Abstract

Cyber terrorism has emerged internationally since the mid-1990s when networking began to take place. However, in most cases, the damage was localized by hacking the network of related organizations and hacking for economic gain in order to inform individual or organization claims. However, as we look at the year 2015, the spread of computer networks and the dependence of the infrastructure on this network are not comparable to those of the 1990s. The fact that major broadcasting companies and financial institutions are temporarily paralyzed by the cyber terrorism incident on March 20, 2013 and June 25, 2013, revealing the vulnerability of the social infrastructure, reveals the danger of cyber terrorism. It is imperative to prepare countermeasures.

In particular, major social infrastructures and services of the modern countries including Korea are gradually being connected and controlled by ICT technology. In case of facility and service failure caused by unauthorized access to such facilities, the impact on the normal operation of other core facilities may become very large. In particular, there is a serious problem in that the infringement of the network connecting the national infrastructure such as communication, finance, water supply, power, etc. and controlling each information system may cause obstacles in the whole country rather than simple cyber infringement. In this way, cyber terrorism cases against the state infrastructure have been actualized. In addition to the cases described above, there are many cases of cyber terrorism in Korea. In recent years, cyber terrorism targeting Korea has tended to occur in order to impose damage to national infrastructure such as GPS, telecommunications, broadcasting, and financial facilities. This is because the risk of individual criminal activity to threats to national security. In the ICT era, cyber terrorism is a new threat to national security and it is a new type of risk source that is discussed in modern risk society. Therefore, there is a need to cope with criminal policy and legislation.

[Keywords] Cyber Terror, Terror, National Security, Change of National Security Situation, Due Process

1. Intro

The development of science and technology in late industrial society has changed human civilization rapidly. Particularly, due to the development of ICT technology, the world has lowered the barriers between countries to the point that the word “global village” is inexplicably brought about the free movement of manpower money and technology. This has a positive ripple effect such as economic co-growth, propagation of democracy and promotion of human rights come. On the other hand, not only economic damage such as abuse and abuse of nuclear energy caused by science and technology, serious environmental crime, unpredictable large-scale accident, and crimes that abuse ICT technology, but also adverse effects that can impose human life and body, it can be said that it is the dark side of. In particular, crime using ICT technology, such as cyber terrorism, has already spread to the masses through the media, and its severity is a direct threat to a
country's infrastructure beyond the level of individual criminal activity, it is changing situation.

Cyber terrorism has emerged internationally since the mid-1990s when networking began to take place. However, in most cases, the damage was localized by hacking the network of related organizations and hacking for economic gain in order to inform individual or organization claims. However, as we look at the year 2015, the spread of computer networks and the dependence of the infrastructure on this network are not comparable to those of the 1990s. The fact that major broadcasting companies and financial institutions are temporarily paralyzed by the cyber terrorism incident on March 20, 2013 and June 25, 2013, revealing the vulnerability of the social infrastructure, reveals the danger of cyber terrorism. It is imperative to prepare countermeasures.

In addition, Korea has not only these internal risk factors but also risk factors according to the security environment surrounding the Korean Peninsula. That is, political and military conflicts with neighboring countries surrounding the Korean peninsula, as well as North Korea's political and military threats that have continued since the division. The problem is that Korea's external threat is not only caused by traditional security risks but also by new types of security risks. While the traditional concept of security is to look at security only by military threats, the new form of security concept, even if securing political and military security, is not reflective of its security. It is a concept that measures the degree of security by measuring the comprehensive quality of human life such as human rights, social development, economy, health and environment. Therefore, it is necessary to analyze Korea's security situation not only from the external perspective of strengthening the national security capacity but also the minimum conditions in which the members of society can live like human beings.

2. Diagnosis of the Security Situation in Korea

2.1. Domestic factor (ⅰ) - contrast as a leading country in ICT technology

Rapid changes in modern society can be summarized as globalization and informatization. As I mentioned at the beginning, modern society has achieved political and economic development according to the progress of globalization, but the fundamental driver of globalization is due to ICT technology[1]. This information society is characterized in that capital for creating added value becomes knowledge and information, not real capital, like industrial society, and the essence of labor for production changes into mental activity rather than physical and physical labor. In addition, it is possible to spread knowledge freely beyond time and space by ICT technology, and it is also characterized by becoming a networked society beyond time constraints in the fields of politics and economy. With the advent of the information age characterized by this knowledge information society and network society, humanity is experiencing a breakthrough. In other words, the development of e-government and e-commerce, free communication due to the spread of the Internet, and the cultivation of political consciousness as a result are gifts not only for the people of a certain country but also for our people living in this era. In addition, the development of ICT technology accelerated the production and distribution of information, facilitating the disclosure of information, and disrupting the paradigm that governments or small numbers of people used to control or monopolize information. Another characteristic of informatization is that the state loses its dominant position of monopoly of information, while the capacity of non-state actors such as civic groups and individuals is strengthened. In summary, the use of ICT technology, rather than the accumulation of wealth by the human labor force of the past, is the production and redistribution of social goods, so that such digitized information has become a source of social wealth and a tool of new power. In Korea, social infrastructure such as public transportation, water supply, sewerage, telecommunications, and finance are integrated and managed by ICT technology, electronic financial...
transactions are activated in private transactions, and ICT. It is hard to imagine that there is no SNS utilizing technology, so our society is highly dependent on ICT technology[2]. Digital information, however, has emerged as a new economic, cultural and political value, but at the same time, it is the emergence of another new source of danger through industrialization[3]. In other words, all of the social organization is linked to the aggregation point of information and communication technology, and not only the structural weakness is highlighted, but also personal deviations (cyber terrorism, online pornography circulation, defamation, copyright infringement, Fraud, etc.) began to increase. As ICT technology has both the opportunity to make dramatic development in human civilization and the danger to threaten human life, there is a need to manage it systematically in terms of risk.

2.2. Domestic factor - a society in which new forms of mass risk coexist
According to a recent survey, the safety level of our society is not of high quality. In other words, the members of our society are perceived to have anxiety about various fields such as national security, natural disasters, environmental pollution, various talents, and new crimes. According to the survey, there is an anxiety about national security and crime occurrence without distinction between men and women. However, there is an anxiety about unpredictable dangers in modern scientific and technological society, such as natural disasters, environmental pollution and human resources. Our society has a social infrastructure based on the developed ICT technology as described above, and the incidence of crime is significantly lower than that of advanced countries. Where does this anxiety come from? Is this anxiety merely a consequence of the subjective feelings of the members of the society or a defense instinct based on the dangerous media coverage, or is it actually an uneasy society? To find answers to these questions, it is necessary to review the concept of risk society presented by Ulrich Beck[4].

2.2.1. Concept and characteristics of dangerous society
It is difficult to uniquely define the concept of a dangerous society. According to Beck, a dangerous society is a society in which the dark aspects behind human social development are gradually leading social discussion, that is, a contradictory society in which the scientific civilization designed for human convenience threatens human existence itself. According to Beck, as modernization dismantled the feudal society of the nineteenth century and created an industrial society, today's modernization dismantles the industrialized society of the 20th century and dismisses the industrial society as "a modern society, A continuation of the continuous development of"[5]. In other words, he defines a dangerous society due to the change of society due to the change of the times. However, the notion of such a dangerous society is so abstract that it is unclear what the dangerous society Beck would like to discuss. 

Eric Hilgendorf pointed out that the concept of risk society proposed by Beck is quite unclear in terms of philosophical, sociological and legal aspects. He pointed out that risk society is the destruction of the natural environment due to the rapid development of science and technology in late industrial society And threats to human survival, the disabling of the human sense system, and the arrival of fear society as a result of the assurance of industrial progress and the collapse of community consensus[6].

The concept of this abstract dangerous society became a hot topic in the Chernobyl nuclear power plant in 1986. Since the development of nuclear power in the West, the introduction of advanced science and technology, including global ecological risk, nuclear abuse and abuse, and social reflection on the danger have started in earnest in the 1970s and early 1980s. I was not interested in this[7]. However, in the late 1990s, the Sungsu Bridge, the collapse of Sumpung Department Store, and the oil spill in Taean have led to the recognition of the possibility that a major catastrophe may occur due to the adverse effects of these technological developments. Discussions about risk have begun.
So what is the new form of risk that Beck suggests? There are two views in the country about the risk concept of Beck. In other words, it is a discussion of how to distinguish between traditional forms of risk and new forms of mass risk. (1) Beck distinguishes 'risk' from past threats (Gefährdung) and a new form of mass risk (Risiko), the former being a personal threat by wealth and political power, the latter by technological-economic development.

Risiko, who has already used the notion of Risiko, Gefahr, and Gefährdung, which is translated into the same danger as Korean, implies a threat to the foreseeable legitimate interests (i.e., nuclear power plants, Gefahr means the possibility of unexpected corruption of legal interests, and Gefährdung means the possibility of infringement of an individual's legal interests. It is a view interpreted as traditional danger. In other words, Beck distinguishes 'danger' from past threats (Gefährdung) and new forms of mass risk (Risiko) [8], the former being a personal threat by wealth and political power, the latter by technological-economic development, Risiko, in the sense that it uses the concept of Risiko, Gefahr, and Gefährdung, which translates into the same danger as the Korean language, which means a threat that can occur at the center of society itself, ). Gefahr is an antagonism of unexpected legal interests, and Gefährdung is a traditional danger that means the possibility of infringement of personal interests [9]. The controversy is that the traditional form of risk (or crisis) is seen from the same point of view, but there is a difference in how the new type of risk is viewed. The risk is the possibility of occurrence, not the problem itself. Considering the possibility of human control over the future, it is reasonable to distinguish between risk and harm.

However, since the concept of Risiko, which is different from the traditional risk (Gefährdung), which means the possibility of infringement of the individual's legal interests by this division, is not a concept with its own limitations, The definition is still unclear. Therefore, the concept of a new form of risk must have an abstraction. Taking all of the above-mentioned arguments into consideration, the new form of risk is "to be expected based on human collective decisions in post-industrial society, As well as a certain industrial mass risk that appears to be unavoidable in the unprotected state personally ". It is necessary to examine the conceptual features of the risk society based on the risk and the concept of risk society discussed above.

2.2.2. Our society as a new risk society

Korea has started to become a dangerous society based on the construction of Kori nuclear power plant in 1977 [10]. However, Korea's risk society differs from the typical characteristics of risk society proposed by Ulrich Beck [11]. Risks are not only technological, socio-economic but also cultural aspects [12].

First, Beck 's risky society 's risks are inevitable products and fateful risks caused by the combination of development and industrialization of science and technology, which were key elements of the Western modernization process. We were able to avoid this if we were to switch from a flawed modernization strategy to a green development model as a result of the desperate need of the growth-oriented model chosen by the desperate need [13].

Second, it is a variation of danger personality. The dangers of Korean society are not only the new massive risk of late industrial society such as large scale environmental pollution, but also the danger of traditional society such as insolvency, industrial accidents, industrial society such as industrial society, transition society, school violence and sexual violence crime. It is showing the phenomenon. Furthermore, the adverse effects and risks associated with the development of science and technology are also showing signs of heightening social unrest.

Why did this dangerous society arise? I think there are various perspectives according to the writer, but basically it is because I stimulated the desire of safety for my existence. In other words, the subjective aspect of the emergence of new mass risk due to the development of science and technology, and the subjective aspect of increasing the anxiety and fear of the social members resulting from this competition. Of course, it is true that the traditional and natural dangers of our society have been reduced compared to
the industrial societies due to such economic growth and development of science and technology. However, objective safety has increased, but the subjective anxiety that the members of society have in the new form of mass dangerous danger poses a serious threat to objective safety. For this reason, members of our society are demanding active intervention in new risk factors, and the state and legislators have responded to the preemptive application of criminal law, not the traditional preventive law, the area of police law. In other words, according to the traditional liberal legal theory, it was virtuous to abstain from intervening in the state, especially the state penal right, but in the dangerous society, it started the penal intervention enough to eliminate the anxiety of the risk of the social member.

2.2.3. Cyber terrorism in dangerous society

In this sense, the concept of cyber terrorism in our society is a traditional risk source such as murder and rape, but the approach to risk regulation is based on the necessity of social defense, or the cyber terror itself is a new form. It is necessary to judge the risk cause.

Ulrich Beck explained that the new forms of risk have invisibility, equality, and boomerang effects, and cyber terrorism is consistent with these characteristics. In other words, i) cyber terrorism, unlike the traditional forms of terrorism, is a risk that goes beyond human cognitive ability, so it can be recognized through scientific knowledge, and ii) the traditional danger in terms of the exposure of crime is the status of social class. Although the degree of exposure is different, cyber terrorism has the potential to be more vulnerable to the social middle class, which has a relatively high reliance on ICT technology, resulting in the disappearance of the line between the privileged and the non-privileged in terms of exposure. In other words, in terms of exposure to risk, cyber terrorism can be leveled differently from traditional risks. iii) Cyber terrorism is also equivalent to the boomerang effect proposed by Beck, because ICT technology has a structure that allows people who see large and small gains to take risks and their negative consequences. iv) Furthermore, social and political discussions on cyber security have been carried out with several serious cyber terrorism in the past, and the political and legislative debate that has arisen has led to the explanation that Beck’s new type of risk is political explosive power. I agree. In this respect, cyber terrorism is a typical example of the risk presented by Beck. Therefore, the top priority of the criminal policy for these risk sources is the construction of the social safety net to protect the safety of the members in response to the cyber terrorism which is a risk of social harm[14].

2.3. Foreign factors - changes in the security environment

Let’s turn our perspective on the security environment out of the country. At the end of the 20th century, the end of the Cold War system under the US and the Soviet Union resulted in a reduction of the possibility of world wars. As a result, conflicts and conflicts between ideologies, systems, and institutions, which served as important criteria in determining the friendship and hostility between countries during the Cold War period, have been remarkably reduced, while the pursuit of core interests and political and economic interests[15]. The importance of peace and economic development through mutual cooperation is becoming more important. In this international situation, the concept of security is changing and our security environment based on this is also changing.

Traditionally, national security was based on military security. However, due to the end of the ideological confrontation between nations and the rise of non-state actors in accordance with the progress of information and globalization, conflicts arise due to territorial and economic interests. In other words, the changed international situation calls for a new paradigm of national security. The recent national security paradigm is not focused on traditional ideology or military superiority but threatens and paralyzes the people, territory, sovereignty. Elements also appear as a concept of comprehensive security that can threaten national security[16].
The paradigm of this new security environment is characterized as follows. 1) As discussed above, in the setting up of the concept of security, not only from the military point of view, but also from the non-military elements such as politics, economy, society, environment and technology. The fundamental change of the subject and the threatened object is that the viewpoint of security has changed from the viewpoint of the state-oriented security concept to the center of the individual and the human community.

3) The emergence of transnational threats as a threat to national security is not a conventional concept of a nationality. Transnational threats are characterized by the fact that the source of the threat is done by non-state actors, while the threats by non-state actors are transcended beyond traditional borders. 4) Finally, each country in the world has reached a state where it can not guarantee the security of the state from the threat of terrorism. These threats are caused by traditional forms of terrorism, such as the September 11 attacks of 2001, but cyber terrorism using advanced ICT technology is also a potential threat to national security.

3. Conclusion - Cyber Terrorism as an Element of National Security

In general, national security means that the core values of a country are free from threats to core values. Traditional national security mainly refers to external military threats, and therefore, most of these threats are state actors. However, since the end of the Cold War, the security environment brought about various threats (e.g., international crime, drugs, the environment, refugees, resources) other than military threats, and the inclusion of comprehensive security to cope with these various threats. In particular, as the information society based on the innovation and development of ICT technology is settled, cyber-level security threats are added, and the security environment of that time is different from the security environment during the Cold War period. In particular, major social infrastructures and services of the modern countries including Korea are gradually being connected and controlled by ICT technology. In case of facility and service failure caused by unauthorized access to such facilities, the impact on the normal operation of other core facilities may become very large. In particular, there is a serious problem in that the infringement of the network connecting the national infrastructure such as communication, finance, water supply, power, etc. and controlling each information system may cause obstacles in the whole country rather than simple cyber infringement. In this way, cyber terrorism cases against the state infrastructure have been actualized. In addition to the cases described above, there are many cases of cyber terrorism in Korea. In recent years, cyber terrorism targeting Korea has tended to occur in order to impose damage to national infrastructure such as GPS, telecommunications, broadcasting, and financial facilities. This is because the risk of individual criminal activity to threats to national security. In the ICT era, cyber terrorism is a new threat to national security and it is a new type of risk source that is discussed in modern risk society. Therefore, there is a need to cope with criminal policy and legislation. However, on the grounds of the limitations, the concept of cyber terrorism as a basic premise for the response of cyber terrorism and the legal and philosophical grounds on which the state should prevent cyber terrorism will be published in the next issue.

4. Reference

4.1. Journal articles


4.2. Books