Kobe and QM Symposium on International Law
"Diversity of Transnational Criminal Justice"

“Harmful Interference into Satellite Telecommunications by Cyber-Attack”

10 April 2015

Yuri Takaya
Research Fellow/Lecturer, Kobe University

Outline

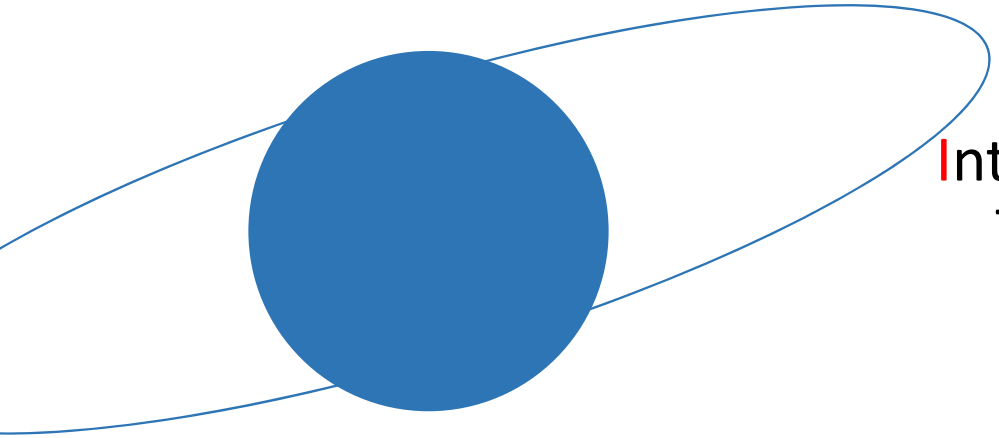
Introduction

1. Computer Network Attacks (CNAs) in LOAC
2. “Harmful Interference” in Space Law
3. ITU’s Initiative to Criminalize CNAs

Conclusion

Introduction: ITU and GEO

◆Geostationary Orbit (GEO): about 36,000 km altitude mainly used for
telecommunication satellite
meteorological satellite



International Telecommunication Union: ITU
The oldest UN specialized organization
in charge of allocating frequencies.

→ how the role of ITU falls into the scope of cyber attack?

Introduction: Terminology

◆In the Law of Armed Conflict

Cyber Attack — Computer Network Attacks (CNAs)

"[A]ctions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves.

US Department of Defense, Dictionary of Military and Associate Terms 08 November 2010 amended in 2014

(excluding: jamming, cyber crime, electromagnetic pulse, radar)

◆CNAs in Space Law → falls in the scope of Space Security

sustainable uses of outer space for peaceful purposes

no intentional / deliberate / harmful destruction or interference

◆CNAs in ITU Law → falls in the scope of Cybersecurity

How does ITU criminalize CNAs to satellite communication?

Introduction: Threat to Satellite Telecommunication in GEO

◆Not Anti-Satellite Test in outer space

2001 US decided to withdraw from Anti-Ballistic Missile Treaty of 1972

to restart Missile Defense test in outer space

(after September 11)

2007 China demonstrated military operation in outer space of hitting its own satellite by its own rocket

◆ But Harmful Interference

95-97%	Human Errors, Hardware Problems
3-5%	Intentionally Caused

◆Most of space systems are highly dependent on computer network systems

→vulnerable to harmful / intentional interference by Computer Network Attacks

1. Computer Network Attacks (CNAs) in LOAC

1. CNAs in the Law of Armed Conflict: Studies in 1999

◆US: 1999 Naval War College's Symposium on
"Computer Network Attack and International Law"

→The following questions were asked in the context of *jus ad bellum* "Legality of CNAs"

"Does CNA violate the prohibition on the use of force found in Article 2(4) of UN Charter, and, if so, when?

"Can it fall within one of two exceptions to that proscription – use pursuant to Security Council authorization in accordance with Chapter VII of the UN Charter and use in self-defense, based either on Charter Article 51 or the customary right thereto?"

"If a State conducts a CNA against another State, can the target respond with classic kinetic force? If so, under what circumstances?"

1. CNAs in the Law of Armed Conflict: Studies in 1999

Questions in the context of *jus in bello*

"When does the law of armed conflict (LOAC) apply to CNA operations?"

"Is it implicated in all cases of CNA or do some fall outside its purview?

"Does it present difficulties for the application of core LOAC principles like discrimination and proportionality or pose particular risks to protected persons and objects?"

"Do lacunae exist in a normative architecture intended to shield non-participants from the effects of conflict?"

"Might CNAs, by contrast, offer possibilities for enhancing their protection?"

1. CNAs in the Law of Armed Conflict: Cases

◆2007 Estonia

Distributed Denial of Service (DDoS) attack

◆ 2007 Syria

Disable the Warning System of an Air Defense Network

◆ 2010 Iran

Stuxnet worm attacked Nuclear Facilities in Iran

1. CNAs in the Law of Armed Conflict: Development of National Policies against CNAs

◆The definition of "cyber attack":

UK: 2010 National Security Strategy

one of four "Tier One" threats to British national security

(the others: international terrorism, international military crises between States, a major accident or national hazard)

2011 Cyber Security Strategy: Protecting and Promoting the UK in a Digitized World

US: 2010 National Security Strategy

"one of the most serious national security, public safety, and economic challenges we face as a nation"

US DOD 2011 Strategy for Operating in Cyberspace

designates cyberspace as an operational domain

US established US Cyber Command to conduct cyber operations

1. CNAs in the Law of Armed Conflict: Development of National Policies against CNAs

Canada: 2010 Canada's Cyber Security Strategy

Russia: Conceptual Views Regarding the Activities of the Armed Forces of the Russian Federation in Information Space

NATO: 2010 Strategic Concept

acknowledging the new threat

committing itself to "develop further our ability to prevent, detect,

defend against and recover from cyber attacks, including by using the NATO planning process to enhance and coordinate national cyber-defence capabilities, bringing all NATO bodies under centralized cyber protection, and better integrating NATO cyber awareness, warning and response with member nations"

1. CNAs in the Law of Armed Conflict: Obstacles to Applying LOAC to CNA

Due to the nature of CNAs……

- ✓not recognized as "force" in Art. 2 (4)of the UN Charter
- ✓Intangibility of target and weapons
- ✓lack of clarification on "when" CNA starts
- ✓IP address is not necessarily a proof
- ✓difficult to identify whether or not CNA is launched by civilians

1. CNAs in the Law of Armed Conflict:
Possible Damage by CNA to Satellite Communications

◆the definition of “CNAs to Satellite Communication” by YURI

“to cause harmful interference to satellite radiocommunication

by sending a malicious code (or virus) to satellite operation systems”

◆Possible Damage

Direct Damage = dysfunction of satellite operating systems (i.e. by DDoS)

Indirect Damage = unauthorized manipulation of communication satellite to endanger other states’ outer space activities

2. “Harmful Interference” in Space Law

2. “Harmful Interference” in Space Law

◆Definition of “harmful interference” in ITU Law is to endanger the functioning of a radionavigation and radiocommunication service

→ related provisions in the Outer Space Treaty of 1967

Article I: “Outer space is the Province of all Mankind”

Any state has the right for free use, exploration of, access to OS

Article III: Application of International Law

Article IV: Exclusively Peaceful Uses of Celestial Bodies

(x Test of Any Kind of Weapons on Celestial Bodies)

Article XI: Appropriate Consultation for Potential Harmful Interference

2. Harmful Interference in Space Law: Outer Space Treaty of 1967

intentional / harmful interference to space activities is not substantially covered by the Outer Space Treaty of 1967 because…

- ✓ Article III allows the possible interference
  in the case of self-defense or collective security
- ✓ Article IV (2) leaves the definition "peaceful" vague
  US "non-aggressive"
  Russia "non-military"
  Japan between "non-aggressive" and "non-military"
- ✓ principles do not reach non-state actor to prohibit harmful interference

2. Harmful Interference in Space Law: Outer Space Treaty of 1967

Art. 6: State Responsibility

States are responsible for its national space activities

Nationals needs to obtain authorization and supervision from their states

Art. 7: State Liability

States are absolutely liable for the damage cause on the surface of the Earth and the airplane in flight

→CNAs by non-state actor is out of scope

→CNAs for non-ground-damage is out of scope

2. Harmful Interference in Space Law: TCBMs

◆ UNGA Resolution 2005-

"Transparency and Confidence-Building Measures in Outer Space Activities"

2005 Russia's proposal (China supports: joint draft for PPWT)

2007 EU initiated to propose Code of Conduct for Outer Space Activities as TCBMs

(Space Debris Guidelines are not included in terms of CNAs)

◆ 2013 Report of Governmental Group of Experts (GGE)

Benefits from TCBMs:

✓Due to technical limit in tracing the original point

✓"where", "when", and "by whom" CNA is launched

✓the clarification of state' intent in advance through TCBMs

✓helps to prove who is the real victim, considering unauthorized manipulation

2. Harmful Interference in Space Law: EU Initiative 2013 Code of Conduct for Outer Space Activities

- ✓no harmful interference in the freedom for outer space activities (para 25)
- ✓the responsibility of states to cooperate in good faith to avoid harmful interference with outer space activities (para 27)
- ✓space debris mitigation to minimize the risk of harmful interference (para 49)
- ✓ITU regulation on addressing harmful radio-frequency interference (para 53)
- ✓information on space policies and procedures to prevent and minimize harmful interference (para 75)
- ✓consultation mechanisms to prevent or minimize harmful interference (para 82)

3. ITU’s Initiative to Criminalize CNAs

3. ITU's Initiatives to Criminalize CNAs

the sovereign right of each state to "regulate" its telecommunication

in the preamble of ITU Constitution and Convention

ITU Law works by National Legislation

※ITU Law: ITU Constitution and Convention + Administrative Regulations (i.e. Radio Regulations)

3. ITU's Initiatives to Criminalize CNAs: Definition of Harmful Interference

ITU Radio Regulations, Section VII- Frequency Sharing

- 1.166 "*interference*"

"[T]he effect of unwanted energy due to one or combination of emission, radiations upon reception in a *radiocommunication* system"

- 1.169 "*harmful interference*"

"[I]nterference which endangers the functioning of a radionavigation service or of other safety services […] seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service […]

3. ITU's Initiatives to Criminalize CNAs:
Protection of Frequency from Harmful Interference

◆The Scope of ITU Work

✓ Legal issues in International Communication Technologies (ICTs)

(digital broadcasting, the Internet, mobile technologies and 3D TV)

◆ How to protect frequencies from harmful interference

✓ Art. 11 of Radio Regulation (RR):

Master International Frequency Register (MIFR) (=Master Register)

→ enhance "international recognition" of radio assignment
→provide protection from harmful interference

3. ITU's Initiatives to Criminalize CNAs: Prohibition of Harmful Interference

ITU Constitution

(there are more provisions which indirectly prohibits..)

◆ Art. 45

not to cause any harmful interference to the radio services or communications of other member states or of operating agencies when they establish and operate any radio services or communications

◆ Art. 48

Ensures states for "entire freedom" in military radio installations, but requires to follow the existing regulation in case of public correspondence

3. ITU's Initiative to Criminalize CNAs: Prohibition of Harmful Interference

◆1982 UN Convention on the Law of the Sea

prohibits any act conducted in the territorial sea aimed at collecting information to the prejudice of the defense or security of the coastal state; any act of propaganda aimed at affecting the defense or security of the coastal state; and any act aimed at interfering with any systems of communication or any other facilities or installations of the coastal State

◆1982 Nairobi Convention

prohibits harmful interference with radio navigation services

◆1976 INMARSAT Convention

requires that its telecommunication infrastructure be used only for peaceful purposes

(→LOAS only applies to State activities in cyberspace during armed conflict)

3. ITU's Initiative to Criminalize CNAs:

- UNGA Resolution 57/239 "Creation of a global culture of cybersecurity"
- The Tunis Agenda of the World Summit on the Information Society (WSIS) in 2005

→the ITU Secretary-General, Dr. Dr. Hamadoun I. Touré, launched

Global Cybersecurity Agenda (GCA)

High-Level Experts Group (HLEG) was established for ITU efforts to criminalize CNAs

3. ITU's Initiative to Criminalize CNA

"Cyberspace allows criminals to exploit online vulnerabilities and attack countries' infrastructure"

- Work Area one (WA1)

Goal: to clarify how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner

- 15 Recommendations

Council of Europe's Convention on Cybercrime of 2001

Council of Europe's Convention on the Prevention of Terrorism of 2005

3. ITU's Initiative to Criminalize CNA:
Council of Europe's Convention on Cybercrime

◆Goal:

"to criminalize cybercrime by requiring states parties to establish cyber offence by adopting / building their domestic law in line with human rights treaties"

↓because..

CNAs allows unauthorized access to satellite operation system

◆Articles 2-8

(illegal access; illegal interception; data interference; system interference; misuse of device; computer-related forgery; and computer-related fraud)

3. ITU's Initiative to Criminalize CNA:
Council of Europe's Convention on Prevention of Terrorism

◆ Rrecommendation 1.11. of the HLEG report

(in line with the Convention on Cybercrime and human rights treaties)

◆ Goal

"to fight against terrorist misuse of the Internet and related ICTs"

◆Relevant to cybersecurity

Article 5 (public provocation to commit a terrorist offence)

Article 6 (recruitment for terrorism)

Article 7 (training for terrorism)

3. ITU's Initiative to Criminalize CNA:
Challenges to Criminalize CNAs to Satellite Communication

Cybercrime is neither in the context of CNAs nor space security.

Because…

✓ LOAC is not applicable because cybercrime is below the level of "force."

✓ Space law is not applicable if cybercrime is committed by non-state actor.

→Even if the criminal of CNAs to satellite communication is identified, states parties to the Outer Space Treaty are still responsible for their national space activities and "launching states" are still liable for the damage caused on the surface of the Earth as well as an airplane in flight. (Art. VI and VII of the Outer Space Treaty of 1967)

Conclusion

◆ Harmful Interference caused by CNA to Satellite-based communications highlights the need to review the existing treaties that serve to prevent and prohibit CNA to all outer space activities.

◆ Due CNA allowed unauthorized access by individuals to space systems, ITU attempts for the criminalization of CNA by domestic law is effective solution.

◆ Legal development over cybersecurity in space law, (ITU law), law of armed conflict and human rights should be studied comprehensively.