# Legal Assessment of Surveillance Activities in Cyberspace —From the Standpoint of Espionage, Infringement of Sovereignty, and Human Rights Laws (Violations of Privacy)—*

Keiko Kono**

**Abstract**

This paper examines the issues of espionage, infringement of sovereignty, and human rights laws (violations of privacy) as they relate to international laws covering surveillance activities conducted in cyberspace. Conventionally, intelligence activities targeting another country were not deemed as espionage under international law as long as these activities satisfied certain conditions. However, activities conducted in cyberspace tend to be distinguished from espionage under international law because their digital or virtual location in another country's domain does not satisfy the conventional location requirement. Also, surveillance during peace time can result in the problem of infringement of sovereignty of the targeted country. On the other hand, communication surveillance targeting a foreign national outside of a country's domain has received much attention in recent years from the standpoint of the extraterritorial application of international law. Nevertheless, it is important to better understand conventional conditions from a digital and virtual context.

## Introduction

What problems arise in terms of international laws when conducting surveillance of another country's activities in cyberspace? This paper will explore this problem from the standpoint of espionage, infringement of sovereignty of other countries, and applicability of human rights violations.

There are various forms of activities carried out in cyberspace. For example, these include internet communications between a country and its embassies in other countries, and situations where the information agency of a country penetrates the information system of another country used to store the government's confidential information, resulting in the loss of important information. *The Tallinn Manual on the International Law Applicable to Cyber Warfare* published by the NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE) in 2013 covers the problems of when malware is installed in the information system of another country for the purpose of surveillance. It explains that experts involved in discussions could not reach a consensus on whether the installation of such malware constituted an infringement of the target country's

* Originally published in Japanese in *Boei Kenkyusho Kiyo* [NIDS Security Studies], vol.19, no.2, March 2017. Some parts have been updated.

** Fellow, Government and Law Division, Security Studies Department.

sovereignty if there was no physical damage.[1] United States Naval War College Professor Michael Schmitt, the director of the project of the *Tallinn Manual*, within his own editorial remarks, stated that surveillance of another country's activities conducted by acquiring signals transiting inside the country's own domain does not result in any legal infringements whatsoever (as long as there is no physical damage or intention of coercing the other country), which is because international law does not prohibit espionage.[2] This likely means that Professor Schmitt believes signal acquisition conducted within another country's domain does not pose a concern of being an infringement of the country's sovereignty.

Installing malware in another country's system for the purpose of surveillance during peace time is believed to carry the high likelihood of being considered an infringement of sovereignty if the act involves unauthorized access of the target country's information system (the term used in Japanese laws is "Unauthorized Computer Access"). However, the conclusion of assessing whether such an act is espionage may change based on whether the act in cyberspace is considered espionage under international law. If the act of acquiring confidential information of another country through cyberspace does not satisfy the existing definition of espionage, it is meaningless to debate the assessment in this context. Espionage has long been established as a war time program, but the *Tallinn Manual* argues that surveillance activities in cyberspace are not considered espionage under international law in cases where they are carried out remotely in an area outside of an adversary's control. However, personal opinion suggests that there is ample room for such actions to be considered espionage considering conventional conditions. Also, the *Tallinn Manual* argues that espionage during peace time is not prohibited under international law,[3] but the problem therein lies with how espionage is ultimately perceived with the infringement of the sovereignty of the target country. If a reconnaissance airplane or ship engages in espionage in a physical domain such as on the ground, in the sea or in the air, the country of the territory in question could easily recognize such action as a use of force by an invading country under Article 2(4) of the United Nations Charter. As of today, however, there has yet to be a case in which this same type of recognition was made with regard to cyberspace.

Although not mentioned in the *Tallinn Manual*, the issue of violation of privacy under human rights laws has suddenly taken on importance in recent years as an issue under international law related to cyber surveillance activities.[4] Even in the event that a certain country's information agency carried out intelligence activities targeting the staff of a foreign embassy within its borders as a legitimate operation, the government must handle data from communications of its own people acquired incidentally during this process according to means that respect the privacy of these people (case of Amann *v*. Switzerland of The European Court of Human Rights [ECHR] [ruling issued on February 16, 2000]).[5] This type of issue has created a sensation publicly as of late because it has occurred not only with regard to people within the country, but also involving

---

1 Michael Schmitt, ed., *Tallinn Manual on the International Law Applicable to Cyber Warfare* (Cambridge University Press, 2013), p.16, Rule 1, para. 6.

2 Michael Schmitt, "The Law of Cyber Warfare: Quo Vadis?" *Stanford Law and Policy Review*, Vol.25 (2014), p.275.

3 Schmitt, *Tallinn Manual*, p.30.

4 Issues related to international human rights law will be covered in the *Tallinn Manual 2.0* planned for publication in February 2017.

5 European Court of Human Rights (ECHR), Case of Amann against Switzerland, Application no. 27798/95, Judgment (February 16, 2000), http://hudoc.echr.coe.int/eng?i=001-58497

the communications of foreign nationals outside of a country's own territory, but it could be said that almost none of those countries conducting surveillance (or countries intending to do so) acknowledges their obligation to respect privacy as it relates to foreign nationals outside of their territory. This issue has often been debated as the problem of extraterritorial application of human rights laws within the papers of international legal scholars in recent years,[6] but the possibility for international human rights treaties to be applied to a country extraterritorially under certain conditions has been proven in precedents of the International Court of Justice (ICJ) and ECHR. The most conventional precedents in either case consider activities conducted in a physical context by an occupational authority during war time or occupying foreign military. In contrast, this paper examines whether state-sponsored activities conducted in a non-physical context such as cyberspace can be discussed in the same terms as conventional precedents. If activities conducted in cyberspace can be considered as an extension of conventional precedents, it should be possible to derive a government's obligation to respect the privacy of foreign nationals outside of its own territory. Conversely, if the obligation to respect the privacy of foreign nationals outside a territory does not exist as advocated by certain countries, it can be presumed that such refute is related to the unique situation of cyberspace.

This paper first considers the potential for cyber espionage to exist in the context of war time and then examines an assessment within the context of peace time while touching upon the potential for infringement of sovereignty. Additionally, there are instances where cyber surveillance activities can violate human rights law in the sense of violating an individual's privacy within the scope of the surveillance, regardless if such activities are carried out in war time or peace time. This paper focuses on intelligence activities instead of criminal investigations to elucidate issues concerning the extraterritorial application of human rights laws. Furthermore, the scope of consideration of this paper focuses exclusively on international communications carried out through cyberspace by extraterritorial foreign nationals.

## 1. Assessment of Cyber Surveillance Activities during War Time

This section discusses the issue of espionage during war time, with focus on how existing international laws established in the context of physical domains are applied with regards to cyberspace. In addition, this section also introduces the fact that privacy rights during war time are a relatively new issue.

### (1) Cyber Espionage

The definition of espionage is stated in Article 46 of the *Protocols Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I)* (hereinafter, "Protocol I"). In other words, espionage is deemed as when "A member of the armed forces of a Party to the conflict who, on behalf of that Party and in territory controlled by an adverse Party, gathers or attempts to gather information shall be considered as engaging in espionage if, while so acting, he is [not] in the uniform of his armed forces" and furthermore when this information collection is done" so through an act of false pretences or

[6] Marko Milanovic, "Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age," *Harvard International Law Journal*, Vol.56 (2015), pp.81-146.

deliberately in a clandestine manner (text underlined by the author). Of these conditions, for convenience, this paper will call "territory controlled by an adverse Party" as the location requirement. Additionally, "[not] in the uniform of his armed forces" will be referred to as the failure to display an emblem requirement and "act of false pretences" will be called the false pretence spying requirement. These requirements are practiced in international customary law as acknowledged in the *Tallinn Manual*,[7] the *Customary International Humanitarian Law* (2009)[8] prepared by the International Committee of the Red Cross (ICRC) as well as by the United States, which is not a signatory to Protocol I.[9]

i. Location Requirement

According to the *Tallinn Manual*, cyber operations conducted remotely from a location not controlled by an adversary do not satisfy the conventional local requirement, and therefore cannot be considered espionage under international law. The *Tallinn Manual* was not the first to state such a belief. The *HPCR Manual on International Law Applicable to Air and Missile Warfare)* (hereinafter, "HPCR Manual") drafted by the Harvard University Program on *Humanitarian Policy and Conflict Research* in 2009 shares the same point of view.[10] Going back further to 1999, the U.S. Department of Defense explained its stance that the digital gathering of information conducted remotely is not considered espionage under international law, citing the basis that a "digital or virtual location" does not carry the same meaning as a physical location.[11]

Considering the context of criminal investigations, the belief that the unauthorized access of data stored outside the country on a cloud or other means without completing procedures for judicial assistance with the country the data belongs to is an infringement of sovereignty is becoming more prominent as of late. Based on such a situation, it is believed that distinguishing between whether the authorities of one country intruded either digitally, virtually or physically has no real meaning (in the case of "digital intrusions in an adversary" per Table 1 below). Another problem is the acquisition of military information of an adversary from outside the adversary's territory. This situation does not involve intrusion into a territory controlled by an adversary, and as a result based on the conventional local requirement such an intrusion is not considered espionage (in the case of "digital intrusions outside an adversary" per Table 1 below). Furthermore, the only situation considered as espionage during war time is when "any member of the armed forces of a Party to the conflict who falls into the power of an adverse Party while engaging in espionage" (Article 46-1 of Protocol I), and such individuals cannot be held accountable concerning their past espionage even if they are captured by the enemy after returning to their unit after completion of their mission (Article 31 of the 1907 Convention

---

7 Schmitt, *Tallinn Manual*, p. 193.

8 ICRC, *Customary International Humanitarian Law* (2009), ICRC website, Rule 107.

9 Michael Matheson, "Additional Protocol I As an Expression of Customary International Law," in International and Operational Law Department, the US Army Judge Advocate General's Legal Center and School, ed., *Law of War Documentary Supplement* (2005), pp.396-398.

10 Program on Humanitarian Policy and Conflict Research (HPCR), ed., *Commentary on the HPCR Manual on International Law Applicable to Air and Missile Warfare* (May 2009), p.259, Rule 118, Commentary para. 6, http://www.ihlresearch.org/amw/manual/

11 U.S. Department of Defense, Office of the General Counsel, *An Assessment of International Legal Issues*, 2nd ed. (Nov. 1999), in *Naval War College International Law Studies*, Vol.76 (2002), p.516.

respecting the Laws and Customs of War on Land and Regulations concerning the *Laws and Customs of War on Land* [hereinafter, "Hague Convention"]). If it is nearly impossible to capture in the act a soldier engaged in cyber surveillance activities remotely from a territory controlled by their own army, there may be little significance in debating whether or not this person is engaging in an act considered to be cyber espionage.

**Table 1 Location Requirement of Espionage (Intrusion/Surveillance) under International Law during War Time**

| Intrusion/Surveillance | | Location requirement of espionage |
|---|---|---|
| Format | Territory | |
| Physical | Inside adversary | Satisfies |
| Digital | | Most view that it does not satisfy |
| | Outside adversary | Does not satisfy |

Note: Digital intrusion/surveillance means remote surveillance.
Source: Prepared by the author.

ii. False Pretence Spying Requirement and Failure to Display an Emblem Requirement

The HPCR Manual explains that the word clandestine used in conventions as a definition of espionage (Article 46-3 of Protocol I) or the word "spy" (Article 29 of the Hague Convention) do not necessarily fully express modern espionage because they mean operations conducted at night time to avoid capture by the enemy or over flights at a high altitude; and so rather the word covert which means hiding the physical body or characteristics of persons engaging in the activities (or equipment) should apply.[12]

It is correct to understand the failure to display an emblem requirement as including the false pretence spying requirement; rather than a requirement by itself. In particular, in the case of aircraft reconnaissance, the military aircraft engaging in reconnaissance is deemed as fully displaying an emblem if it has signage indicating its nationality or that it is a military aircraft, and therefore, even if the crew of the reconnaissance aircraft are not wearing uniforms, they will not be deemed as engaging in espionage due to the failure to display emblem requirement because they did not hide their identity.[13] If cyberspace is considered the same as aircraft reconnaissance, a soldier not wearing an emblem engaging in surveillance activities publicly using a military terminal should not be deemed as espionage under international law. Similarly, for example, a civilian in a contractual relationship with the military conducting the same activities may not be considered espionage under international law as long as these activities are public in nature. However, even if espionage does not apply to a civilian in this situation, the same civilian could be deemed separately as an illegal combatant directly participating in hostilities. Particularly, theories have been presented in which the gathering of information that could be directly used for military

[12] HPCR, *Commentary on the HPCR Manual*, p.258, Rule 118, para.1; ICRC, *Commentary on the Additional Protocol I to the 1949 Geneva Conventions* (1987), ICRC website, p.567, para. 1776.

[13] HPCR, *Commentary on the HPCR Manual*, p.260, Rule 120, para.2.

operations[14] and searching for vulnerabilities of attack targets for a specific operation[15] can be considered direct participation. If a civilian is assessed as such, they will lose protections granted to civilians in international law (in the sense of being exempted from attack) and could be exposed to attacks by the enemy. Or, even if not direct, if a civilian participates in hostilities at the very least indirectly, they may have their rights as a civilian limited after capture.[16]

In this manner, as for the issue of under what conditions activities through cyberspace are considered espionage, the actual handling of such situations remains unclear at this point in time given that there have not been a large accumulation of incidents carried out by states. Nevertheless, the one concern for civilians is direct participation in espionage or hostilities, meaning there is no change in the possibility that such a civilian engaging in these activities will be classified as an illegal combatant. In either case, the issue for civilians is the loss of protection normally afforded to them. Based on this situation, some theories explain that the psychological element of whether or not the civilian was aware should be included when determining whether there was direct participation in hostilities.[17]

(2) Privacy Rights of Civilians during War Time

When assuming that surveillance activities conducted through cyberspace are not considered cyber espionage because such activities do not satisfy the location requirement, such activities will be classified as military operations that are not generally prohibited. Article 51 of Protocol I stipulates that civilians "shall enjoy general protection against dangers arising from military operations." In this instance, military operations refer to "all the movements and activities carried out by armed forces related to hostilities," according to the commentary on conventions provided by the ICRC.[18] As a traditional example, psychological warfare not accompanying physical destruction such as the distribution of propaganda (Article 21 of the 1923 Rules of Air Warfare[19]) is considered a military operation.

Both conventions related to armed conflict, including Protocol I, and international customary law do not prohibit military operations, and for this reason, surveillance through cyberspace is legal. Nevertheless, there are no provisions fully protecting the privacy rights of civilians in armed conflict laws, even when civilian Internet communications completely unrelated to armed conflict are acquired during such surveillance activities and then this information is misused by the military.

The biometric program carried out by the U.S. and Canadian militaries in Iraq and

---

14 Hans-Peter Gasser, "Protection of the Civilian Population," in Dieter Fleck, ed., *The Handbook of International Humanitarian Law*," 2nd. ed. (Oxford University Press, 2008), p.262, para.5.

15 Schmitt, *Tallinn Manual*, p.120, Rule 35, para.5.

16 According to the Geneva Convention relative to the Protection of Civilian Persons in Time of War of August 12, 1949 (Convention 4) (hereinafter, "Civilian Convention"), there are situations where rights of civilians protected in this convention are limited for those suspected for engaging in "activities hostile to the security of the State" (Article 5).

17 Avril McDonald, "The Challenges to International Humanitarian Law and the Principles of Distinction and Protection from the Increased Participation of Civilians in Hostilities," A Paper Presented at the University of Teheran at a Round Table on the Interplay Between International Humanitarian Law and International Human Rights Law (April 2004), p.23.

18 ICRC, *Commentary on API*, p.617, para. 1936.

19 Hague Rules Concerning the Control of Wireless Telegraphy in Time of Warfare and Air Warfare, Drafted by a Commission of Jurists at The Hague (December 11, 1922-February 17, 1923), Part II Rules of Air Warfare.

Afghanistan became a much talked about topic in recent years from the standpoint of the privacy rights of civilians during war time. This program involved creating a database of several million people by collecting information such as iris, fingerprints, and facial images, etc., in order to identify terrorists who were hiding in the general population. Reports indicate that the program was able to easily identify terrorists by reconciling information in the database with information obtained from the fragments of Improvised Explosive Devices (IEDs) after explosion, the corpses of suicide bombers, and deserters, etc.[20] However, there is concern that indiscriminately collecting and storing the information of male individuals from the ages of 15 to 70 simply because physically they met the definition of combat aptitude represents a violation of the privacy rights of the general population. Also, given the high potential danger of this database being misused for genocide based on religion or ethnicity after the transition to a territorial government, it is known that in the United States a number of human rights organizations demanded that the U.S. Secretary of Defense reconsider the program.[21] As for this problem, armed conflict laws do not have stipulations for guaranteeing the privacy rights of civilians. However, with that being said, the foreign militaries on the ground implementing this program are accountable for their relationship with the local population. According to the Advisory Opinion of Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory (2004),[22] the ICJ determined that Israel violated various provisions stipulated in the 1949 Geneva Convention relative to the Protection of Civilian Persons in Time of War in its relationship with occupied peoples, and this is because together with this it was determined that Israel also violated the provisions of the international human rights treaties that it has ratified. Although this matter did not become a point at issue, it was confirmed within the Advisory Opinion that Israel has the obligation to respect the privacy rights of occupied peoples per international human rights laws.[23]

Consequently, whether it is a biometric program or surveillance through cyberspace, although such acts are not restricted particularly by armed conflict laws, parties could be held accountable based on international human rights treaties in the event they unjustly violate the privacy rights of the general population locally who are not involved in hostilities whatsoever.

## 2. Assessment of Cyber Surveillance Activities during Peace Time

This section will discuss cyber surveillance activities during peace time as they relate to espionage and infringement of sovereignty, while human rights laws (violations of privacy) will be left to Section 3 and thereafter. The legal assessment of espionage differs completely even if the same format is used during peace time and war time. This is because "the legitimacy of espionage in time of war arises from the absence of any general obligation of belligerent to respect the territory

---

20 "To Track Militants, U.S. Has System That Never Forgets a Face," *The New York Times* (July 13, 2011), http://www.nytimes.com/2011/07/14/world/asia/14identity.html; "The Eyes Have It: Biometric Data and the Afghan War," *The Economist* (July 7 2012), http://www.economist.com/node/21558263/print

21 Electronic Privacy Information Center (EPIC), "Iraqi Biometric Identification System," EPIC website, https://epic.org/privacy/biometrics/iraq.html; Alison Mitchell, "Distinguishing Friend from Foe: Law and Policy in the Age of Battlefield Biometrics," *Canadian Yearbook of International Law*, Vol.50 (2013), p.298.

22 Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, Advisory Opinion, *I. C. J. Reports 2004*, p. 136.

23 Ibid., p.188, para.128

or government of the enemy state" during war time.[24] In contrast, during peace time, espionage that involves intrusion into another country essentially is an infringement of that country's sovereignty because there is a general obligation to respect the territory of the other country.

One example frequently cited as espionage during peace time is the U-2 spy plane crash that occurred in 1960 ("physical intrusion into adversary" per Table 2). On May 1, 1960, a United States U-2 reconnaissance aircraft took off from Pakistan and flew a reconnaissance mission over the former Soviet Union, but it was shot down in Soviet territory and the crew were captured. The shot-down U-2 did not have its nationality marked on the fuselage, but it is said that the former Soviet Union already knew about the surveillance activities that had been conducted for the four years preceding the incident. However, the former Soviet Union side did not immediately publicize that it had shot down the aircraft. For that reason, the United States government, which did not know the facts, initially provided a false explanation that the aircraft was operated by the National Aeronautics and Space Administration (NASA) for weather observation purposes. U.S. President Dwight D. Eisenhower fully acknowledged responsibility for U-2 reconnaissance flights only after May 11. On May 18, the former Soviet Union presented a condemnatory resolution to the United Nations Security Council. This resolution claimed that "aggressive action by the Air Force of the United States America against the Soviet Union" represents an infringement of the former Soviet Union's sovereignty that goes against the principles and purpose of the United Nations, and that such acts of aggression create threats against universal peace. Ultimately, however, this resolution did not pass because it did not receive votes of approval from Western Bloc countries.[25]

As with this incident where a United States reconnaissance aircraft violated the territorial airspace of the former Soviet Union, if a country digitally penetrates the information system of another country, it will be an infringement of that country's sovereignty (in the case of "digital intrusion inside adversary" per Table 2). The cyber attack on the U.S. Office of Personnel Management (OPM) discovered in 2015 and leakage of a large amount of personal information is an archetypical example. In 2015, OPM discovered that its information system storing the personal information of federal employees was subject to a cyber attack on two occasions resulting in the leakage of a large amount of personal information. The scope of victims included not only the present employees of federal government organizations (including part-time workers such as contract workers), but also retirees and even job applicants, reaching a total of some 21.5 million individuals. Of these, 20.9 million individuals had their background check information leaked, including name, social security number, address, date of birth, residence, school history, professional history, travel history, immediate family members, and the people they know, etc. It was also confirmed that some employees had their fingerprint data leaked.[26] From June in the same year the initial cyber attack was discovered, the U.S. Government suspected the involvement of the Chinese Government, but in the end the U.S. Government did not impose economic sanctions

---

[24] Quincy Wright, "Espionage and the Doctrine of Non-Intervention in Internal Affairs," in Roland J. Stanger, ed., *Essays on Espionage and International Law* (Ohio State University Press, 1962), p.12; Craig Forcese, "Spies Without Borders: International Law and Intelligence Collection," *Journal of National Security Law and Policy*, Vol.5 (2011), p.202.

[25] Quincy Wright, "Legal Aspects of the U-2 Incident," *American Journal of International Law*, Vol.54 (1960), pp.836-841; Ingrid Delupis, "Foreign Warships and Immunity for Espionage," *American Journal of International Law*, Vol.78 (1984), pp.53-75.

[26] U.S. Office of Personnel Management website, https://www.opm.gov/cybersecurity

or other measures. There have been media reports that the Chinese Government arrested suspects involved in the incident, but high level officials in the U.S. Government who suspected the involvement of the Chinese Government view this incident as a traditional case of espionage,[27] which suggests that the location requirement is not strictly understood in this case.

When using the assumption that espionage is permitted because it is not prohibited under international law, there is effectively no possibility that the country engaging in espionage will be criticized, so there is almost no meaning in pursuing its accountability based on the reason of infringement of sovereignty. Furthermore, in the case of acquiring the information of another country from a facility inside the territory of one's own country, there is no digital intrusion in the other country, and thus, there is no concern over infringement of sovereignty (in the case of "digital intrusion outside adversary" per Table 2). As for espionage during peace time, given the situation that there is no clear definition or provision in international treaties, there is the belief that this should be left to the domestic laws of the country involved.[28] Although the definitions of each country are not necessarily the same, when defining obtaining protected public information as espionage, this make the interpretation possible that espionage is punishable regardless if it was conducted outside of the country.

**Table 2 Location Requirement of Espionage (Intrusion/Surveillance) and Infringement of Sovereignty during Peace Time**

| Intrusion/Surveillance | | Infringement of sovereignty | Location requirement of espionage |
|---|---|---|---|
| Format | Territory | | |
| Physical | Inside adversary | Yes | Satisfies |
| Digital | | Yes | Most view that it does not satisfy |
| | Outside adversary | No | Does not satisfy |

Note: Surveillance accompanying digital intrusion means remote surveillance.
Source: Prepared by the author.

### 3. Cyber Surveillance Activities and Human Rights Laws (Violations of Privacy)

This section examines the problem of human rights laws that occur when communications carried out across borders are monitored through cyberspace. Assessment from the standpoint of espionage or infringement of sovereignty as addressed up to the previous section has absolutely no correlation when considering human rights laws. As touched upon in the first section, when Israel was found to have violated human rights treaties in the case of Legal Consequences of the Construction of a Wall in the Occupied Palestinian Territory, the ICJ did not touch upon the legality of occupation during war time. This is because a government authority cannot be exempted from its obligation to guarantee the human rights of individuals under its effective control, regardless if the war time occupation is legal or illegal. However, the issue of privacy rights related to cyber surveillance activities extends to both domestic communications and international communications, but the point of debate from the standpoint of the extraterritorial application of human rights laws is mainly international communications. This interest of this

[27] "Chinese Government Has Arrested Hackers It Says Breached OPM Database," *The Washington Post* (December 2, 2015).

[28] Wright, "Espionage and the Doctrine of Non-Intervention in Internal Affairs," p.13.

paper lies in the legal consequences of surveillance of such international communications, and therefore, for convenience, this paper will advance discussions based on the demarcation of transnational surveillance and extraterritorial surveillance.[29] This section widely introduces legislation and judicial precedents, and for this reason, examples from the three countries of the United States, United Kingdom and Germany are covered.

(1) Transnational Surveillance and Extraterritorial Surveillance

It is now becoming clear that various methods are used to carry out the surveillance of communications by the information agency of countries. Table 3 presents specific examples of transnational surveillance and extraterritorial surveillance. Here, this section will present a general outline of how surveillance activities conducted by major countries are being judged in terms of the relationship with these categories. The clauses used to assess whether surveillance activities are illegal under human rights laws are mainly Article 8 of the European Convention on Human Rights of 1950 and Article 17 of the International Covenant on Civil and Political Rights[30] of 1966.

> Article 8 of the European Convention on Human Rights[31]
> (Right to respect for private and family life)
> 1 Everyone has the right to respect for his private and family life, his home and his correspondence.
> 2 There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.
>
> Article 17 of the International Covenant on Civil and Political Rights
> 1 No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.
> 2 Everyone has the right to the protection of the law against such interference or attacks.

However, these human rights treaties do not necessarily apply worldwide. The extraterritorial application of these on individuals living outside the covered territory has been recognized only when certain conditions are satisfied. The point at issue that arises whenever an incident occurs that fulfills this condition is the clauses of Article 1 of European Convention on Human Rights and Article 2 of the International Covenant on Civil and Political Rights as below.

---

29 The types of surveillance indicated herein follow the paper below. Ashly Deeks, "An International Legal Framework for Surveillance," *Virginia Journal of International Law*, Vol. 55 (2015), p.9.

30 The covenant came into effect on March 23, 1976. Japan became a signatory on May 30, 1978 and ratified the covenant on June 21 the same year, with the covenant taking effect for the country on September 21 the same year.

31 The convention came into effect on September 3, 1953. *Basic Treaty Compilation 2016* (Toshindo, 2016) edited by Kimio Yakushiji, Shigeki Sakamoto, and Masahiko Asada was referenced for the Japanese translation.

Article 1 of the European Convention on Human Rights
The High Contracting Parties shall secure to everyone within their jurisdiction the rights and freedoms defined in Section I of this Convention.

Article 2 of the International Covenant on Civil and Political Rights
1 Each State Party to the present Covenant undertakes to respect and to ensure to all individuals within its territory and subject to its jurisdiction the rights recognized in the present Covenant, without distinction of any kind, such as race, colour, sex, language, religion, political or other opinion, national or social origin, property, birth or other status.
* Text underlined by the author

If it can be confirmed that transnational surveillance or extraterritorial surveillance discussed in this paper satisfy the above conditions, the victim that suffered negative effects from the surveillance can demand the reinstatement of their rights from the country that conducted the surveillance, irrespective of where they live or their nationality. There is a definitive difference between occupied Palestine cited above and these surveillance activities. For the former, in a physical context an occupation is taking place in war time and the occupying authorities for the entire area occupied must guarantee the freedom and rights stipulated in the the International Covenant on Civil and Political Rights in its relationship with the Palestinian people (excluding the portion in which the application is restricted based on state of emergencies of the public). For the latter, a country carrying out surveillance through cyberspace does not necessarily exert physical authority over people or things outside of the territory. Therefore, a country carrying out surveillance will tend to refute that the victim is located within its area of control or under its control, and thus, deny the extraterritorial application of human rights treaties.

**Table 3: "Transnational Surveillance" and "Extraterritorial Surveillance"**[32]

| |
|---|
| ● "Transnational Surveillance"<br>Foreign Nationals a and b residing in Country Z communicated via the Internet, but this communication between a and b by chance passed through the territory of Country X. The information agency of Country X acquired the data just as this communication between a and b passed through the territory of Country X. Or, Foreign National a residing in Country Z and Foreign National c residing in Country X communicated via the Internet. The information agency of Country X acquired the data just as this communication between a and c passed through the territory of Country X. |
| ● "Extraterritorial Surveillance"<br>Foreign Nationals a and b residing in Country Z communicated via the Internet, but this communication between a and b by chance passed through the territory of Country Y. The information agency of Country X acquired the data just as this communication between a and b passed through the territory of Country Y. Or, data stored inside the territory of Country Y was acquired. |

[32] For some time, the NSA has acknowledged certain surveillance activities were c (Footnotes) r exceed the scope defined in the memorandum of understanding between the United States and Germany, and later the extent of the involvement of the German authorities became an issue in Germany. "GCHQ and NSA Targeted Private German Companies and Merkel," *Spiegel Online* (March 29, 2014); "German Intelligence Under Fire for NSA Cooperation," *Spiegel Online* (April 24, 2015).

(2) Examples of Various Countries[33]

1) United States

The widespread surveillance of communications by the information agency of the United States dates back to September 2001 when the September 11 terror attacks occurred. At the time, the U.S. Government permitted the National Security Agency (NSA) to start new digital spying (signals intelligence) because of its failure to prevent the terror attacks and to prepare for terror attacks that could continue to occur. This decision was based on the understanding that espionage would be permitted as part of the Authorization for Use of Military Force (AUMF)[34] approved for the President by the United States Congress, which gave the NSA authority to intercept certain international communications in which the United States was the origin of the sender or receiver without obtaining a court order.[35] The international communications subject to this approval include those for which a rational reason exists to link them with members of Al-Qaeda, people cooperating with Al-Qaeda, or members of organizations working with Al-Qaeda. This spying activity is differentiated from terrorist surveillance programs, but details of this activity have not been made public.[36] This program was called the President's Surveillance Program together with these other spy activities and has been renewed around every 45 days by the President. However, around 2004, the Department of Justice began to indicate its doubts about the validity of the legal basis for this program. Following this, the program's framework was reviewed and since 2007 the NSA was forced to return to rules set forth under the existing domestic law called the Foreign Intelligence Surveillance Act (FISA).[37] The watershed moment came with the amended FISA[38] established in July 2008 following the Protect America Act of August 2007.[39] Following this, surveillance programs on Section 702 of FISA commonly called PRISM and Upstream were initiated. Each of these programs was conducted inside the territory of the United States and from the point that they targeted foreign nationals that could be reasonably deemed as outside the

---

33 France's Law Regarding International Electronic Surveillance Measures of November 30, 2015 (LOI No. 2015-1556 du 30 novembre 2015 relative aux mesures de surveillance des communications électroniques internationals) covers communications sent or received outside of France. On the other hand, the European Court of Human Rights has received a complaint that France's espionage related laws violate Article 10 of the European Convention on Human Rights (right to freedom of expression and information), but this complaint was received from an organization with offices in France, so it will be omitted from this paper. "Europe: Queue of Complaints Against Snooping Laws Grows by the Month," *Internet Policy Review* website (March 12, 2016), https://policyreview.info/articles/news/europe-queue-complaints-against-snooping-laws-grows-month/397

34 Joint Resolution to Authorize the Use of United States Armed Forces Against Those Responsible for the Recent Attacks Launched Against the United States, Public Law. No.107-40,115 Stat. 224 (September 18, 2001) (AUMF).

35 Kikuchi Shigeo "*Addendum: The President's Authority during a State of Emergency*" from "*Legislation concerning Military Authority in Major Countries*" of the Special Research Result Report for the National Institute for Defense Studies (2010) referenced.

36 U.S. Department of Justice, *Legal Authorities Supporting the Activities of the National Security Agency Described by the President* (January 19, 2006), p.5; Offices of Inspectors General of the Department of Defense, Department of Justice, Central Intelligence Agency, National Security Agency and Office of the Director of National Intelligence, *Unclassified Report on the President's Surveillance Program*, Report No. 2009-0013-AS (July 10, 2009), p.6.

37 Foreign Intelligence Surveillance Act (FISA) of 1978, 50 U.S.C. § 1801 et seq.

38 Foreign Intelligence Surveillance Act of 1978 Amendments Act of 2008 (Public Law 110-261).

39 Protect America Act of 2007, 50 U.S.C. § 1805a.

United States, these programs correspond to transnational surveillance per Table 3.[40] Surveillance activities under Section 702 of FISA at least nominally involved the courts from the point that they required the submission of annual reports from the Attorney General and Director of National Intelligence to the Foreign Intelligence Surveillance Court. Compared with the previous President's Surveillance Program that did not require court orders, these programs can be seen as forward progress. On the other hand, the surveillance targets of the NSA were no longer limited to Al-Qaeda and were revised to include foreign intelligence (information on international terrorism or weapons of mass destruction). In this sense, the NSA's surveillance activities were broadly expanded compared to the previous President's Surveillance Program.[41]

On the other hand, surveillance activities based on Executive Order 12333 (E.O. 12333),[42] although not covered in this paper, correspond to transnational surveillance per Table 3 because these surveillance activities are expected to be taking place outside of the United States.[43] Surveillance activities conducted by the NSA have been the subject of several lawsuits by human rights organizations based in the United States, but in each case these lawsuits were by domestic residents, and therefore, details will be omitted as they are not in the interests of this paper.

In either case, the U.S. Government shows reluctance about the extraterritorial application of human rights treaties in a positive light in its relationship with foreign nationals residing outside of its own territory.[44] Incidentally, certain improvements were made to surveillance activities under Section 702 of FISA from the standpoint of human rights protections following the release of "Presidential Policy Directive - Signals Intelligence Activities, Policy Directive 28" (PPD-28)[45] in January 2014. While acknowledging that signals intelligence is an essential method from the purpose of pursuing the interests of national security and diplomacy, PPD-28 requires that all targets of signals intelligence shall be respected and have their dignity maintained regardless of their nationality or whereabouts, and it specifies the stance that the handling of personal information must consider their interests according to privacy laws. In this manner, PPD-28 states various protections for targets of surveillance. For example, with regard to the retention period of personal information obtained, which is the biggest improvement under PPD-28, Section 4 of PPD-28 stipulates that personal information must be discarded after five years in principle, regardless if the person is a United States citizen or not. Nevertheless, it has been widely acknowledged that the

---

40 Privacy and Civil Liberties Oversight Board (PCLOB), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act* (July 2, 2014), p.21. According to the report, the difference between the two programs is that PRISM obtains "to" and "from" communications data from the email address of persons targeted for surveillance from the Internet Service Provider (ISP), while Upstream acquires not only "to" and "from" communication from the email address of persons targeted for surveillance like PRISM, but also an "about" communication data of third-party communication mentioned in the same email address, and this data is acquired from ISPs managing the "Internet backbone." Ibid., p.33,

41 Offices of Inspectors General, *Unclassified Report on the President's Surveillance Program*, p.31; PCLOB, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA*, pp.24-25.

42 Executive Order 12333- United States Intelligence Activities (December 4, 1981).

43 PCLOB, Report on the Surveillance Program Operated Pursuant to Section 702 of FISA, p.107.

44 Public Hearing Regarding the Federal Government's Surveillance Program Before the Privacy and Civil Liberties Oversight Board (PCLOB), Testimony of John B. Bellinger III (March 19, 2014), pp.2-3, https://www.pclob.gov/events/2014/march19.html

45 Presidential Policy Directive - Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435 (January 17, 2014) (PPD-28), http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities

personal information of foreign nationals subject to surveillance is retained longer than five years in actuality. As a result, a pessimistic outlook that essentially nothing has really been changed compared to previous programs can also be considered.[46]

(2) United Kingdom

Cases involving the United Kingdom represent good examples in which the legality of transnational surveillance was pursued. Ten human rights organizations in the United Kingdom filed lawsuits against the Investigatory Powers Tribunal from June to December 2013. Each of these complaints stated that the U.K. Government violated Article 8 of the European Convention on Human Rights mainly guaranteeing the privacy rights of communications because the Government Communications Headquarters (GCHQ) that serves as the information agency of the United Kingdom shared information obtained by the NSA and the GCHQ itself acquired communication data using a surveillance program (called Tempora) under the domestic law called the Regulation of Investigatory Powers Act (RIPA).[47]

Moreover, 7 of the 10 plaintiffs in these cases were human rights organizations based outside of the United Kingdom.[48] However, nearly all of these complaints were not allowed by the Investigatory Powers Tribunal, with the exception of a few,[49] and therefore, a group of the same plaintiffs filed a lawsuit with the European Court of Human Rights. Currently, this case is pending.

Furthermore, separate from these complaints, in 2015, 663 cases of similar nature were brought against the Investigatory Powers Tribunal, and 369 of these were complaints from a plaintiff based outside of the United Kingdom.[50] Of these 663 cases, 10 were first to proceed to trial, but the Investigatory Powers Tribunal determined that the U.K Government has no obligations under Article 8 of the European Convention on Human Rights with regard to communications in five plaintiff cases[51] that either were not present in the United Kingdom or were not based in the United Kingdom, refuting the jurisdictional rights of the court.[52] This case, too, is expected to be

---

46 Daniel Severson, "American Surveillance of Non-U.S. Persons: Why New Privacy Protections Offer Only Cosmetic Change," *Harvard International Law Journal*, Vol.56, no.2 (2015), pp.485-486.

47 The authority for surveillance activities under the Regulation of Investigatory Powers Act 2000 (RIPA) was carried over to Part 6 of the Investigatory Powers Act 2016 approved by Her Majesty the Queen on November 29, 2016.

48 Seven of the plaintiffs were human rights organizations based in Pakistan, the United States, Canada, Egypt, Hungary, Ireland, and South Africa. ECHR First Section, 10 Human Rights Organisations and Others against the United Kingdom, Statement of Facts, Application no.24960/15 (May 20, 2015), communicated to the UK Government on November 24, 2015, Appendix.

49 Investigatory Powers Tribunal (UKIPT), Case Nos: IPT/13/77/H (Claimant; Liberty), IPT/13/92/CH (Claimant; Privacy International), IPT/13/168-173/H (Claimant; (1)American Civil Liberties Union, (2)Canadian Civil Liberties Association, (3)Egyptian Initiative for Personal Rights, (4)Hungarian Civil Liberties Union, (5)Irish Council for Civil Liberties, (6)Legal Resources Centre), IPT/13/194/CH (Claimant; Amnesty International Limited), IPT/13/204/CH (Claimant; Bytes For All), Amended Open Determination (June 22, 2015), [2015] UKIPTrib 13_77-H 2, http://www.ipt-uk.com/docs/Final_Liberty_Ors_Open_Determination_Amended.pdf

50 The breakdown includes 94 cases from Germany, 12 cases from Italy and Sweden, 11 cases from France, 145 cases from the United States, and 33 cases from other countries (including 12 from Canada and 10 from Australia).UKIPT, Human Rights Watch Inc & Others v. The Secretary of State for the Foreign & Commonwealth Office & ORS, Judgment (May 16, 2016), [2016] UKIPTrib15_165-CH, p.5, para.12, http://www.ipt-uk.com/docs/Human_Rights_Watch_FINAL_Judgment.pdf

51 Ibid., pp.4-5, para.11.

52 The Investigatory Powers Tribunal has indicated it will hand down the same conclusion as this case for the several hundred complaints remaining that have yet to go to trial. Ibid., pp.24-25, paras.58, 60-63.

submitted to the European Court of Human Rights in the near future. In addition, the European Court of Human Rights is currently hearing similar cases, including Big Brother Watch v. United Kingdom,[53] and as such attention will be focused on the future findings of the court.

(3) Germany

Looking at arguments from similar cases in the past, the German Government can be categorized as having nearly the same stance as the United Kingdom's Investigatory Powers Tribunal. While this case involves the electromagnetic interception of satellite communications at a facility in Germany and not Internet communications, when a German national living in Uruguay and a Uruguayan national submitted a claim relying on Article 8 of the European Convention on Human Rights, the German Government denied the application of this article to this complaint citing that both plaintiffs were not in an area under the jurisdiction of Germany (case of Weber and Saravia v. Germany of the European Court of Human Rights[54]). The interception of the satellite communication debated in this case was conducted under the domestic law called the *Act* on Restrictions on the Secrecy of Mail, Post and Telecommunications (hereinafter G10 Act).[55] Given that the G10 Act is considered the legal basis for international communications over the Internet, the German Government is expected to argue that there exists no jurisdiction for communications outside of the territory of Germany, and particularly that of foreign nationals.

Furthermore, Bundesnachrichtendienst (BND; Federal Intelligence Service), the organization in charge of external intelligence gathering, not only conducts surveillance activities under the G10 Act, but has also been carrying out surveillance activities under the Bundesnachrichtendienst Act (BND Act).[56] According to Article 6 of the amended BND Act submitted in 2016, BND is placed in charge of strategic surveillance activities targeting the two-way communications of foreign nationals residing outside of Germany.[57] While the German Government has stated it will guarantee human rights following the provisions of the BND Act and the Basic Law for the Federal Republic of Germany regardless of the nationality of callers,[58] the true intention of whether this means a legal obligation in the strictest sense or whether this is merely a policy consideration

---

53 This complaint alleges that there is no legal basis domestically in the United Kingdom for the U.S. authorities to share information with the United Kingdom, and that the comprehensive interception of outside communication under RIPA 8(4) of GCHQ relies on a vague and unpredictable security concept and lacks balance; therefore, it is illegal as it cannot be considered intervention under the law per Article 8(2) of the European Convention on Human Rights. One of the plaintiffs is Dr Constanze Kurz, a researcher based in Berlin, Germany, and so the issue will be the extraterritorial application of this convention. ECHR Fourth Section, Big Brother Watch and Others against the United Kingdom, Statement of Facts, Application no. 58170/13 (September 3, 2013), communicated to the UK Government on January 9, 2014.

54 ECHR Third Section Decision Gabriele Weber and Cesar Richard Saravia against Germany, the Admissibility of Application no. 54934/00 (June 29, 2006), http://hudoc.echr.coe.int/eng?i=001-76586

55 Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz, Acts Restricting the Privacy of Correspondence, Posts and Telecommunications (Article 10 Act).

56 Gesetz über den Bundesnachrichtendienst (BND-Gesetz (BNDG)), Act on the Federal Intelligence Service (BND Act).

57 A Consolidated Version of the BND [Federal Intelligence Service] Act [BND-Gesetz] based on the bill that the German government published on June 28, 2016, Reporters Without Borders website, https://www.reporter-ohne-grenzen.de/fileadmin/Redaktion/user_upload/BNDGE_English_Translation_by_RSF.pdf

58 Note Verbale to the Office of the High Commissioner for Human Rights by the Permanent Mission of the Federal Republic of Germany to the Office of the United Nations and to the Other International Organisations in Geneva (October 21, 2016), Note No.: 424/ 2016.

similar to the United States' "Presidential Policy Directive - Signals Intelligence Activities, Policy Directive 28" (PPD-28) remains to be seen. United Nations special rapporteurs on human rights have raised concerns that there is no domestic legal framework in place for surveillance activities conducted by the German authorities outside of Germany.[59] This calls to mind that the German Government is not anticipating the extraterritorial application of human rights laws with regard to such extraterritorial surveillance.

(4) Assessment of International Institutions

The issue of whether or not privacy rights for communication apply to transnational surveillance and extraterritorial surveillance does not have a legal assessment in place given that there are still no international precedents covering this issue directly. In 2013, after some of the surveillance activities of the NSA came to light, General Assembly Resolution[60] "The right to privacy in the digital age," *A/RES/68/167* was adopted, and while the fears of each country were presented, this has yet to result in a clear finding of violation of international laws.

Although there is not necessarily an example of mass surveillance of Internet communications, the European Court of Human Rights case of Liberty and others v. the United Kingdom (July 1, 2008 ruling)[61] can be cited as a precedent for reference. This complaint involved the interception of two-way communications (telephone calls, fax transmissions, emails) of human rights organizations based in the United Kingdom and Ireland by a facility run by the Ministry of Defence of the United Kingdom. The European Court of Human Rights found that procedures of how the data acquired through this interception would be later processed was not fully made public by the United Kingdom, and thus, it represented interference in communication in violation of Article 8 of the European Convention on Human Rights. If the ruling of the court regarding this matter were to be used as an example of the mass surveillance of Internet communications, it is believed that there is room to bring to trial whether or not there was illegal or arbitrary interference in the privacy rights of victims and to acknowledge that the government jurisdiction covers exterritorial foreign nationals.

## 4. Application of Human Rights Laws to Cyber Surveillance Activities

The previous section examined surveillance activities through cyberspace conducted by major countries with a focus on transnational communication. Given the difficulty of obtaining primary sources, this paper was not able to fully consider extraterritorial surveillance because the examination leaned mostly toward transnational surveillance.[62] This issue will be for future consideration. Table 4 below categorizes the application of human rights treaties for each type of

---

59 Letter to Germany's Ambassador to the UN in Geneva by the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression & the Special Rapporteur on the Situation of Human Rights Defenders & the Special Rapporteur on the Independence of Judges and Lawyers (August 29, 2016), p.7, http://www.ohchr.org/Documents/Issues/Opinion/Legislation/OL_DEU_2.2016.pdf

60 A/RES/68/167 (December 18, 2013), preamble; A/RES/69/166 (December 18, 2014), preamble.

61 ECHR Forth Section, Liberty and Others against the United Kingdom, Application no. 58243/00, Judgment (July 1, 2008).

62 Douwe Korff, "Note on European & International Law on Trans-national Surveillance Prepared for the Civil Liberties Committee of the European Parliament to Assist the Committee in its enquiries into USA and European States' Surveillance," European Parliament, Committee on Civil Liberties, Justice and Home website (August 23, 2013).

surveillance activity conducted by the countries examined in this paper.

First, in the case of the physical domain, although not in all cases, when certain conditions are met the extraterritorial application of human rights treaties has been acknowledged for operations or security activities conducted by an occupying authority during war time or foreign military in an extraterritorial domain per A, and already several international precedents exist. In addition, precedents do exist where extraterritorial application was acknowledged for transnational activities per B. The example quoted in (1)B in Table 4 involves a case where a soldier fired from within their own territory, but the bullet hit a foreign national in an area outside this territory causing a serious injury (case of Andrew v. Turkey of the European Court of Human Rights; ruling handed down on June 3, 2008[63]). At the time of the incident, the location where the shot was fired was not under the control of Turkey, the home country of the soldier who fired the shot, but the court concluded that the injury incurred by the victim resulted from direct and immediate results of the said solder shooting from close range, and thus, the victim should be deemed as being in an area under the jurisdiction of Turkey at the time of the incident. Pressing this belief, there is the possibility to affirm the presence of the jurisdiction of the surveillance country similar to transnational surveillance as ([2]B of Table 4) through cyberspace. As (1)B represents the authority of a state over people and (2)B is authority over data, there are differences observed between the two. Also, compared to (1)B where the act was completed for the first time when the round impacted the person outside the territory, (2)B involves all acts, from data acquisition, opening and analysis, to retention and disposal, being completed inside the country. However, despite these differences, the condition of (2)B being discussed in the context of the extraterritorial application of human rights laws is because the data of the communication belongs to the individual performing the communication. Consequently, if the condition of (2)B, too, can be said to have caused the damages of the victim (violation of privacy) as a direct and immediate result of surveillance activities by a certain country, it is believed there is no hindrance to deeming the victim as being inside the jurisdiction of the surveillance country.

On the other hand, as for extraterritorial surveillance through cyberspace ([2]A of Table 4), too, in terms of extraterritorial authority, even if the same as physical violence ([1]A), when the location of the data (Country Z in Table 3) and the location of data acquisition (Country Y) are different, countries reluctant to apply human rights treaties may refute that the complainant (victim) was inside the country's jurisdiction. Nevertheless, similar to transnational surveillance, when damages (violation of privacy) incurred by the victim are the direct and inevitable consequence of surveillance activities of a certain country, in a digital meaning, the victim should be considered to be none other than inside the jurisdiction of the surveillance country.

Whereas, if the meaning of the word jurisdiction stipulated in human rights treaties is to be limited to the physical context only, while carrying out the effects of digital authority over data, the conclusion will always be the absence of jurisdiction by the government, and the privacy rights of not only the targets of the surveillance, but those affected incidentally during the process of surveillance activities will never be protected or respected. However, if a certain country has the technology or ability to actually acquire omnipresent data in the world, it will be important to make efforts to explain the effects of this authority following a modern context.

---

[63] ECHR Fourth Section, Andreou against Turkey, Application no. 45653/99, Judgment (October 27, 2009), http://hudoc.echr.coe.int/eng?i=001-95295

**Table 4 Types of Activities Targeting Extraterritorial Foreign Nationals and Application of Human Rights Treaties**

| | | A (extraterritorial activities) When activities are conducted outside of the country's territory | B (transnational activities) When activities conducted inside the country's territory impact another country |
|---|---|---|---|
| (1) Physical domain | | | |
| | Examples of activities targeting extraterritorial foreign nationals | • Occupational administration of occupying authority during war time<br>• Activities of foreign military in host country | • Shooting of person outside the territory |
| | Application of human rights treaties | Applied | Applied |
| (2) Cyberspace | | | |
| | Examples of activities targeting extraterritorial foreign nationals | Extraterritorial surveillance<br>U.S.: E.O 12333<br><br>U.K.: Section 7 of ISA | Transnational surveillance<br>U.S.: Section 702 of FISA<br>Germany: Article 5 of G10 Act and Article 6 of BND Act<br>U.K.: Section 8(4) of RIPA |
| | Application of human rights treaties (protect confidentiality of communications) | Viewpoint of experts divided | Viewpoint of experts divided |

Note 1:
- Surveillance under Section 702 of the Foreign Intelligence Surveillance Act is conducted inside the territory of the United States to obtain "foreign intelligence" targeting "non-United States citizens." It is commonly called PRISM and Upstream.
- Surveillance under the Act on Restrictions on the Secrecy of Mail, Post and Telecommunications (Basic Law for the Federal Republic of Germany Article 10 Relevant Laws; G10 Act; Gesetz zur Beschränkung des Brief-, Post- und Fernmeldegeheimnisses, Artikel 10-Gesetz) is conducted inside the territory of Germany targeting "international electronic communications."
- Surveillance conducted under the Federal Intelligence Service Act (Bundesnachrichtendienstgesetz [BND Act]) is conducted inside the territory of Germany targeting "two-way electronic communication between foreign nationals living in foreign countries."
- Interception of "external communications" under the Section 8(4) of Regulation of Investigatory Powers Act 2000 (RIPA) is conducted inside the territory of the United Kingdom. It is commonly called Tempora.
- Surveillance under Executive Order 12333 of December 4, 1981 (E.O12333) refers to counter-intelligence activities conducted outside of the United States.
- Section 7 of the Intelligence Services Act 1994 (ISA) involves acquiring information through electromagnetic transmissions using equipment located outside of the territory of the United Kingdom.

Note 2:
1. "Physical domain" refers to activities targeting foreign nationals residing outside the territory.
2. "Cyberspace" refers to activities targeting the communications data of foreign nationals residing outside the territory. As for 2., the country where the foreign national resides and the country where the communication data are not necessarily the same.

Source: Prepared by the author based on UK Home Office, Equipment Interference: Code of Practice 2016 (January 2016): ECHR Press Unit, "Factsheet: Extra-territorial Jurisdiction of States Parties to the European Convention on Human Rights," ECHR website (February 2016), etc.

## Conclusion

This paper examined surveillance activities conducted by information agencies through cyberspace mainly from the three issues of espionage, infringement of the sovereignty of other countries, and human rights laws. It also considered the issue of how to assess these issues as they relate to the concepts of conventional international laws.

This paper began by examining the mass surveillance activities conducted by the NSA of the United States from the point at issue of espionage during war time given that they were initially considered a part of a war time operation in September 2001. This paper confirmed that for these activities to be considered as conducted during war time they had to satisfy the location

requirement and the false pretence spying requirement, but theories such as the *Tallinn Manual* strictly adhere to the location requirement, and therefore, conclude that there is an extremely low possibility that remote surveillance activities through cyberspace are considered espionage under international laws. Although prominent theories[64] are seen that permit surveillance activities through cyberspace during peace time because there are no legal provisions banning them, when assuming this view, it is believed there is little real meaning in criticizing the perpetrating country carrying out a cyber attack that steals confidential information by penetrating the information system of another country based solely on this belief, even if the format constitutes infringement of sovereignty. There is even no concern for infringement of sovereignty in the case where a country acquires data from international communications exchanged between another country and its foreign embassy inside the country.

However, when discussing the legal aspects of a state exercising its authority (jurisdictional rights) today, it is believed there is room for considering whether there is qualitative difference such as whether this takes place using physical means or digital means. Rather, it is only natural to consider that performing such acts without the permission of the other country is an infringement of that country's sovereignty, even if this was conducted using a digital or virtual location.[65] Given this situation, it is believed that refuting espionage based solely on the strict interpretation of the location requirement lacks persuasiveness.

On the other hand, this paper confirmed that surveillance activities through cyberspace potentially bring up the issue of the violation of privacy rights even though they are legal under international laws and even when conducted as a just operation under international laws. In particular, this paper found that when a country conducts surveillance of communication data of foreign nationals residing outside of its territory it tends to be pessimistic toward guaranteeing and respecting rights under human rights laws even through it is easy to obtain such data. As a basis for justifying this position, the country conducting surveillance will explain that the foreign national outside of its territory is not located within its area of control or under its control. Is "jurisdiction" as stipulated in human rights treaties really a quality that cannot be defined according to a digital context? With regards to human rights laws, too, it is important to define conventional concepts from the digital and virtual standpoint of cyberspace. As seen in this paper, at the current point in this direction is not necessarily uniform in theory or in practice. Security in cyberspace has sharply grown in importance, and for Japan, too, an urgent task will be storing knowledge on international laws concerning surveillance activities in cyberspace, including the three points at issue covered in this paper, based on an understanding of worldwide trends in both theory and practice.

---

[64] Julius Stone, "Legal Problems of Espionage in Conditions of Modern Conflict," in Stanger, *Essays on Espionage and International Law*, pp.29-43;Stefan Talmon, "Tapping the German Chancellor's Cell Phone and Public International Law," *Cambridge Journal of International and Comparative Law* website (November 6, 2013); Katharina Ziolkowski, "Peacetime Cyber Espionage: New Tendencies in Public International Law," in idem, ed., *Peacetime Regime for State Activities in Cyberspace* (NATO CCE COE, 2013), pp.425-464; Schmitt, *Tallinn Manual*, p.30; Deeks, "An International Legal Framework for Surveillance," pp.301-302.

[65] Professor Schmitt states that the 2014 cyber attack on Sony Pictures Entertainment (SPE) is an infringement of the United States' sovereignty because North Korea was responsible for the attack.Michael Schmitt, "International Law and Cyber Attacks: Sony v. North Korea," *Just Security* website (December 17, 2014), https://www.justsecurity.org/18460/international-humanitarian-law-cyber-attacks-sony-v-north-korea/