Abstract

In early 2016, the Republic of Korea enacted the "Anti-Terrorism Act for the Protection of the Korean People and Public Safety" and provided the testimony to counter terrorism crimes by international terrorist groups including IS. On the other hand, the legislative response to cyber terrorism, which is more important than the traditional terror crime in terms of the severity and repeatability of the damage, has been insufficient. In this situation, the government of the Republic of Korea deliberated and voted on the “National Cyber Security Bill” in December 2016. Despite the existence of the Anti-Terror Law, there may be criticism that the enactment of a special law for cyber terrorism is unduly violating the fundamental rights of the people. Therefore, it is necessary to first examine whether a separate legislative response is required because cyber terrorism has some difference from traditional terrorism. In this paper, cyber terrorism originated from traditional terrorism, Since the substance is a totally different crime, we need to respond to it separately from terrorist crime, confirming that the legitimacy of the enactment of the special law is guaranteed. In addition, if the necessity is recognized, the special law has the possibility of restricting the freedom of expression in the basic rights of the people, especially in the online space. Therefore, the philosophical basis of the restriction is examined. In this study, It was found in the fundamental purpose of the state and described it as a specific expression of the obligation to protect the basic rights of the state. In addition, the hypothesis that cyber terrorism can be regarded as a new type of risk source proposed by Ulrich Beck also emphasized the necessity of preemptive response before the occurrence of cyber terrorism in response to the risk source. Of course, can not infringe the essential content of the basic rights in the process.

[Keywords] Cyber Terrorism, Terrorism, Law of Prevention of Cyber Terrorism, Freedom and Safety, Prevention of Crime

1. Introduction

In early 2016, the Republic of Korea enacted the “Act On Anti-Terrorism For The Protection Of Citizens And Public Security” and provided the testimony to counter terrorism crimes by international terrorist groups including IS. On the other hand, there was no legislative response to cyber terrorism, which is more important than traditional terrorist crimes in terms of severity and repeatability. In this situation, the government of the Republic of Korea deliberated and voted on the "National Cyber Security Bill" in December 2016. Despite the existence of the Anti-Terror Law, there may be criticism that the enactment of a special law for cyber terrorism is unduly violating the fundamental rights of the people. Therefore, since cyber terrorism has some differences from traditional terrorism, it is necessary to first examine whether a separate legislative response is necessary. In addition, if the
necessity is recognized, the special law may limit the freedom of expression in the basic rights of the people, especially in the online space. Therefore, it is necessary to examine the philosophical basis of the restriction, will review the matter.

2. Concept and Characteristics of Cyber Terrorism

It is not easy to distinguish between traditional terror crime and general violent crime[1], just as it is not easy to define terror crime, it is not easy to define the concept of cyber terrorism because of the mixture of real space and cyber space. Generally, cyber terrorism is understood as “direct sabotage or attack on hardware or software, website or information communication infrastructure on cyberspace such as hacking, virus infection, DDoS”. If so, what characteristics of cyber terrorism should we consider to limit the basic rights of the people in order to prevent cyber terrorism.

To examine the characteristics of cyber terrorism, one must examine what is different from traditional terrorism. Terrorism is “an act intended to interfere with the exercise of the power of a state, local government or foreign government, to do nothing without duty, or to intimidate the public”[2]. In other words, the conceptual elements of traditional terrorism are: (i) threats to the use or use of violent acts; (ii) political, national and ideological motives as elements of excess subjective constitution; and (iii) separation of victims and the masses as objects of terrorism[3].

However, even if cyber terrorism is derived from traditional terrorism, it is questionable whether it can be viewed as a sub-form of traditional terrorism. First, the traditional forms of terrorism are the core elements of the use or use of violent acts, while cyber terrorism is not a hard infringement, but a malicious infringement of hacking, viruses, malicious codes and so on. Second, while traditional terrorism requires political purpose as an excess subjective component in addition to the intention of crime, cyber terrorism does not require an over-subjective constitutional factor. Therefore, cyber terrorism on the subjective side is different from traditional terrorism. The traditional forms of terrorist crime are not aimed at the illegal acts of violence themselves, but rather by the use of acts of violence to achieve their specific purposes[4]. In addition, those who are directly victimized by such acts of violence, The recipient is clearly distinguished. However, cyber terrorism is often aimed at state-based facilities such as power, telecommunications, and finance. If the infrastructure of the country fails to operate normally due to cyber terrorism, not only direct victims but also the members of the society who enjoy the infrastructure are directly affected. It is different from terrorist crime. Therefore, even if cyber terrorism appears in traditional terrorism, it is not necessary to consider it as a subordinate concept, and it is reasonable to consider it as a separate form of crime.

The next issue to consider is the subject of cyber terrorism. In other words, can it be the subject of cyber terrorism as well as non-state actors such as individuals. There is no reason to deny the state actor’s terrorist crime subjectivity in the traditional form of terrorism, so there is no need to deny the subjectivity of the state in cyber terrorism. In recent years, armed conflicts as a form of total war between countries are rare, and there is no reason to exclude the state from the subject of cyber terrorism because there are many dispute resolution methods such as cyber terrorism and low intensity conflict.

Finally, it is necessary to examine the Internet use of terrorist groups. Recent national security is a trend that focuses on comprehensive security threats. The UNODC recognizes[5] the inherent security risks of cyber terrorism and not only moves toward a comprehensive policy approach, but also recognizes cyber terrorism as an inherent security threat, It is approaching as a policy countermeasure rather than as a dogmatic[6]. In other words, the international community including the UNODC sees cyber terrorism as a cyber terrorism, as well as cyber terrorism, which causes cyber
terrorism to hurt public goods such as state infrastructure. Therefore, the problem of terrorist criminals such as internet use is not a traditional paradigm of international security-security, domestic-security but a representative example of the approach of both. Therefore, acts such as Internet use of terrorist organizations are sub-types of cyber terrorism. It is reasonable to approach.

3. Legal Basis of Cyber Terror Prevention

We examined the concept and characteristics of cyber terrorism and examined the necessity of separate legislation due to the difference from general terror crime. Because cyber terrorism has difficulty in proving the seriousness of the damage and proving the damage, proactive prevention is an important task rather than a posterior response. In terms of the prevention of cyber terrorism, how can the judicial system prevent real and direct infringements against the law? According to the traditional criminal justice system composed of the category of infringement crime, the cyber terrorist act has a logic structure that it can not be penalized without criminal law if there is no special clause because there is no direct infringement against the individual or the state. However, the punishment of a criminal after a terrorist crime has actually occurred can not be more than a retaliation against an actor. Therefore, despite the fact that no actual damage has occurred, it is necessary to consider the grounds for punishing cyber terrorism and further preliminary action. It is also necessary for the state to consider what legal basis it should have in order to curb terrorist crime. If so, we must first derive the evidence from the Constitution. In other words, the law aiming at the prevention of terrorist crime should examine how the Constitution relates to the basic rights of the people, and thus the state that aims to protect the lives and property of the people, it can guarantee the constitutionality of legislation.

3.1. National obligations for crime

3.1.1. The legitimacy of state existence and the duty of crime prevention

One of the characteristics of the September 11 attacks in 2001 was to awaken the desire for fear of life and security of life that was inherent in the abyss since the birth of mankind. Of course, this perception is not caused by 9/11 terror. The history of mankind itself is a history of pursuing its own safety and the maintenance of life. The discussion of "safety of life" is a theme that applies to members of underdeveloped nations or members of Western advanced nations. If so, what is this "safety" and what is the state to do to enjoy this safety.

After the introduction of the notion of sovereignty by the French political philosopher Jean Bodin in the 16th century, the concept of personal safety began to develop in relation to the state, beginning with Thomas Hobbes[7]. As Hobbes saw Europe at the time of the war in disintegration and freedom of religion, the natural state of man was in a state of struggle against all men of the so-called universes, so overcoming these situations of death and disorder is at the top of all powers The Leviathan. That is, all human beings sign a social contract entrusting their rights to Leviathan for survival, and this "safety" is the basis of state power to protect the lives and bodies of individuals threatened in disorder.

John Locke goes further here and assumes the importance of a nation that protects the life and personal safety of an individual, and that country, when securing peace and security in a state where the exercise of power is restricted by law. In the social contract theory, individuals are obliged to transfer their natural right to the state under the premise that the state guarantees the safety of life and body, and the state has the obligation to create an environment in which its members can live safely and peacefully. Therefore, the state is recognized not only as its existence itself, but also the justification of its existence in preventing the life, health and property rights of its members from
being infringed by other individuals or organizations and maintaining the order of society[8].

3.1.2. Obligation to protect national fundamental rights and prevent crime

Fundamental rights have the characteristics of (i) the passive defense of state power and (ii) the active formation of state order[9]. The duty of the state to protect the lives and property of the people from cyber terrorism is derived from the objective order which is the latter of the fundamental rights. The fundamental right as the basic element of this objective order is to protect the nation from the crime including cyber terrorism, to protect them.

The basic right of the classical sense meant a basic right to protect the passive position of the nation, that is, the life and property rights of the people, from the state, not from the state. In modern society, however, basic rights are required to take an active role, not just passive status. The State must inevitably limit the fundamental rights of third parties to protect the basic rights of the people from cyber terrorism. In this regard, the relationship between the state and the people, and the conflicting values of freedom and security, always means a tension. Therefore, it is best to resolve the tension by establishing clear laws that everyone can understand. Considering the various forms of cyber terror crime that can be manifested in various ways, it is the responsibility of the state to abide by the existing system of legal system and to dismantle the maintenance of institutional and legal systems to prevent future crimes.

3.2. The rising of risk society and crimes of terrorism

The German philosopher Georg Wilhelm Friedrich Hegel described in 1821 his “Grundlinien der Philosophie des Rechts” that “criminal law depends on the state of society in that age and its time”. As such, criminal law is influenced by social change. Since the 1970s, ROK society has achieved rapid economic growth, the development of science and technology, and the democratic development that is hard to find anywhere else in the world. However, this compact modernization brought about negative aspects, such as large-scale environmental pollution, large-scale collapse and explosion, industrial accidents, and the emergence of various types of violent crimes that were not seen before in the 1950s. Ulrich Beck has been involved in the development of so-called “neue großrisiken”, a side effect of nuclear, chemical, ecological and genetic engineering technologies, and new types of crime(environmental, economic and terrorist crimes) Society as a Risk society. And ROK society is a representative aspect of the dangerous society proposed by Beck[10].

Due to the economic growth and development of science and technology, our society has reduced the traditional and natural risks compared to the 1950s when the criminal law was enacted. However, this 'objective safety' has increased, but 'subjective anxiety' about the new mass danger perceived by ordinary citizens in the dangerous society and the cruelty of recent violent crimes and hate crimes significantly threatens objective safety. Because of this, the public in our society demands an active role for new threats to the state and the law, especially the criminal law. In this context, the paradigm of the state is the Prevention country(Präventionsstaat), which aims at minimizing the intervention of the penal rights, and at the same time, in the 19th century liberal legal state, to Safety Country(Sicherheitsstaat)[10]. As the national paradigm shifts, the function of the criminal law is required to change the direction to prevent mass danger and to secure safety. The discussion of Risk Criminal Law(Risikostrafrecht) begins here. The dangerous criminal law means that criminal law should actively intervene in order to control these modern risks, since it can not solve the problems of the 21st century that are newly raised with the spiritual tools of the 18th century[11]. In particular, the traditional functions of the criminal law in new types of crimes such as economic crime,
environmental crime, terrorist crime and drug crime are no longer limited to maintaining social order. Therefore, And to control the overall social structure by upgrading the strong intervention and the related penalties in the pre-crisis period before the emergence of the crisis (Gefährdung)[10].

Terrorist crimes, including cyber terrorism, can also be discussed on the same line. Terrorist crimes that coincided with the history of mankind existed before discussing the regulation of terrorist crime in modern society. However, in the 1970s and 1980s, due to urbanization and technological development due to changes in social structure, cyber terrorism in modern sense is different from classical terrorism. In addition, since cyber terrorism is more illegal than general criminal offense, there is a need to regulate pre-terrorist acts as well as enforcement actions before the stigma of legal interests becomes real.

4. Considerations for Establishing Cyber Terror Prevention Law

4.1. Comparison of freedom and safety

National liberty can be violated at any time by the State or a third party. Therefore, the State should endeavor to guarantee the freedom of the people based on the purpose of existence and the obligation to protect fundamental rights in the Constitution. There is also the opinion that demanding freedom from the state and safety from others at the same time is an impossible proposition[12]. As John Locke argues, always guarding the duality of state power, state power plays a role in protecting the safety of the people, but paradoxically there is also the danger of threatening the fundamental rights of the people themselves. Freedom from these paradoxes is not a concept of conflicting or conflicting national freedoms and security, but securing personal security when the state power is limited by law and guarantees the survival and well-being of the social community. Therefore, the state power must have clear laws backed up to guarantee the safety of the people.

4.2. Limitations in cyber terror crime prevention

What needs to be considered in responding to cyber terrorism is how to resolve the relationship between freedom and security, such as the two sides of a coin. Through the prevention of cyber terrorism, the state can fulfill its duty to protect basic rights to prevent infringement of the life and property rights of the people from other countries or autographs, but inevitably limits the basic rights of the people inevitably. Therefore, we should consider whether the law aiming at the prevention of cyber terrorism can give some control to the state to prevent it from unduly infringing on people's fundamental rights. If the contents of the law aiming at the prevention of cyber terrorism infringe on the fundamental rights of the people excessively, there is a possibility to violate the principle of proportionality. On the contrary, in order to guarantee the basic rights of the people, Of the total number of deaths, it is not possible to substantially guarantee the obligation to protect the basic rights of the state as a prevention of crime. The Constitution Law stipulates that “all the freedoms and rights of the people may be restricted by law only when necessary for national security, order maintenance or public welfare, and that the essential contents of freedom and rights can not be infringed even when restricted”. In this way, it is recognized that the rule of law also restricts the basic rights of the people to unlimited, but in certain cases. Therefore, even if the basic rights of the people are restricted due to national security, order maintenance, public welfare, etc., the basic rights can be restricted only within the purpose, method and limit set by the Constitution Law.

5. Epilogue

In this paper, we examine whether the law is necessary and what grounds it is, in spite of
the Anti-Terrorism Act in accordance with the National Cyber Security Act. Cyberterrorism originates from traditional terrorism, but in reality it is a totally different crime. Therefore, it is necessary to deal with terrorism separately from crime. If so, prevention of cyber terrorism is also important, which may inevitably limit the basic rights of the people. In this study, we found that the basis of the restriction was found in the fundamental purpose of the state for the prevention of crime, which is expressed specifically by the obligation to protect the basic rights of the state. In addition, the hypothesis that cyber terrorism can be regarded as a new type of risk source proposed by Ulrich Beck also emphasized the necessity of preemptive response before the occurrence of cyber terrorism in response to the risk source. Of course, can not infringe the essential content of the basic rights in the process.

6. References

6.1. Journal articles


6.2. Books


6.3. Additional references