Identifying the Scope of the Applicable International Law Rules towards Malicious Cyber Activities against Space Assets

*Setsuko Aoki**

Abstract

This article studies five category of malicious cyber activities against space assets in order to assess to what extent the existing international telecommunications law and space law address such activities and identify which rules should be pursued to effectively solve them. Five category of such activities include jamming, hijacking, hacking, spoofing, and robbing the control of telemetry, tracking and control (TT&C) of a satellite (a kind of anti-satellite (ASAT)). Actual incidents are selected for analysis. Those are: (i) jamming: Iranian deliberate harmful interference to the Eutelsat satellites solved in the ITU; (ii) hijacking: a terrorist organization, Liberation Tigers of Tamil Eelam (LTTE) hijacking US Intelsat-12 satellite solved by diplomatic negotiation between the Sri Lankan and US Governments using international telecommunications law developed by the ITU and individual national laws; (iii) hacking: alleged Chinese hacking of US NOAA's information systems; (iv) spoofing: Iranian spoofing of the GPS signals to guide a US/CIA's RQ-170 UAV into the Iranian territory; and (v) robbing the control of TT&C: alleged Chinese taking control of US remote sensing satellites including Landsat-7 and Terra AM-1. Concluding remarks include: 1) international telecommunications law developed in the ITU can adequately address harmful interference or hijacking as a result of malicious cyber activity as long as that is conducted by a non-State actor; 2) efforts have started in the ITU to strengthen its fact-finding ability in line with the TCBM measures taken in space activities. This orientation may be remembered as a beginning of the new stage that international space law and international telecommunications law would be merged into one field of law: 3) It remains unclear about the implications of an intangible damage occurred to a satellite when its TT&C is robbed of as a result of malicious cyber activity, while it is clear that such an action constitute the violation of the principles of respect for state sovereignty, national jurisdiction and non-intervention. Thus, for promoting peaceful uses of outer space, the elaboration of relevant Articles of the Outer Space Treaty is urgently needed to formulate clear conditions for national space activities.

* Professor of Law, Keio University Law School, Japan, saoki@ls.keio.ac.jp.

1. Introduction

This article studies five category of malicious cyber activities against space assets in order to assess to what extent the existing international telecommunications law and space law address such activities and identify which rules should be pursued to effectively solve them. Five categories of malicious cyber activities to space assets are: jamming, hijacking, hacking, spoofing, and robbing the telemetry, tracking and control (TT&C) of a satellite, a premature type of anti-satellite (ASAT). Cases presented for each category is as follows: i) intentional jamming to Eutelsat satellites from the Iranian territory; ii) hijacking of a US private satellite transponders by a Sri Lankan terrorist organization; iii) hacking of the weather information systems of US NOAA; iv) Iranian spoofing of the GPS signals to guide a US UAV into the Iranian territory; and v) robbing the control of TT&C of the US Landsat-7 and Terra AM-1.

2. Jamming: France V. Iran in the ITU/RRB

2.1 Background

It is reported that since 2003, the Islamic Republic of Iran had been continuously jamming satellite-based radio and television broadcasting programs provided by BBC and VOAPNN through French Eutelsat and US Intelsat satellites to block political and cultural influences from the Western world.[1] Such jamming was conducted not only through "terrestrial jamming" transmitting rogue frequencies to the local consumer-level satellite dishes, but also through "orbital jamming" from the territory of Iran. Orbital jamming means sending contradictory signals directly toward a satellite via a rogue uplink station so as to disrupt the TT&C of a satellite, and affect the downlink to ground stations in wide areas of the Middle East and Europe. Orbital jamming is one category of malicious cyber activities against space assets.[2]

Iranian jamming may be assessed the violation of customary international law on human rights reflected in Article 19 of the Universal Declaration of Human Rights (1948)[3] and Article 19 (2) of the International Covenant on Civil and Political Rights (ICCPR) which emphasize the right to freedom of expression.[4] However, there are also views that Iranian actions are not against international human rights law and space law.[5] For instance, the

1 Small Media, *Satellite Jamming in Iran: A War over Airwaves* (Smallmedia, 2012), pp.7-8, 35-42 & 53-60.
2 *Ibid.*, pp. 19-25; David Livingstone and Patricia Lewis, *Space, the Final Frontier for Cybersecurity?* (Chatam House, 2016), pp.16-17.
3 A/RES/217A (10 December 1948).
4 Entry into force: 23 March 1976. 999 UNTS 171. Iran is not a Party to ICCPR.
5 Several factors make it difficult to categorically decide that Iran had violated international law. For instance, Art. 19(3) of the ICCPR provides the minimum

1982 UN General Assembly resolution on "Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting" (DBS Principles) provides that the right of broadcasting States to disseminate radio and television broadcasting program by satellite regardless of frontiers is not without limitation and should be subject to the cooperation and consultation with receiving States, respecting the principle of sovereignty. The allocation of rights and obligations between the broadcasting States and receiving States is not necessarily clearly provided for in the DBS Principles.[6] Therefore, this article does not go into the details on the legality of Iranian jamming. Instead, focus is strictly placed on the current situation in the conflict resolution rules on orbital jamming between France and Iran under the international telecommunications law including International Telecommunication Union (ITU) Constitution, Convention and Radio Regulations (RR).[7]

2.2 "Harmful interference" resolved through bilateral negotiation

RR categorizes radio interference into three: "permissible interference",[8] "accepted interference",[9] and "harmful interference"[10] pursuant to the consequence for the effective communications regardless of the intention of the operators. Among the three, only "harmful interference", defined as "[i]nterference which endangers the functioning of a radionavigation service or of other safety services or seriously degrades, obstructs, or repeatedly

---

restrictions of the right to freedom of expression for the protection of national security or of public order based on law and necessity. Iran had enacted a national law in 1994 to ban private ownership of satellite technology including satellite dishes. See, e.g. Small Media, *supra* note 1, p. 30.

6 A/RES/37/92 (10 December 1982). It has to be noted that the DBS Principles advanced the right of the free dissemination of information than the recommendation in Article 9 of the UNESCO's *Declaration of Guiding Principles on the Use of Satellite Broadcasting for the Free Flow of Information, the Spread of Education and Greater Cultural Exchange* (15 November 1972), which requested that broadcasting and receiving States should reach or promote prior agreements concerning the contents of the DBS, and that prior consent shall be required concerning commercial advertising. <http://unesdoc.unesco.org/images/0000/000021/002136eb.pdf>.

7 Latest version of the Constitution and Convention of the ITU adopted by the 2014 Plenipotentiary Conference (published in Basic Texts, 2015) as well as the latest version of the RR (2016 version) are found: <https://www.itu.int/en/history/Pages/ConstitutionAndConvention.aspx>.

8 This term means "[o]bserved or predicted interference which complies with quantitative interference and sharing criteria contained in these Regulations or in ITU-R Recommendations or in special agreements as provided for in these Regulations." RR, 1.167.

9 This term means "[i]nterference at a higher level than that defined as permissible interference and which has been agreed upon between two or more administrations without prejudice to other administrations." RR, 1.168.

10 See, *infra* note 11.

interrupts a radiocommunication service operating in accordance with Radio Regulations",[11] shall be prevented. Each Member State to the ITU is bound not to engage in harmful interference to radio services of other countries and ensure that operating agencies authorized by the State concerned would abide by the same rule.[12] If a Member State has information of harmful interference committed by its operating agency, it shall ascertain the facts and take the necessary action to eliminate it.[13] The success of this mechanism depends on the goodwill and mutual assistance between Member States. If the cooperation has not produced a satisfactory result, then a State affected by the harmful interference may forward details of the case to the Radiocommunication Bureau (BR),[14] which reports this to the Radio Regulation Board (RRB). An affected Member State may appeal to the RRB. However, RRB or any other organs of the ITU is not capable of sanctioning a Member State which violates its Constitution, Convention and the rules of procedure, and only plays a role of a coordinator to the States having disagreement by urging to exercise the utmost goodwill and cooperation to localize the sources of interference and eliminate it.[15]

RRB received a complaint from France, a national State of Eutelsat, which stated harmful interference emanating from Iranian territory had persisted and adversely affected the transponders and channels of Eutelsat's satellites operated in the east longitude 9, 13, 21.5 and 25.5 degrees. RRB determined such claim was correct. However, in its capacity, it only urged Iranian Administration to locate the source of harmful interference and stop it.[16] Iran rejected its involvement 33 times to the RRB from August 2009 to February 2013,[17] but Iran conducted bilateral negotiation with France over those years. The status of bilateral negotiation was reported to the IGO/EUTELSAT, EU, and COPUOS/LSC,[18] where these organizations informally assisted in amicable settlement of the situations. In March 2013, France reported to the RRB that harmful interference had been eliminated and the issue was resolved, thus identification of a perpetrator not necessary anymore.[19]

11 RR, 1.169. Also, see, Annex, Definition of Certain Terms Used in this Constitution, the Convention and the Administrative Regulations of the ITU,1003.
12 ITU Constitution, Arts. 6 & 45.
13 RR, Art. 15.21, §13.
14 RR, Art. 15.42.
15 <https://www.itu.int/en/ITU-R/conferences/RRB/Pages/default.aspx>; RR, Art. 15.1, §1- Art.15.46.
16 ITU Press Release, "ITU Radio Regulations Board Urges Iran to End Interference Hampering EUTELSAT Satellite Operations", (26 March 2010).
17 ITU RRB13-1/DELAYED/2-E (12 March 2013), p.7.
18 See, e.g., A/AC.105/1003 (10 April 2012), para. 63.
19 ITU RRB13-1/DELAYED/5-E (18 March 2013), pp.1-2.

2.3 "Harmful interference" as an issue under the TCBM in space activities

This experience urged the ITU to strengthen the obligations of Member States to address deliberate harmful interference events by enhancing its conflict resolution process within its capacity. For instance, RR was amended to draw a stronger attention of Member States not to cause harmful interference by it or by its operating agencies.[20] Other measures taken by the ITU includes the strengthening the international monitoring systems (IMS) under the RR, 16.5 which provides that "[a]dministrations shall, as far as they consider practicable, conduct such monitoring as may be requested of them by other administrations or by the Bureau" to identify the source of harmful interference. IMS has been pursued since 1987 relating to the distress and safety system. Experiencing the Eutelsat incident, efforts for the more systematic development of IMS were taken to assist in identifying sources of harmful interference.[21] These two measures were yet taken within the traditional philosophy of international telecommunications law developed in the ITU.

New philosophy of addressing deliberate harmful interference issues was also presented. This seems worth noting as this may indicate that deliberate harmful interference should be resolved in line with space law obligations to give due regard to the corresponding interests of all other States in space activities, and to offer the good faith consultation on potentially harmful interference.[22] The European Conference of Postal and Telecommunications Administrations (CEPT) submitted a common European proposal (ECP-8) titled "New Resolution on strengthening the role of ITU with regard to transparency and confidence-building measures in outer space activities" in 2014. This proposal was inspired by the UN General Assembly resolution 68/50 (Transparency and confidence-building measures in outer space),[23]

20 First, RR, 15.21 was amended in the World Radio Conference (WRC) held in 2012. Previous version states that "[i]f an administration has information of an infringement of the Convention or Radio Regulations, committed by a station over which it may exercise authority, it shall ascertain the facts, fix the responsibility and take the necessary action" (RR, 15.21, § 13 (2004 edition)). The amended RR, 15. 21 reads: "[i]f an administration has information of an infringement of the Constitution, the Convention or the Radio Regulations (in particular Article 45 of the Constitution and No. 15.1 of the Radio Regulations) committed by a station under the jurisdiction, the administration shall ascertain the facts and take the necessary actions." The amended version specifically refers to "the Constitution" and concrete article numbers of the Constitution and the RR, which draws special attention of Member States not to cause "harmful interference" by it or by its operating agencies. See, RR, 15.21, § 13 (amended in WRC-12).

21 ITU RRB1-31/8-E (8 April 2013), pp.25-28.

22 *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies*. Entry into force: 10 October 1967; 610 UNTS 205 [Outer Space Treaty], Art. IX.

23 A/RES/68/50 (10 December 2013).

which encourages UN Member States to review and implement the proposed transparency and confidence-building measures (TCBM) contained in the governmental experts group report adopted in 2013[24] (para.2), and also encourages relevant entities and organizations of the UN system to coordinate on matters related to the recommendations contained in the report (para.5). ECP-8 was submitted to and approved at the 2014 ITU Plenipotentiary Conference (PP-2014) and became Resolution 186 (Busan, 2014).[25] Resolution 186 instructs the Director of the RB, *inter alia*, to "promote access to information, upon request by administrations concerned, related to satellite-monitoring facilities, in order to address cases of harmful interference" (para.1) and "to continue taking action to maintain a database on cases of harmful interference" (para.2) to enhance the fact-finding capability of Member States.[26] Resolution 186 was amended in the 2018 Plenipotentiary Conference (PP-18), in which Member States and Sector Members are invited "to consider participating in the cooperation agreements on the use of satellite monitoring system" (para. 3 in the new section). [27]
Resolution 186 may be remembered as a beginning of the new stage that international space law framework would encompass space service parts of international telecommunications law developed in the ITU. In this regard, Article IX of the Outer Space Treaty could provide useful criteria to solve harmful interference, such as "due regard" and good faith consultation obligations in face of "potentially harmful interference".

3. Hijacking: Sri Lanka V. LTTE

3.1 Background

A terrorist organization, Liberation Tigers of Tamil Eelam (LTTE) of Sri Lanka hijacked the transponders of Intelsat-12 geostationary satellite owned/operated by the US Intelsat Ltd., and transmitted their radio/television programs in Sri Lanka and a part of India.[28] Sri Lanka had enacted a national law to regulate television broadcasting in 1982 which contained a provision to prevent a terrorist organization from using satellite transponders.[29]

24 A/68/189 (29 July 2013).
25 Final Acts of the Plenipotentiary Conference, Busan, 2014 (2015), pp.438-440.
26 *Ibid.*, p.439; Jorge Ciccrossi, *ITU Role, Regulations and Actions to Prevent and Resolve Harmful Interference to Space Services*, 10th UNOOSA Space Law Workshop, 2016, pp.14-18.
27 AFCP/55A1/10, Resolution 186 (Rev. Dubai, 2018).
28 Intelsat, "News Release: Intelsat Works with Sri Lankan Authorities to Halt Unauthorized Use of Its Satellite", (11 April 2007).
29 Sri Lanka Rupavahini Corporation Act, Act No. 6 of 1982. Pursuant to this Act, Ministry of Information and Mass Media punished Communiq Broadband Network Company due to its failure to prevent the LTTE from broadcasting its propaganda programs in 2006.

3.2 Termination of the unauthorized satellite use through ITU regime and national legislation

When Sri Lankan Government noticed that Inelsat-12 had been hijacked and used by the LTTE, it immediately requested that the US governmental agencies including Federal Bureau of Investigation (FBI), Department of Justice and Department of State as well as a private company Intelsat Ltd., address the situation. Sri Lanka also took an initiative to convene an extraordinary conference of International Telecommunications Satellite Organization (ITSO) [30] to make efficient measures to make Intelsat, Ltd. cut off the communications.[31]

ITU Constitution fully recognizes "the sovereign right of each State to regulate its telecommunication", [32] and provides that Member States reserve the right to cut off any private telecommunications which may appear dangerous to the security of the State, to public order or to decency,[33] as well as that each Member State reserves the right to suspend the international telecommunication service, which of course includes satellite telecommunications, either generally or for certain relations and/or for certain kinds of correspondence, outgoing, incoming or in transit.[34] Thus, Sri Lankan request to cut off telecommunication service to LTTE was smoothly carried out in cooperation with the US which had jurisdiction and control of the said satellite. [35]

The US acted swiftly in accordance with the ITU Constitution rules mentioned above, US Communications Act,[36] Act on Aliens and Nationality (with respect to designation of foreign terrorist organizations (FTO)), [37] etc. Since LTTE was designated as a FTO, whoever providing "material support or resources" knowing that it is a FTO is subject to criminal penalty.[38] As "material support or resources" include providing telecommunication services, Intelsat, Ltd. had to act promptly to abide by the US laws. Sri Lanka later announced that LTTE's illegal actions had been resolved by the law enforcement both by Sri Lanka and the US.[39]

This seems to indicate that if an entity that conducted a malicious cyber activity is a private person, existing laws of ITU, ITSO as well as the US and

30 Walter Jayawardhana, "Intelsat Switches Off LTTE from Their Satellite", *Sri Lanka News* (25 April 2007).
31 ITSO Agreement, Art. 5(d) (viii).
32 ITU Constitution, preamble.
33 *Ibid.*, Art. 34 (2).
34 *Ibid.*, Art. 35. See, also, RR, 1.3 (definition of "telecommunication").
35 Outer Space Treaty, Art. VIII.
36 47 USC §502.
37 8 USC §1189.
38 18 USC §2339A & 2339. "Material support or resources" is defined in §2339 A (b) (1).
39 Embassy of Sri Lanka, "LTTE Transmissions of TV and Radio Programs to Europe and Asia Terminated by Intelsat Ltd." (24 April 2007).

Sri Lankan national laws suffice to solve the incident. This is different from the case that two sovereign States have to solve an issue based on the goodwill of the other Party.[40]

4. Hacking: Information systems of the US NOAA

4.1 Background

September in 2004, weather satellites information systems operated by the US National Oceanic and Atmospheric Administration (NOAA) were hacked through internet accessible web applications and system configuration information, etc. was stolen. It was repeated in October in 2004. NOAA, accordingly, stopped providing weather data for at least 48 hours to minimize the damage and restored the system. It is reported that such an interval affected future weather forecast statistics. Investigation by the US Department of Commerce (DoC) under the request of the Congress concluded that a variety of information in addition to that of weather had been stolen from the three of the National Environmental Satellite, Data, and Information Service (NESDIS) systems. The DoC report suggested Chinese involvement of that hacking.[41]

4.2 Elaboration of the international space law needed on the implications of intangible damages

From the international space law point of view, it is important to identify if the invasion remained only ground stations or a hacker invaded mission instruments of NOAA's satellites through communication links. If the hacking was conducted only in the ground station, which is an intelligence activity and will be addressed by national criminal laws. However, if that hacking involved mission instruments invasion, it was the infringement of the US jurisdiction and control over its space objects granted by the US registration of such satellites pursuant to Article VIII of the Outer Space Treaty. In the latter case, in addition to the violation of the respect for the national jurisdiction to the US, the violation of the principle of non-intervention for the US national property would be also recognized, for the

40 Similar cases include, e.g. the US maritime communications satellite, FLTSAT-8, hijacked by a Brazilian private entity in 2009. In that case, US-Brazil cooperation in accordance with ITU telecommunication laws successfully stopped its misuse. Kiran Krishnan Nair, "Expanding Space Security to Contain SATCOM Misuse by Terrorists, Narcotraffickers, Criminals and Other Non-State Actors", *Annals of Air and Space Law*, Vol. 39 (2014), p.304.

41 NOAA, *Successful Cyber Attack Highlights Longstanding Deficiencies in NOAA's IT Security Program, Final Report* No. OIG-16-043-A (26 August 2016).

intended use of the space objects owned by the US was compromised by the forcible cyber means.[42]

In the latter case, further, a problem needs to be considered on what kind of damage occurred to the US space object by malicious cyber activity against its mission instruments, other than the infringement of the respect for exclusive national jurisdiction under customary international law. Under the UN space treaties, "damage" [43] to space objects in outer space is usually interpreted as the physical damage brought about as a result of the physical collision between space objects.[44] It is true another interpretation exists that intangible damage caused by electromagnetic waves or malware is included for the "damage" under the Liability Convention and that malware can be regarded as a constructive space object,[45] but it has to be noted that at the time of the drafting of the Liability Convention, intangibles were never interpreted as space objects, and even today, the predominant view disagrees with such interpretation.[46] In addition to the elaboration of customary international law in this regard, the damage caused to a remote sensing satellite by the invasion of its mission instruments has to be studied under international space law regime to better address this type of malicious cyber activities.

5. GPS Signal Spoofing: US V. Iran

5.1 Background

US CIA's Unmanned Aerial Vehicle (UAV) RQ-170 monitored Iranian nuclear plants flying from Afghanistan towards near the north-eastern frontier of Iran. It is reported that Iran hacked the GPS signals information

42 While the principle of non-intervention is the foundation of international law as a corollary of the respect for sovereignty, the exact meaning of this principle remains somewhat unclear. In general, it is understood as the intervention/interference by a State against the internal or external affairs of another State, which is reserved for the exclusive jurisdiction of that State ("reserved domain") through forcible or dictatorial means to impose its policy. See, e.g., Rüdiger Wolfrum, (ed.), *The Max Planck Encyclopedia of Public International Law*, Vol. III (Oxford University Press, 2012), pp. 207-208; *idem*, (ed.), *The Max Planck Encyclopedia of Public International Law*, Vol. VI (Oxford University Press, 2012), pp. 289-299.

43 The definition of the "damage" is found in Art. I (a) of the *Convention on International Liability for Damage Caused by Space Objects*. Entry into force: 1 September 1972; 961 UNTS 187 [Liability Convention].

44 See, e.g., Stephan Hobe, Bernhard Schmidt-Tedd & Kai-Uwe Schrogl, (eds.), *Cologne Commentary on Space Law*, Vol II (Carl Heymanns Verlag, 2013), pp.128-129; Carl Q. Christol, "International Liability for Damage Caused by Space Objects", *American Journal of International Law*, Vol. 74 (1980), p.354.

45 See, e.g., Helena Correia Mendonça, Magda Cocco, et al., "International Laws Regulating Satellite Communications and Their International Disruption in Times of Peace and Conflict", *Annals of Air and Space Law*, Vol. 40 (2015), pp.129-131.

46 Hobe, et al, *supra* note 44, pp.128-129.

sent to the RQ-170 and spoofed that RA-170's GPS system with false coordinates, making it misunderstand it was flying back to Afghanistan station but in reality that rouge signal brought RQ-170 landed in the territory of Iran and captured RQ-170 almost intact.[47] While it is largely unclear what had actually occurred, this article is written on the hypothesis that US GPS satellites suffered spoofing. Iranian ambassador to the UN sent a letter to the UN Secretary General and Chair of the UN Security Council stating that Iran had taken a forced action to RQ-170 landed as that had invaded Iranian territorial air. Iran claimed an apology and compensation for the infringement of its territorial sovereignty for the US. US demanded the return of RQ-170.[48]

5.2 Legal implications of this incident under customary international law

Iranian spoofing may be considered as the violation of the prevention of the "transmission or circulation of false or deceptive distress, urgency, safety or identification signals" provided for in Article 47 of the ITU Constitution. But the provision that states "[m]ember States retain their entire freedom with regard to military radio installations" [49] implies that sending false signals is permissible also in peacetime as long as that is conducted by the military. US Department of Defense (DoD) takes this interpretation.[50] Scholars divide in their views, but those who support the US DoD views also emphasize the merits avoiding the non-compliance with Article 47 of the ITU Constitution and relating RR in time of peace for the practical utility. [51] It seems difficult to categorically conclude that Iranian spoofing was against ITU law regimes. Intelligence collection and spying is most probably against national laws related, but there exists no explicit international law rules in this regard. [52] If

47 Jordan J. Paust, "Remotely Piloted Warfare as a Challenge to the *Jus Ad Bellum*", in Marc Weller (ed.), *The Oxford Handbook of the Use of Force in International Law* (Oxford University Press, 2015), p.1099; Matthew J. Schwartz, "Iran Hacked GPS Signals to Capture US Drone" (16 December 2011), <https://www.darkreading.com/attacks-and-breaches/iran-hacked-gps-signals-to-captur>.

48 See, e.g., CNN "Obama Says U.S. Has Asked Iran to Return Drone Aircraft) (13 December 2011), <https://edition.cnn.com/2011/12/12/world/meast/iran-us-drone/index.html>.

49 ITU Constitution, Art. 48 (1).

50 DoD, Office of General Counsel, *An Assessment of International Legal Issues in Information Operations* (1999) [DoD/OGC], pp.32-34.

51 Deborah Housen-Couriel, "Disruption of Satellite Transmissions *Ad Bellum* and *in Bello*: Launching a new Paradigm of Convergence", *Israel Law Review*, Vol.45 (2012), pp.451-452; Frans von der Dunk, "Legal Aspects of Satellite Communications", in Idem, (ed.), *Handbook of Space Law* (Edward Elgar, 2015), pp.466-467; Francis Lyall & Paul B. Larsen, *Space Law: A Treatise* (Ashgate , 2009), p.207; Nair, *supra* note 40, p,302.

52 Robert Jennings and Arthur Watts (eds.), O*ppenheim's International Law*, 9th ed., Vol. 2 (Longman, 1992), pp.1176-1177; John Kish, *International law and Espionage* (Martinus Nijhoff, 1995), p. xv; DoD/OCG, *supra* note 50, pp.46-47.

Iran forced RQ-170 to fly into the Iranian territory, it is not only the infringement of the territorial air of Afghanistan, but also the violation of the respect for the immunity of the US governmental property.[53] As Iran used dictatorial interference to obtain military information of another country, such abuse of rights on the part of Iran seems to be construed as the violation of non-intervention principle under customary international law.[54] Necessity may not seem to be invoked by Iran as this does not constitute a grave and imminent peril to an essential interest against Iran.[55]

However, the question if Iran conducted "use of force" by this intervention will most probably be answered in the negative. Criteria presented by Professor Michael N. Schmitt to assess if a certain malicious cyber activity is thought as a use of force would be useful here. Those criteria constitute: i) severity (scale and effects), ii) immediacy, iii) directness, iv) invasiveness, v) measurability of effects, vi) military character, vii) state involvement, and viii) presumptive legality.[56] At first glance, Iranian action meets the prerequisite to be a potential use of force in terms of the actor, target, and the method employed. However, it does not satisfy the most important criterion "severity". Nor does it meet other criteria including invasiveness and directness. In this case, only some minor criteria such as military character and state involvement are met. It can be safely said that it falls short of use of force, and only falls under the violation of non-intervention and immunity of governmental property.

Against Iranian actions for the RQ-170, the US is entitled to take countermeasures not amount to the use of force to Iran. In addition, retorsion can be employed by the US. Whereas retorsion is usually taken to the unfriendly action which is not against international law, it can be resorted to against an unlawful act under international law as well. Needless to say, the US may pursue an international responsibility of Iran.[57]

---

53 International Group of Experts and Michael Schmitt, *Tallinn Manual on International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013) [Tallinn Manual], pp.97-101.

54 Case Concerning Military and Paramilitary Activities in and Against Nicaragua (Nicaragua v. United States of America), Judgement, *ICJ Reports* (1986) [Nicaragua Case], para. 205; Paul A. L. Ducheine, "Military Cyber Operations", in Terry D. Gill and Dieter Fleck (eds.), *The Handbook of the International Law of Military Operations*, 2nd ed. (Oxford University Press, 2015), pp.467-469; Corf Channel Case (United Kingdom v. Albania), judgement, *ICJ Reports 1949*, p.35; Michael N. Schmitt, "The Use of Cyber Force and International Law", in Weller, *supra* note 47, p.116.

55 Articles on Responsibility of States for Internationally Wrongful Acts, A/56/10 (2001) [A/56/10], Art. 25.

56 Tallinn Manual, *supra*, note 53, pp.48-51.

57 A/56/10, supra note 55, Part I, Chapter V, Part II, Chapter II.

From international space law point of view, the exact contents of damage caused to GPS satellites by the invasion of its mission instruments have to be studied.

6. Robbing the control of TT& C: a premature type of ASAT

One of the early examples of the robbing the control of TT&C is said to have been taken place in 1999 for the UK military communication satellite, Skynet, while the detail of the fact is unknown.[58] As a clearer and more recent two examples would be referred to here. Those are US cases. The first is the robbing of the control of TT&C of Landsat-7, co-operated by NASA and US Geological Survey (USGS) for more than 12 minutes both on 20 October 2007 and 23 July 2008. Likewise, it is reported that TT&C of Terra AM-1 of NASA had been perhaps robbed of on 20 June 2008 and 22 October 2008 for two minutes and nine minutes respectively.[59] It is assessed that both satellites had been hacked and robbed of the control when the public internet was used to update software from Svalbard ground station in Norway. (For the upgrading software, public internet was periodically used in operating both satellites.) The investigation concluded that such premature type of ASAT had been conducted by China.[60] If the robbing of the control of TT&C, then the change of the orbit of a satellite and making it collide with other satellite may be possible, invading TT&C of a satellite is more dangerous than other types of malicious cyber activities relating to the safety of outer space.

The essential issue seems the same with cases of the hacking of US NOAA satellites and the spoofing of US GPS. International space law remains fully explored about the implications of intangible damage including the one caused by cyber means. In case of malicious cyber activities, the action often started from the ground stations and the damage generated also on the ground such as the NOAA NESDIS case. Thus, infringement of the TT&C itself can be less seriously considered than the measurable damages on the ground. However, considering the fact that the taking control of TT&C could eventually bring the full-scale destruction of satellite, the conditions and legal effects for the invasion of the TT&C should be urgently elaborated.

58 See, e.g., Heather Harrison Dinniss, *Cyber Warfare and Laws of War* (Cambridge University Press, 2012), p.285.

59 US-China Economic and Security Review Commission, *2011 Report to the Congress* (2011) pp.214-216.

60 *Ibid*., pp.215-217.

7. Conclusion

From the brief analysis of the five category of malicious cyber activities, the following could be referred to as lessons learned and tasks for the future:
First, International telecommunications law developed in the ITU could appropriately address a certain type of malicious cyber activities such as deliberate harmful interference through jamming and hijacking of transponders, if such an activity is conducted by a non-State actor.
Second, it should be noted that efforts have been made in the ITU to strengthen its fact-finding ability in line with the TCBM measures taken in space activities. This orientation may be remembered as a beginning of the new stage that international space law and international telecommunications law would be merged into one field of law. In addition, it is expected that Article IX of the Outer Space Treaty would provide useful criteria such as "due regard" and good faith consultation obligations in face of "potentially harmful interference" to solve harmful interference.
Third, some types of malicious cyber activities involve the invasion of TT&C or mission instruments of satellites to bring about a certain consequence mostly on the Earth. If the robbing of the control of TT&C results in its collision with other space object(s) or the physical destruction of that satellite, this is a full-fledged ASAT. While that shall be avoided for the peaceful uses of outer space, there are international law rules to address it. In contrast, ambiguity prevails in case where no tangible damage occurs to a satellite by the robbing of the TT&C through a malicious cyber activity. That is the violation of the principle of respect for state sovereignty, and as its corollaries, it is the violation of the principles of national jurisdiction and non-intervention. However, these principles are not duly translated into space law rules. The elaboration of Article VIII (State of registry holds jurisdiction and control over such space object) and Article IX (due regard, efforts to avoid potentially harmful interference, etc.) could be a first step to formulate clear conditions for national space activities in the era that international space law should also engage in addressing increased malicious cyber activities.