57TH COLLOQUIUM ON THE LAW OF OUTER SPACE

Session 5

RECENT DEVELOPMENTS IN SPACE LAW

Chairmen:
Philippe Clerc
Sylvia Ospina

Rapporteur:
E. Boullé

Computer Network Attacks in Outer Space: The Case of Harmful Interference to Satellite-Based Communications

Dr. Yuri Takaya-Umehara[*]

Abstract

While the nature of Computer Network Attacks (CNA) highlights obstacles to the application of the law of armed conflict, harmful interference caused by CNA to satellite-based communication falls into the scope of space law, especially the ITU law. Considering the need for cybersecurity in interference-free telecommunication, the ITU recommends its member states to adopt the Conventions on Cybercrime of 2001 and the Convention on the Prevention of Terrorism of 2005, or follow them as guidelines in developing their internal legislation. In this respect, the author reviews the existing principles and norm in space law that serve to prevent CNA and examines the ITU efforts in the criminalization of computer-based fraud in relation to CNA.

1. Introduction

In recent years, the avoidance of intentional or deliberate interference to satellite-based radio communications has entered into the context of space security.[1] Among the cases of unintentional or accidental interference, caused

* Lecturer, Kobe University, Japan, yuritakaya_japan@hotmail.com

1 For example: ITU Workshop on International Satellite Communication, "The ITU - challenges in the 21st century: Preventing harmful interference to satellite systems," 10 June 2013, Geneva; and Secure World Foundation, Panel Discussions on "Radio Frequency Interference and Space Sustainability," 17 June 2013, Washington DC; Martha Mejia-Kaiser, "Space law and Unauthorized Cyber Activities," in: Katharina Ziolkowski (ed.), *Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy*, NATO CCD COE Publication, Tallinn 2013, pp.349-372.

by several factors such as human errors or hardware problems,[2] 3-5 % of entire interference is deliberately caused.[3] Although it is unclear whether or not such interference was occurred to support any armed conflict on the Earth, the potential damage caused by Computer Network Attacks (CNA) is serous to any systems that uses internet. As it is obvious that most of space systems are highly dependent on computer systems, their vulnerability to CNA highlighted the need to review the existing law that serves to prevent CNA to outer space activities. For this purpose, the present paper considers: the definition and cases of CNA [2]; harmful interference in space law [3]; harmful interference in the ITU law [4]; and legal efforts to criminalize CNA in the ITU law [5].

2 What is CNA?

2.1. Definition

CNA is defined as "[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."[4] In sum, both the weapon and the target of the attack are the network itself and information contained on such networks.[5] The information covers operating code of a computer, its automated processes and applications, as well as files and data it contains.[6] In this respect, it distinguishes from forms of electronic

[2] The causes of accidental interference are categorized in 6 reasons: uplink personnel mistakes (human error); cross-pole interference caused by misaligned uplink signal in opposite transponders; unknown carriers; hardware problems; adjacent satellite interference; and terrestrial service interference. iBRAHiM ÖZ, "Fighting with Satellite Interference," presented at ITU Workshop on International Satellite Communication, *ibid*. Texts are available at: http://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/ibrahim-oz.pdf (last accessed on 3 August 2014).

[3] *Ibid*. Also see, Ram S. JAKHU, "Satellite: Unintentional and Intentional Interference," presented at Secure World Foundation, *supra* note 2. Texts are available at: http://www.swfound.org/media/108687/Jakhu-Satellite%20Interference%20and%20Space%20Sustainability%20(17JUN13).pdf (last accessed on 3 August 2014).

[4] US Department of Defense, *Dictionary of Military and Associate Terms* 08 November 2010, as amended through 15 June 2014. Texts are available at: http://www.dtic.mil/doctrine/dod_dictionary/data/c/10082.html (last accessed on 3 August 2014).

[5] Heather Harrison DINNIS, *Cyber Warfare and the Law of War*, Cambridge Studies in International and Comparative Law, Cambridge University Press, 2012, p. 4.

[6] *Ibid*., p. 5.

warfare using electromagnetic pulse (EMP) generators or jammers, radar, radio, optics such as laser, infrared devices, and high-powered microwaves.[7] Thus, "CNA to satellite-based communication" means to cause harmful interference to satellite radiocommunication by sending a malicious code (or virus) to satellite operation systems.

2.2. CNA Cases

To understand the seriousness of damage caused by CNA, the present section briefly introduces three major incidents. The first one is a Distributed Denial of Service (DDoS) attack that uses many compromised computers to flood a target system with requests for information until it collapses under the strain.[8] On 27 April 2007 DDoS attacked social infrastructure such as the banking, governmental services and media in Estonia,[9] proving that CNA is quite effective to a state highly dependent on advanced computer technologies. Assuming the involvement of Russia for launching the attack,[10] Estonia requested assistance from its NATO allies under the terms of that alliance; however, due that cyber-attack was not defined as a clear military actions by NATO, no official action was made. The second case is a combination of CNA and a conventional attack. On 6 September 2007, in order for Israel's air force to bomb a suspected nuclear site at Dayr az-Zawr in Syria, CNA was launched to disable the advance warning system of an air defense network.[11] The third incident was caused by the Stuxnet worm in June 2010, mainly attacking Bashir and Natanz nuclear facilities in Iran. The worm was designed to seek out its final target and cause damage by making quick changes in the rotational speed of motors and sabotaging the normal operation of control systems. [12] Such a function to affect the speed of converters is applicable to gas pipelines, chemical plants and a number of other different machines.
Those cases were quoted in the context of *jus ad bellum* in the law of armed

---

7 *Ibid*., p. 4.

8 *Ibid*., p.38.

9 *Ibid*.

10 Tony Halpin, "Putin Accused of Launching Cyber War," *The Times*, London, 18 May 2007, Overseas News 46. Texts are available at: http://www.thetimes.co.uk/tto/news/world/europe/article2595192.ece (last accessed on 20 Sept. 2014).

11 David A. Fulghum, Robert Wall and Amy Butler, "Cyber-Combat's First Shot: Attach on Syria Shows Israel Is Master of the High-Tech Battle," 167, 21, 2007, *Aviation Week & Space Technology*, p. 28.

12 *Supra* note 5, pp.291-292.

conflict due its potential damage that could be equivalent to "an armed attack" or "armed force."

2.3. Obstacles to Prohibiting CNA

Legal studies in applying the law of armed conflict to CNA identified several obstacles to prohibiting CNA. Major difficulties are closely related to the nature of CNA. First, CNA is not yet internationally recognized as "force" in Article 2(4) of the UN Charter [13] that prohibits the use of force in international relations against territorial integrity or political independence.[14] Second, the target and weapons to use for CNA are the information that are intangible. Third, it is difficult to define when CNA actually starts in light of proving the existence of an attack, as CNA lets computer network be infected but does not trigger to attack immediately. Forth, IP address is not necessarily linked to the original attacker. For example, DDoS attack uses numerous computers to launch CNA and it is not traceable as CNA approaches to the target via numerous internet providers. Fifth, even individuals irrelevant to armed conflict can launch CNA. Those obstacles have been identified in application of the law of armed conflict.

In the case of harmful interference caused by CNA to satellite-based communications, there are two possible consequences: direct and indirect. The former is dysfunction of satellite operating systems by, for example, DDoS; and the latter is unauthorized manipulation of communication satellite to endanger other satellite-based communication or any other outer space activities.

3. Harmful Interference in Space Law

Regardless of the type of consequences, direct or indirect, CNA against any space systems or operations are in the scope of space law that aim to ensure peaceful uses of outer space. However, it does not mean that any kind of CNA against space activities is immediately categorized as "aggressive" uses of outer space. CNA itself is not recognized as "force" in international law and there is another possible use of CNA as a sanction in the context of collective

[13] United Nations, *Charter of the United Nations*, 24 October 1945, 1 UNTS XVI. Texts are available at: http://www.refworld.org/docid/3ae6b3930.html (last accessed 1 Sept. 2014).

[14] *Case Concerning Military and Paramilitary Activities in and against Nicaragua* (Nicaragua v. United States of America) (Merits) (1986) ICJ 14, International Court of Justice, para. 190.

security under the UN Charter.[15] For example, CNA can be used against nuclear facilities not to "destroy" but to "stop" the production of nuclear weapons, like the Natanz case in 2010.

Therefore, the present section limits the scope of study to harmful interference by CNA to satellite-based communications, and examines the existing principles and norms in: the Outer Space Treaty of 1967 (OST)[16] [3.1.]; Transparency and Confidence-Building Measures (TCBMs) [3.2.]; and Code of Conduct for Outer Space Activities [3.3.].

3.1. Principles to Prevent Harmful Interference

The definition of "harmful interference," which is to be clarified in [4.2.], is to endanger the functioning of a radionavigation and radiocommunication service. The relevant principles to such harmful interference are Article I, III, IV and IX of the OST.

Article I aims to ensure the freedom in outer space activities, consisting of the rights to use, explore and access to outer space, to any states. Article I (1) provides that outer space is the province of all mankind where the exploration and use of outer space need to be carried out for the benefit and in the interests of all countries. The phrase reminds of obligation to respect the right of other states right by refraining from carrying out activities that only benefit to specific state or a group of states. Article I (2) and (3) confirm that any state is entitled to enjoy the right to explore, use and access to outer space. As CNA infringes this freedom of exploration and use of outer space by dysfunctioning space systems, it breaches Article I.

Article III stipulates that international law including the UN Charter applies to outer space activities. This provision brings the same controversy over the legality of use of force for self-defense and collective security, not substantially helpful to prevent harmful interference by CNA.

Article IV (1) specifically prohibits placing, installing and stationing weapons of mass destruction in outer space in any other manner, while Article IV (2) requires the exclusively peaceful uses of the Moon and celestial bodies. Neither CNA nor the test of CNA is explicitly prohibited in this provision; however, harmful interference by CNA with space activities on the Moon and other celestial bodies is against "exclusively" peaceful uses of outer space.

---

15 *Supra* note 5, p. 109.

16 Treaty on Principles Governing Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, 27 January 1967, 610 *UNTS* 205.

According to Article IX, states parties are guided by the principle of co-operation and mutual assistance; and conduct all their activities with due regard to the corresponding interests of all other states. Although it does not cover non-state actor's CNA, this provision is most effective in preventing CNA by requiring states parties to undertake appropriate international consultations if they have reason to believe that their activities or experiments would cause potential harmful interference with other states' space activities.

3.2. Transparency and Confidence-Building Measures

Although Transparency and Confidence-Building Measures (TCBMs) are non-binding and voluntary, the purpose and function of TCBMs serve to enhance safety and security in outer space activities. TCBMs are a means by which governments can share information to: create mutual understanding and trust; reduce misperceptions and miscalculations; and thereby help both to prevent military confrontation and to foster regional and global stability.[17] Compared with Confidence-Building Measures (CBMs) in the context of the prevention of an arms race in outer space (PAROS) in the early 1990s, transparency-oriented measures by information-sharing is more prioritized to deter any harmful conduct to other states' space activities. The Governmental Group of Experts (GGE), established in 2010,[18] confirmed TCBMs elements in space treaties as binding and proposed in the final report of 2013 new TCBMs in the context of military uses of outer space with the aim of enhancing clarify in states' intent in space activities. The most important function of TCBMs in terms of harmful interference, particularly caused by CNA, is to prove state' intent in outer space activities. As there is technical limit in tracing the original point "where", "when", and "by whom" CNA is launched, the clarification of state' intent in advance helps to prove who is the real victim, considering that CNA enables any state to be suspected as an attacker by unauthorized manipulation.

3.3. Code of Conduct for Outer Space Activities

In December 2008, EU first launched its proposal for the International Code of Conduct for Outer Space Activities, in response to the request by the UN Secretary General to member states for concrete proposals for TCBMs. With

[17] UN Doc., A/68/189, "Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities," 29 July 2013, p. 18.

[18] UN Res. A/RES/65/68, "Transparency and confidence-building in outer space activities," 13 January 2011.

holding three rounds of multilateral Open-ended Consultations,[19] EU involved 95 member states in forming the voluntary "rules of the road" to enhance safety, security, and sustainability in outer space activities.[20] In the latest draft of 2013, harmful interference is referred in the following 6 paragraphs: 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); and consultation mechanisms to prevent or minimize harmful interference (para. 82).

In terminology, the draft seems to use different word from the ITU regulation. Only para. 53 uses the terms "harmful radio-frequency interference," while the rests use "harmful interference." This difference seems to draw a line between space law and the ITU law in defining harmful interference. In addition, due to the non-binding nature of the code of conduct, there is a limit in prohibing CNA from targeting satellite communications, leading to the next question to what extent the ITU law prohibit harmful interference caused by CNA.

In sum, although the prevention of harmful interference is in the scope of the existing principles, TCBMs and the draft code of conduct, their effectiveness remain unclear in terms of preventing harmful interference, particularly caused by CNA. Therefore, the following section examines to what extent the ITU law serves to this end.

4. Harmful Interference in ITU Law

The preamble of the ITU Constitution and Convention[21] fully recognizes the sovereign right of each state to "regulate" its telecommunication. With a long history in telecommunication since the late 19th century, national legislations

[19] Open-ended consultations were held in Kiev (May 2013), Bangkok (November 2013), and Luxembourg (May 2014).

[20] EEAS, "The EU leads a multilateral initiative on an International Code of Conduct for Outer Space Activities." Texts are available at: http://eeas.europa.eu/non-proliferation-and-disarmament/outer-space-activities/index_en.htm (last accessed on 30 Sept. 2014).

[21] Constitution and Convention of the International Telecommunication Union, Constitution, 1825 *UNTS* 331; Convention, 1826 *UNTS* 390, 1 July 1994.

have been well developed to regulate their activities in accordance with the ITU law. In other words, any harmful interference to earth-based telecommunication by its nationals remains the scope of national legal systems. On the other hand, the harmful interference to satellite-based communication by CNA still remains in the international domain of the ITU law, consisting of the ITU Constitution and Convention and the Administrative Regulations (i.e. Radio Regulations and Telecommunications Regulations). To clarify the ITU law mechanism to prohibit harmful interference, the present section reviews the existing procedures that serve to protect frequencies from harmful interference and prohibit harmful interference.

4.1. Protection of Frequency from Harmful Interference

As the oldest specialized UN organ, originally founded in 1865 as the International Telegraph Union, the present ITU covers the latest issues in the whole International Communication Technologies (ICTs) sector including digital broadcasting, the Internet, mobile technologies and 3D TV.[22] In the beginning of satellite era, the need for frequency control in satellite radiocommunication was emphasized in the UN *Ad Hoc* COPUOS's report to the General Assembly urging that ITU and the States members of the 1959 Administrative Radio Conference of ITU allocate adequate frequencies for space programmes.[23] Since then, it has played a critical role in ensuring interference-free uses of Geostationary orbit (GEO) for satellite communication with updating the ITU law thought Plenipotentiary Conference.

The ITU allocates radio frequencies among various radio communications services, not among its member states. To avoid harmful interference to the radio stations of other members, radio communication providers record their radio assignments in the Master International Frequency Register (MIFR) in accordance with Article 11 of the Radio Regulation (RR). The recording of assigned frequencies and orbital positions aims to ensure formal international recognition thereof and provide protection against interference; however, it became more complicated when ICTs sector, namely internet, entered into the scope of the ITU where no effective countermeasure was considered against CNA.

---

22 ITU, "History," tests are available at: http://www.itu.int/en/about/Pages/history.aspx (last accessed on 15 August 2014).

23 UN Doc. A/4141, "Report of the Ad Hoc Committee on the Peaceful Uses of Outer Space, " paras 57-66.

4.2. Definition of Harmful Interference

In the ITU law, the difference between "interference" and "harmful interference" lies in whether it involves safety services or not. While the former is "[T]he effect of unwanted energy due to one or combination of emission, radiations upon reception in a *radiocommunication* system, […],"[24] the latter is first found in the Atlantic City Regulations of 1947, a decade before the first launch of satellite. It is defined as "[A]ny radio service or any induction which endangers the functioning of a radio-navigation service or of a safety service or obstructs or repeatedly interrupts a radio service operating in accordance with these Regulations."[25] The phrases were updated and added to Annex 3 to the ITU Convention of 1959, though almost the same wordings.[26] In 2012, the latest version of definition is "[I]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations (CS)." [27]

Although a computer virus or a malicious code used in CNA is not "energy" in the definition of "interference," it is designed to endanger a radionavigation service or other safety services, or interrupting radiocommunication services. Taking it into consideration, the ITU law applies to CNA designed to cause harmful interference to satellite-based communications.

---

24 "The effect of unwanted energy due to one or combination of emission, radiations upon reception in a *radiocommunication* system, manifested by any performance degration, misinterpretation, or loss of information which could be extracted in the absence of such unwanted energy," ITU Radio Regulations, Section VII- Frequency Sharing, 1.166 "*interference,*" Edition of 2012. Texts are available at: http://www.itu.int/en/sama/Pages/download.aspx?pub=R-REG-RR-2012-ZPF-E (last accessed on 12 August 2014).

25 Bin CHENG, *Studies in International Space Law*, Clarendon Press Oxford, 1997, p. 96.

26 "Any emission, radiation or induction which endangers the functioning of a radionavigation service or of other safety services, or seriously degrades, obstructs or repeatedly interrupts a radiocommunication service operating in accordance with the Radio Regulations," Annex 3 to the International Telecommunication Convention, 1959,

27 "Interference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly interrupts a radiocommunication service operating in accordance with Radio Regulations (CS)." *Ibid*., 1.169 "harmful interference."

4.3. Prohibition of Harmful Interference in the ITU Law

In order to avoid harmful interference between radio stations of different countries,[28] the ITU effects allocation of any associated orbital position in the GEO or of any associated characteristics of satellites in other orbits. Among provisions in the ITU law that prohibit causing harmful interference, this section examines Article 45 and Article 48 of the ITU Constitution.

Before reviewing them, the subjects of the ITU law are to be clarified. Article 6.1 of the Constitution first stipulates that all telecommunication offices and stations established or operated by member states "which engage in international services or which are capable of causing harmful interference to radio services of other countries" must observe the provisions in the ITU law. Article 6.2 extends the same obligation to private operate agencies/entities authorized by member states. Thus, Article 6 covers civil and commercial activities, while it excludes military activities from obligation in accordance with Article 48.

Article 45 requires ITU member states: 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;[29] to ensure all agencies to follow the provision;[30] and to recognize the necessity of taking all practical steps to prevent the operation of electrical apparatus and installations from causing harmful interference.[31] While Article 45 applies to non-military radiocommunication activities, Article 48 first ensures member states "entire freedom" in military radio installations,[32] though requiring them to observe statutory provisions to prevent harmful interference as well as to follow the Administrative Regulations concerning the types of emission and the frequencies to be used. [33] And if their military installations are to be used for public correspondence or other services in the scope of the Administrative Regulations, member states are also obliged to comply, in general, with the regulatory provisions for the conduct.[34]

---

28 Art. 1(2)(a). As to services on earth, ITU "effects allocation of bands of the radio-frequency spectrum, the allotment of radio frequencies and the registration of radio-frequency assignments."

29 Art. 45(1) of the ITU Constitution.

30 Art. 45(2) of the ITU Constitution.

31 Art. 45(3) of the ITU Constitution.

32 Art. 48(1) of the ITU Constitution.

33 Art. 48(2) of the ITU Constitution.

34 Art. 48(3) of the ITU Constitution.

As two provisions require states to control all telecommunication offices and stations engaged in international services and capable for causing harmful interference,[35] member states are responsible for their civil, commercial and military activities. Even if states lack their domestic law to authorize commercial activities, such as a licensing system, operating agencies enter in the scope of state control in accordance with Article 45 covering "recognized" as well as "duly authorized" operating agencies. [36]

Although the ITU law has particular provisions to prohibit harmful interference, it does not serve to mitigate cyberthreat by CNA causing harmful interference. As the ITU recognizes the increasing risk since the early 2000s, it explores practical measures to criminalize a cyber-attack. The following section examines the current ITU efforts in the criminalization of CNA.

5. Criminalization of CNA by ITU

Recognizing the need to promote, develop and implement a global culture of cybersecurity, as outlined in the UNGA Resolution 57/239[37] and the Tunis Agenda of the World Summit on the Information Society (WSIS) in 2005,[38] the ITU Secretary-General, Dr. Dr. Hamadoun I. Touré, launched Global Cybersecurity Agenda (GCA). It aims to establish an international framework to promote cybersecurity and enhance confidence and security in the use of ICTs.[39] For this ITU initiative, the High-Level Experts Group (HLEG) was established, with more than 100 experts,[40] to explore the possibility of criminalizing computer-based fraud with international network to share

35 Art. 6(1)(2) of the ITU Constitution.

36 Art. 45(1)(2) of the ITU Constitution.

37 UNGA Resolution, A/RES/57/239, "Creation of a global culture of cybersecurity," 31 January 2003. Texts are available at: http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf (last accessed on 20 September 2014).

38 ITU Doc. WSIS-05/TUNIS/DOC/6(Rev1)-E, "Tunis Agenda for the Information Society," 18 November 2005, p. 7. Texts are available at: http://www.itu.int/wsis/docs2/tunis/off/6rev1.pdf (last accessed on 20 September 2014).

39 ITU Global Cybersecurity Agenda (CGA), High-Level Experts Group (HLEG), "Report of the Chairman of HLEG," p.9. Texts are available at: http://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf (last accessed on 7 August 2014).

40 HLEG comprise more than 100 experts from a broad range of backgrounds in policy-making, government, academia and the private sector. *Supra* note 39, p.2.

evidences. The present section assesses the ITU efforts to criminalize CNA that involve non-state actors.

5.1. ITU Attempts to Criminalize CNA

Considering the borderless nature of cyberspace that allows criminals to exploit online vulnerabilities and attack countries' infrastructure,[41] five Work Areas[42] were set up by GCA to draft recommendations to the ITU. Legal measures were considered in Work Area one (WA1)[43] to clarify how criminal activities committed over ICTs could be dealt with through legislation in an internationally compatible manner.[44] In the 15 recommendations,[45] the following international instruments were highlighted: the Convention on Cybercrime;[46] Convention on the Prevention of Terrorism of 2005;[47] and UNGA Resolutions 55/63 and 56/121 on "Combating the criminal misuse of information technologies."[48] Particularly the Convention on Cybercrime was reiterated in recommendations as an example of measures realized as a regional initiative[49] that provides a model for national legislation as a guideline.[50]

Since the conclusion of the Convention on Cybercrime in 2001, the ITU has encouraged member states to follow national legislation to criminalize cyber-attack. A decade later, the ITU started a project on the harmonization of policies and legislations for the ICTs in African, Caribbean, and Pacific Group of States in 2011.[51]

---

41 *Ibid*.

42 Five Work Areas are: legal measures; technical and procedural measures; organizational structures; capacity building; and international cooperation.

43 On 5 October 2007, the HLEG appointed leaders of Work Area One "Legal Measures" on a voluntary basis: Mr. Jaak Tepandi, Professor of Knowledge Based Systems, Institute of Informatics, Tallinn University of Technology, Estonia and Mr. Justin Rattner, Chief Technology Officer, Intel.

44 *Supra* note 44, p.1.

45 *Supra* note 44, pp. 6-9.

46 Council of Europe Convention on Cybercrime, 23 November 2001, *ETS* No. 185.

47 Council of Europe Convention on the Prevention of Terrorism, 16 May 2005, *CETS* 196.

48 UN Res., A/RES/55/63, "Combating the criminal misuse of information technologies," 22 January 2001. UN Res., A/RES/ 56/121 "Combating the criminal misuse of information technologies," 23 January 2002.

49 *Supra* note 44, WA1 Recommendations 1.3., p. 6.

50 *Ibid*.

51 ITU-EC-ACP Project, "Support for the Establishment of Harmonized Policies for the

5.2. The Convention on Cybercrime

Why does the HLEG recommend ITU member states to ratify or follow the Convention on Cybercrimes in terms of cybersecurity? The Convention aims to criminalize cybercrime by requiring states parties to establish cyber offence by adopting their domestic law. The Preamble refers that the Convention intends to supplement the existing Council of Europe conventions on cooperation in the penal field in order to make criminal investigations and proceedings related to computer-related offence more effective. Furthermore, it states that the goal of the Convention is also in line with several human rights treaties.[52]

In the recommendation 1.4. of the HLEG report, the importance of implementing Articles 2-9 and Articles 14-22 by establishing criminal offences under domestic law were emphasized.[53] In the context of CNA to space-based communication, as CNA allows unauthorized user to 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. Those articles require intentional commitment and lack of right) are applicable. The latter, Articles 14-22, are procedural law and jurisdiction.

As the Convention is originally EU-initiated, the HLEG report recommends other non-European ITU member states to ratify or follow it as a guideline. Considering that 43 states already ratified the Convention, CNA to cause harmful interference to satellite communication could be prohibited by the Convention with common international network for data sharing.

ICT Market in the ACP States." Details are available at: http://www.itu.int/en/ITU-D/Projects/ITU-EC-ACP/Pages/default.aspx (last accessed on 8 August 2014).

52 The Preamble refers to: the 1950 Council of Europe Convention for the Protection of Human Rights and Fundamental Freedoms; the 1966 United Nations International Covenant on Civil and Political Rights; the 1981 Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data; the 1989 United Nations Convention on the Rights of the Child.

53 Articles 2-9 are related to: illegal access; illegal interception; data interference; a system interference; misuse of devices; computer-related forgery; computer-related fraud; and offences related to child pornography. Articles 14-22 are about common provisions such as: scope of procedural provisions; conditions and safeguards; expedited preservation of stored computer data; expedited preservation and partial disclosure of traffic data; production order; search and seizure of stored computer data; real-time collection of traffic data; interception of content data; and jurisdiction.

5.3. The Convention on the Prevention of Terrorism

In the context of terrorist attacks, the recommendation 1.11. of the HLEG report refers to the Convention on the Prevention of Terrorism of 2005 as an effective instrument, in line with the Convention on Cybercrime, to fight against terrorist misuse of the Internet and related ICTs. It strongly recommends ITU member states to use the convention as a guideline, or as a reference for developing their internal system and practice. Particular provisions of importance are: Article 5 (public provocation to commit a terrorist offence); Article 6 (recruitment for terrorism); and Article 7 (training for terrorism). Although the purpose of the convention is to enhance the efforts of parties in preventing terrorism and its negative effects on the full enjoyment of human rights, in particular the right to life, it would be applicable to CNA when it causes harmful interference to "endanger" a radionavigation service or other safety services, or interrupting radiocommunication service.

6. Conclusion

While the nature of CNA highlighted obstacles to applying the law of armed conflict, harmful interference caused by CNA to satellite-based communication fits in the scope of space law and the ITU law. However, there seems to be a difference in using the terms "harmful interference" in the international code of conduct for outer space activities and the ITU law. Besides such difference, their effectiveness remain unclear in terms of prohibiting CNA that interfere with general space activities.

On the other hand, in order to ensure cybersecurity against cyberthreat, the ITU takes initiative in the criminalization of cybercrime by establishing national-law-based mechanisms. As CNA to satellite-based communication is internet-based, the EU invites the non-European ITU member states to ratify or follow as guidelines the Council of Europe Conventions on Cybercrime and the Prevention of Terrorism. Those two conventions would be applicable to CNA if it endangers a radionavigation service or other safety services, or interrupting radiocommunication service.

In any case, CNA that could be triggered by non-state actors to interfere with satellite communication needs further consideration in line with the ITU legal efforts in strengthening cybersecurity in satellite communication.