility for their deployment remains with States.**
- **Yet, still need to evaluate the relevant substantive & procedural IHL provisions and the issue of accountability in practice.**

Internet of Things (IoTs)

- To be ‘ethically designed’ for users’ wider control over personal data/IoT services by choosing specific sets of principles/rules within a digital architecture/device.
- Such ‘technological normativity’ = socio-techno arrangements, as in the case of a speed limit system built in a car.
- Interaction between private sector & government to ensure technologies neither violate law nor the State’s int’l legal obligations, esp. human rights.

Cryptocurrencies

- **Since March 2014, US Inland Revenue Service (IRS): convertible virtual currency = property for US deferral tax purposes.**
- **Thus, its theft = a crime under US law, and proscribed by Art 7 and/or Art 8 of the Budapest Convention.**
- **Cf *RuneScape* (Dutch Supreme Court 31 Jan 2012):** Although the online game's publisher owns the online game and licensed it to players to play the game, its property value was like other intangible goods (e.g. electricity) which could be stolen from licensee who did not own it.

Net Neutrality

➨ **Early 2015, US Federal Communications Commission (FCC) adopted the new rules on 'network neutrality' for US Government and ISPs:**

- equal treatment to data in the Internet without discrimination between different packets or data, e.g. by charging differentially by user, content, site, application, mode of communication

➨ **In light of US global dominance in cyberspace, what if network neutrality ends??**