GLOBAL RISKS, BIOTECHNOLOGY, AND THE FUTURE OF BIOSECURITY

(Only complete the Author list after the review process has been completed)

ABSTRACT

The global risks that emerged as a transnational phenomenon on the backdrop of recent post-cold war, globalization, and information-centered society are manifesting as the failure of technology systems developed by humans and the crisis of social systems in addition to unexpected natural disasters. In order to establish a national strategy for preemptive response, we use the emerging security theory, which is a new security theory, and pay attention to the science, technology, knowledge and information-intensive characteristics of emerging security threats. This paper explored ways to help policy makers to prevent risk and increase resilience of global risks, especially those in the biotechnology field. We analyzed the concept and characteristics of biosecurity and analyzed the situation both at home and abroad. In particular, in-depth analysis was conducted by not only segmenting the biosecurity into infectious diseases, bioterrorism, biological weapons, health security, and food security but also focusing on emerging technologies such as gene editing and synthetic biology. Through in-depth interviews with key decision-makers and experts, we proposed a science-based policy direction for biosecurity.

Key words: global risks, emerging security, science and technology, biotechnology, biosecurity

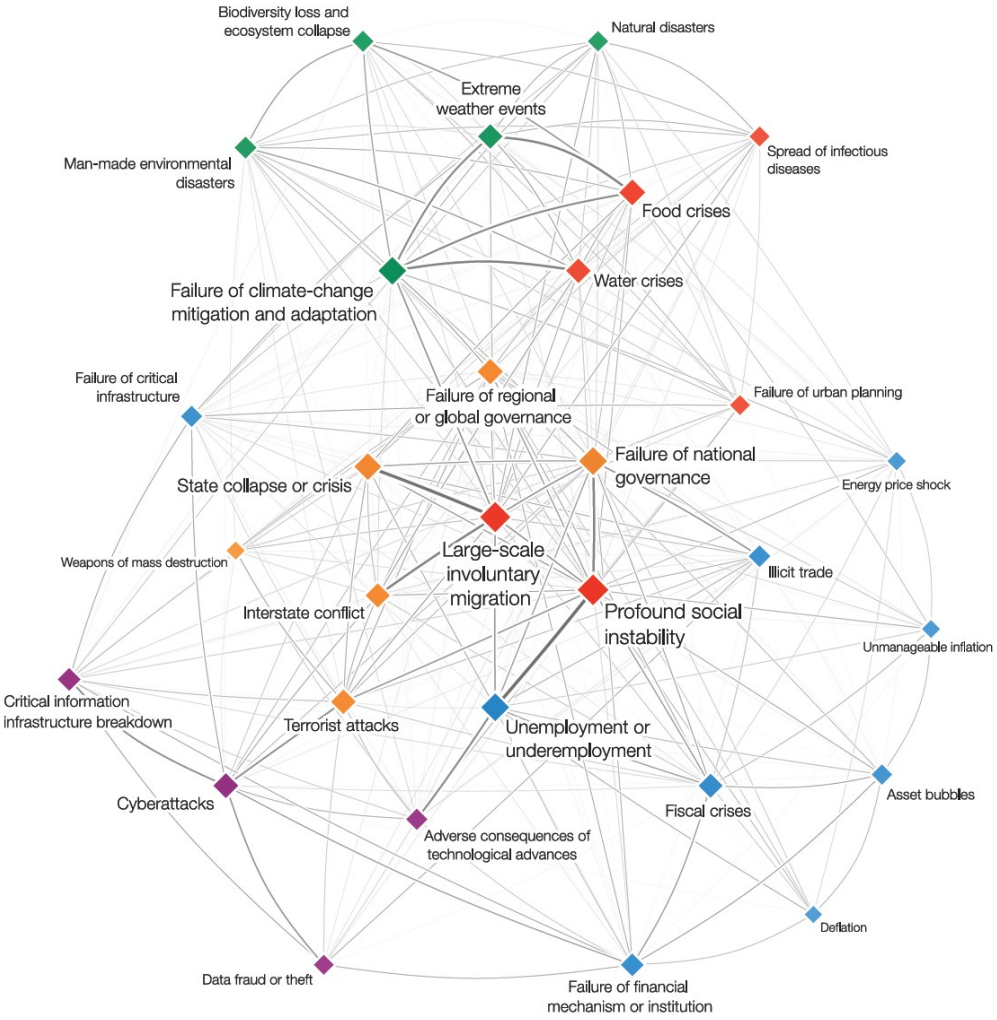
INTRODUCTION

Global Risks

For over a decade, the Global Risks Report of the World Economic Forum (WEF) has focused attention on the evolution of global risks and the deep interconnections between them. The Report has also highlighted the potential of persistent, long-term trends such as inequality and deepening social and political polarization to exacerbate risks associated with, for example, the weakness of

the economic recovery and the speed of technological change. And WEF analyses the difference in risk perceptions over different time horizons and the perceived interconnections among risks, as visualized in Figure 1, based on the Global Risks Perception Survey (GRPS). The final part of this Report explores the relationship between global risks and the emerging technologies of the Fourth Industrial Revolution (4IR). We face a pressing governance challenge if we are to construct the rules, norms, standards, incentives, institutions and other mechanisms that are needed to shape the development and deployment of these technologies. How to govern fast-developing technologies is a complex question: regulating too heavily too quickly can hold back progress, but a lack of governance can exacerbate risks as well as creating unhelpful uncertainty for potential investors and innovators. Currently, the governance of emerging technologies is patchy: some are regulated heavily, others hardly at all because they do not fit under the remit of any existing regulatory body. Respondents to the GRPS saw two emerging technologies as being most in need of better governance: biotechnologies – which tend to be highly regulated, but in a slow-moving way – and artificial intelligence (AI) and robotics, a space that remains only lightly governed.

Then, what is an effective government strategy to respond to these global risks including emerging technologies?



Sources: WEF Global Risks Perception Survey 2016

Figure 1: The Global Risks Interconnections Map

The Emergence of a New Security Paradigm

In recent years, non-traditional security, which distinguishes itself from traditional security centered on military security, such as spread of infectious diseases and cyber terrorism as well as climate change and poverty, are increasing dramatically. Today, the global risks that occur worldwide are multi-layered and complex problems, and are new security problems that cannot be understood by the concept of traditional security that emphasizes military security at the national level. These new threats are deeply interdependent due to the free movement of people, goods and information around the world, and they are not only very damaging, they cannot think of risk factors alone.

This paper attempts to understand the new security paradigm, which is recently emerging in the so-called network age. It presents the concept of “emerging security” to comprehend a variety of transnational and global risk, taking place

in such fields as environmental security, cyber security, health security, human security, and societal security. The word, “emerging security”, was combined with two words, “emergence” from complexity theory and “security” from International Relations. With this new terminology, this paper pursues a new security studies in a proactive way, moving beyond the somewhat passive conceptualization of “non-traditional security”, the concept of emerging security was presented to describe the phenomenon in which various safety issues at the micro level are continuously increasing their quantity and inter-connectivity, and in a certain moment transforms as security problems at the macro level. The reality of emerging security is significant in the sense that it transforms the object and subject of global risk, and further influences the nature of world security politics, dominated by the notion of traditional security that pays special attention to the role of military security.

Although there has been a number of previous attempt to theorize the newly rising security paradigm since the end of the Cold War in the early 1990s, those existing studies are inadequate so as to explain the post-modern nature of security affairs in the 2010s. This paper, in particular, reviews the theory of the Copenhagen School which has expanded the traditional security paradigm in the 1990s. It also introduces the theory of securitization in which a social problem is being escalated into a security problem. This paper, however, argues that it is not enough for us to stay with the Copenhagen School in understanding the new security problems in the Post-Cold War era, especially the twenty-first century. It also emphasizes the emergence of non-conventional threats since the 9-11 incident and the necessity of a new, more efficient strategy against them. While the security concepts in the Cold War era had been established based on the military-strategic perspective, those in the Post-Cold War era are featured by their expansion in security subjects, objects, and application areas across diverse actors and social aspects. Therefore, the emergence of emerging security can be viewed as an emergence of a new security paradigm that is understood not only in terms of the emergence of new security phenomena but also in terms of both traditional security and non-traditional security.

On the other hand, the emergence of global risks is expanding the number of security actors as well as new security areas. In addition to national actors, non-state actors such as international organizations, multinational corporations, global civil society, and even technology and social systems themselves are causing risks. Therefore, to solve the new security problem, it is important to establish a mechanism of multilayered and complex governance that is sought at the regional and global level beyond individual countries. Therefore, it is necessary to further distinguish the types of risks that arise from the complex environment. The 'degree of coupling of components' refers to the degree of need for connection between different components, and the ‘complexity of interaction’ refers to the degree of feedback between components that occurs for smooth operation of the system. The types of risks that arise in the emerging security sector based on the attributes of these two systems can be divided into the following four types.

High coupling of components low	‘sudden limited risk’ *traditional security*	‘sudden infinite risk’ *cyber security*
	‘gradual limited risk’ *human security*	‘gradual infinite risk’ *health security*
	low high complexity of interaction	

Figure 2: The nature of the system and the type of risk encountered

To effectively cope with these four types of global risks, we need to introduce appropriate governance forms for each attribute. The 'sudden limited risk' refers to the government-led model, 'sudden infinite risk' refers to the intergovernmental cooperation model, 'gradual limited risk' refers to the regional participation model and the 'gradual infinite risk' refers to the transnational participation model.

Emerging Security vs. Science and Technology

So, what are the key factors for emerging security?

Recently, it is urgently required to strengthen the social role of science and technology for the happiness of the people. In the meantime, the field of science and technology's social role has been focused on economic growth as a blind spot of policy, the promotion of science and technology has been focused on economic growth, measures for social role have been established several times in Korea, but follow-up measures are insufficient. The people recognized 'improvement of quality of life' as the most important role of science and technology. Meanwhile, developed countries such as the United States, the European Union and Japan are continuing to strengthen their role of science and technology promotion in solving social problems.

On the other hand, emerging security threats also have a science, technology, knowledge, and information-intensive nature, which is increasingly related to science and technology. The characteristics of emerging security arise mainly from security problems arising from the technical environment, and interactions with many other things (or technology) variables as well as human actors play an important role. In the emerging security field, various technological variables also play an important role in terms of the solution of the threat or the cause of the threat. Applying these discussions to emerging security cases, threats in this field are not generated solely by human actors, but are generated by science

and technology variables themselves. Therefore, in order to identify the cause of the threat in the emerging security field and to establish a solution, it is necessary to secure the necessary scientific and technological capacity to break the rising link of micro-security to macro-security

In other words, it is essential to recognize the importance of the national level in the establishment of the emerging security policy direction in the future and to establish a science and technology-based national strategy.

In particular, over the past three years, the world has experienced a lot of risk factors and cases in the biotechnology field directly related to human beings, such as the International Cooperation for the Prevention of the Ebola Diffusion (2014), the Obama Administration's Antibiotic Drug-resistant Bacteria National Strategy (2014), MERS (2015), Global Health Security Initiative (GHSA, 2015), and emphasis on food security, and shared their knowledge.

Therefore, in this paper, we would like to consider the direction of science and technology policy for biosecurity of emerging security.

Methodology

To our research was conducted in four stages. First, we began with a review of the extant literature on biosecurity, focusing on earlier work regarding the implications of technological change on biosecurity. Second, we selected interview subjects in relevant fields, interest in problems involving the nexus between biotechnology and biosecurity. Third, we checked our initial conclusions with our original interview subjects and then consulted a wide variety of expert sources knowledgeable about biotechnology and/or biosecurity. Finally, we solicited feedback on preliminary versions of our analysis and conclusions through presentations at conferences.

MAIN Findings

What is Biosecurity?

In the field of diplomacy and security, biosecurity is defined as "measures to protect various actors from pathogenic microbes that are intentionally or accidentally sprayed or naturally occurring". It includes various phenomena in terms of subject, type of threat, and subject of conduct. For example, it is biosecurity to prevent biodiversity by preventing natural diseases from transferring to crops and livestock, and also to protect human health from various pathogens is also biosecurity, agent is also a biosecurity.

And biosecurity encompasses not only health, agriculture, or environmental research, but also biodefense or biological warfare, which responds to the security threat posed by pathogenic microbes being biologically active. In other words, the main security targets for biosecurity include not only human, animal, plant, or biodiversity, but also countries. It is the presence of pathogens that pass through various areas of biosecurity, and there are differences in whether the emergence of pathogens is natural or artificially mineralized.

Biosecurity is categorized into the following types according to the threat propagation path, issuers of security threats (actors), responding subjects (security providers), and related governance.

Infectious diseases that occur naturally and potentially impair the normal functioning of society are biosecurity problems. The situation that infectious diseases with large-scale deaths that hinder normal functions of society occurs in developing countries and spreads worldwide, calls for infectious diseases as security issues in the 21st century. An infectious disease is a new form of security threat from the fact that it can cause massive human and material harm without military invasion. In other words, if it is localized, it is a matter of public health, but if it is spread over the border, it becomes a security problem.

Second, bioterrorism is a biological attack by non-state actors and has been recognized as a biosecurity problem since the early 1990s. The perception of bioterrorism began with the fear that the terrorist group could obtain the Soviet Union's accumulated biological weapons as the former Soviet Union collapsed. After the September 11, 2001 terrorist attacks, the perception of biosecurity has been strengthened. Due to the rapid development of biology research capabilities, worldwide spread, the acquisition of information on the Internet, and the availability of pathogenic microorganisms from terrorist groups and the ease of developing biological weapons, bioterrorism is called the "Poor man's nuclear bomb".

Third, biological weapons are the oldest biosecurity problem, and there are biological weapons in which national actors use pathogenic microorganisms for military attacks. The threat posed by biological weapons has been addressed in

terms of deterrence and arms control rather than public health, even though biological weapons are a direct threat to military personnel as well as civilians. Thus, the security threats posed by biological weapons are managed by disarmament treaties.

The nature of the biosecurity phenomenon that we face today is too complicated to divide into core issues and surrounding issues in a dichotomous context, and it is necessary to redefine the concept of biosecurity as a broad meaning based on this recognition.

Meanwhile, generally, biotechnology has the broad concept of ''technology related to living organisms, biologically derived materials and biological models''. Therefore, this paper intends to adopt the broad meaning of biosecurity as “security agendas and problems related to living organisms, biological systems, genomes, or materials”.

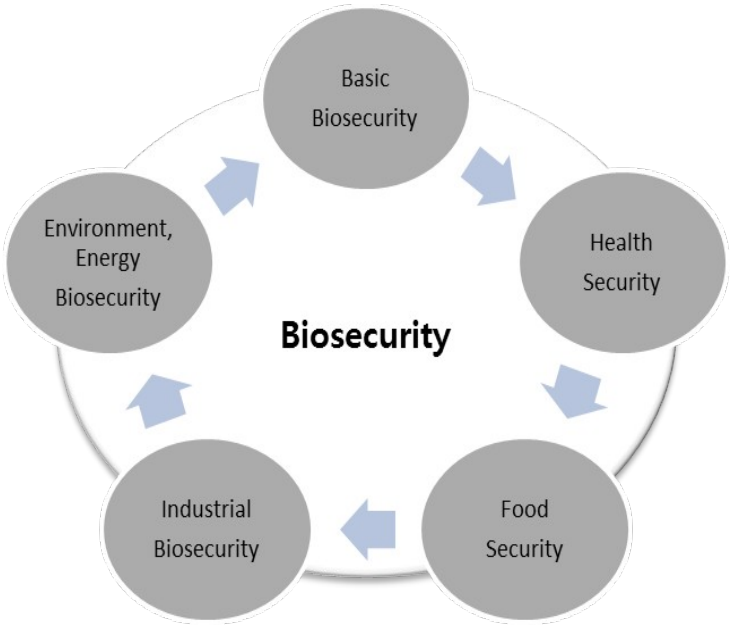


Figure 3: The scope of Biosecurity

In addition to analyzing biosecurity (infectious disease, bioterrorism, biological weapons, etc.), sub biosecurity problems include focusing on health security and food security with a high degree of interest from the national point of view.

The concept of health security is “protection from the political, economic and social threats to personal health in the human security theory and a human rights approach”. In health security, the difference is that one person gets a cold in one household and one million people in a city, which is equivalent to the population of the whole city, and the latter is a clear national security problem.

In the meantime, the issue of food at the national level has to be approached from the point of securing food centered on crops including rice, rather than the concept of food safety, and it is necessary to discuss the governmental food security in order to maintain the nation and maintain the healthy life of the people. Food security is a “state in which food is always accessible and safe and nutritious, economically and quantitatively, in order to maintain the active and healthy life of all citizens and to meet food preferences”. In addition, food production, distribution, and consumption are defined as being environmentally friendly and sustainable.

And the rapidly developing biotechnology has a 'dual-use' risk that potentially can control or generate disease. There is also the risk that new technologies such as genetic engineering can manipulate viruses or bacteria to develop new diseases or facilitate the production of highly usable pathogens. Recently, emerging biotechnologies such as synthetic biology, genetic editing, and nano biotechnology, as well as open source software and hardware, are concerned that biotechnology and production are becoming more sophisticated and easier at lower cost.

Biosecurity is characterized by asymmetry besides intrinsic diversity. From the perspective of threat agents and threats, biosecurity can be defined by national or non-state actors, even from threatened pathogens that have been spread by violent or nonviolent means. In addition, since pathogens are invisible and propagating, individual countries are not enough as providers of biosecurity, and national defense measures may not be effective. In addition, there is still a lack of understanding of the inherent characteristics of biosecurity, for example, the scientific and technological characteristics that are the origin of the threat.

Status and Tasks of Biosecurity

Currently, new human infectious diseases cause continuous threats and losses, and the incidence is rapidly increasing. The number of cases of infectious diseases worldwide has increased from less than 1,000 (1980-1985) to 3,000 (2005-2010), and the variety is increasing. Especially, the outbreak of antibiotic-resistant bacteria is serious. In Korea, where antibiotics are used in a large amount, the infection is more severe and infectious diseases such as malaria are increasing due to climate change. If the infectious disease is limited to one country, it is a security problem if it is spread across the border. Governance to address security threats from naturally occurring infectious diseases is the International Health Regulations (IHR) of the World Health Organization (WHO), which was created in 1948. WHO adopted IHR 2005, which reflects a changing health environment in 2005, and entered into force in 2007. Recent awareness of the security threats of infectious diseases has also changed the relevant global governance. The WHO, the governance of health, recently added the necessary measures to address security implications beyond the public health and

treatment of infectious diseases. Apart from the WHO, the United States launched the Global Health Security Agenda (GHSA) in 2014 to address the fight against infectious diseases from a security perspective.

There is a conflict between the skeptical point of view that bioterrorism is not realistic and the point of emphasizing the threat of bioterrorism on the basis of possibility of mass killing if the probability of occurrence is low. There is no single written international convention dealing with the development and use of non-state actors' biological weapons. The reason for the absence of international conventions in bioterrorism is that the perception of security threats from bioterrorism is relatively recent, and the fundamental limitation is that non-state actors cannot be the subject of international conventions.

Security threats posed by biological weapons were managed by disarmament treaties. After the use of biological and chemical weapons in World War I, the Geneva Protocol, which prohibited the use of biological weapons between States Parties to the Protocol, was signed in 1925, and in 1969, after the United States unilaterally abandoned aggressive biological weapons, the development, production, accumulation, acquisition and disposal of biological weapons (disarmament) are regulated by the Biological Weapons Convention (BWC) in 1972. The BWC is limited in that it does not keep pace with the insufficiency of the mechanism to confirm compliance with the Convention, the private enterprise and biology laboratory regulations that can be used to develop biological weapons, and the technical complexity of biology.

A representative research institute that conducts policy research on emerging security, including biosecurity, is the Belfer Center for Science and International Affairs at the Harvard Kennedy School. The 'Science, Technology, and Public Policy Program' (STPP), which is operated by the center, focuses on the intellectual exploration that enables science and technology to play an essential role in our whole life. Climate change and renewable energy, Internet policy, cyber security, and biosecurity all contribute to research. There are many projects currently in the center program, and there are many analytical studies on security policy. Climate change and sustainability issues in the energy and environment sector, nuclear management in the international security sector, and information and communication technology and innovation are the security issues in the cyber-era, the managing the microbe problems such as bioterrorism and infectious diseases. Another research institute is MIT's Program on Emerging Technologies (PoET). This program is conducting extensive research on bio-security focusing mainly on synthetic biology.

There are not many examples of policy and science and technology research focused on biosecurity, namely, infectious disease, bioterrorism and biological weapons in Korea. The policy researches on the whole new emerging security including biosecurity have been continuously carried out by researchers of the related scholars and researchers of the Institute of Foreign Affairs and National

Security (IFANS), centering on Institute of International Affairs of the Seoul National University. The policy researches on health security and food security have been carried out by the Korea Health Industry Development Institute (KHIDI) and the Korea Rural Economic Institute (KREI).

Research related to biosecurity and research on technology development is centered on basic research support of the Ministry of Science and ICT, development of technology related to health and security, and development of technology related to food security are supported by the Korea Health Industry Development Institute (KHIDI) and the Korea Institute of Planning & Evaluation for technology in Food, Agriculture, & Forestry (IPET). Studies related to biodefense have been conducted mainly by researchers of the Korea Research Institute of Bioscience and Biotechnology (KRIBB).
As a detailed issue, R&D investment has been expanded in the field of infectious diseases mainly in practical use fields such as diagnosis technology, vaccine and therapeutic technology development along with basic and mechanism research aiming at excavation for the past 5 years (2010-2014). Investments are invested mainly in the bottom-up research projects, and there are limitations in practical application and field utilization of research results. On the other hand, investments that can be utilized in the field of clinical, policy, monitoring, forecasting, 15% (Won 107.3 bn), respectively.

Korea's crop self-sufficiency rate (including feed use) dropped from 80.5% in 1970 to 43.1% in 1990 and to 23.8% in 2014, and the main crops other than rice were below 10% (32 of the 34 OECD countries), Barley and soybeans self-sufficiency rate of 24.8% and 11.3%, respectively, but wheat and corn that can replace rice are 0.7% and 0.8%, respectively. Despite the serious self-sufficiency rate of crop, Korea still does not become a major problem because it is much more economical to import than to produce in Korea, and it is not necessary to promote domestic production of grain in the face of increasing rice inventory. However, if the world faces a food shortage crisis, our economy will be at great risk because of the monopoly of some countries that have the lead in crop supply, and even if we have the ability to overcome them, it will not. In preparation for this, the Korean government set the first agricultural target as "stable supply of safe agricultural products" in the "Agriculture, Rural and Food Industry Development Plan (2013-2017)" established in 2013, from 23.6% in 2017 to 30% in 2017. In addition, the related national plans are paying attention to the role of science and technology in securing food security and propose important issues. "Agriculture, Rural and Food Industry Development Plans (2013-2017)" focuses on the role of science and technology for food security.

CONCLUSION

The following science and technology-based policy directions for biosecurity are suggested through in-depth analysis and evaluation of the detailed issues of biosecurity defined in this paper: infectious diseases, bioterrorism, biological weapons, health, and food.

First, since Korea is highly dependent on foreign countries and open to the public, it is exposed to the threat of biosecurity spreading from the outside. Therefore, it is necessary to promote biosecurity policy at a level comparable to diplomatic and security. In other words, the security threat posed by the pandemic and food crisis in the 21st century does not leave biosecurity as a low politics issue anymore. Dealing with biosecurity issues at the diplomatic and security level implies the inclusion of biosecurity issues in bilateral and regional diplomacy, participation in relevant global discussions, and implementation of international agreements.

Second, as the risk of emerging security arises from a transnational and global dimension, it is necessary to build a countermeasure system beyond the national level. It is not enough to recognize and respond to biosecurity problems such as infectious diseases, bioterrorism, biological weapons, health, and food as security threats, and it is not enough for individual countries to take action, so global response and cooperation are effectively.

Third, the threats that arise in the field of biosecurity are generated not only by human actors but also by the science and technology variables themselves. In the problem solving, the science and technology variables have more meaning than the simple tools utilized by human actors. Points should be considered. Therefore, it is necessary to prioritize the roles of science and technology in order to understand the nature of threats in various biosecurity fields and to find concrete countermeasures.

Fourth, biosecurity should be systematically addressed within the framework of emerging security based on science and technology along with cyber security, nuclear security, environment security, energy security, and population security as emerging security problems (non-traditional security).

Fifth, in order to identify the causes of threats in the field of biosecurity and to provide solutions, it is necessary to secure the necessary scientific and technological capabilities for cutting down the rising link of micro-security to macro-security is needed.

Sixth, biosecurity of the past has only discussed macroscopic discernment, but now we should pay close attention to micro-security, which is a possibility of emergence, from a security point of view. What is at stake here is to find out the rules that enable emergence and to identify when and how catastrophic phenomena will occur.

Seventh, it is necessary to understand the characteristics of emerging security and try to find new security governance suitable for it. The issue of exploring the

contents of such emerging security governance is also a future research topic. The establishment of governance related to biosecurity is currently the highest priority in the field of science and technology when the amendment of the related laws is completed.

Eighth, there is a need to expand the bioindustry base to strengthen biodefense capabilities. This will be a key factor in the development, stockpiling, and diagnostic capabilities of vaccines and treatments. In particular, the domestic productivity and stockpile of vaccines and treatments for biologic agents that can now be used as biological weapons should be increased. Thus, it is necessary to enhance the strategic deterrence ability of agents capable of causing biological warfare. Currently, vaccines against anthrax, smallpox, yellow fever, which are recognized as the most threats, have no domestic production capacity.

As a policy direction for health security, which is a detailed security problem, first, it is necessary to strengthen the governance and promotion system of One Health concept. Second, it is necessary to strengthen the coordination function of the R&D portfolio, which has a high level of health security policy and flexibility. Third, the government-private partnership model in the field of health and security needs to be promoted. Fourth, strengthening global R&D cooperation system for preemptive response of health security is needed. Fifth, it is necessary to complement governance related to health security.

As a policy direction for food security, which is a detailed security problem, it is necessary to reform the R&D system to secure food security and to differentiate and pursue the short- and medium-term R&D strategies in parallel. The following policy challenges need to be set in order to establish food security and its foundations. First, it is necessary to develop high quality edible rice. Secondly, by developing customized rice suitable for various purpose and processing characteristics such as special rich rice, special nutritional and efficacious rice, not only should it be enhanced to a new level, but it should also be used as a new type of pharmaceutical material. Third, the technology needed to search for new food crops to replace or supplement rice, to cultivate new crops, to promote their use, and to develop alternative crops to promote the conservation and utilization of agricultural land. Fifth, it is necessary to develop agriculture technology that can accelerate automation and reduce production cost in response to increase in aging and female farmers and decrease in rural population. Sixth, in order to cope with climate change, weather disaster prediction technology and ecosystem change detection technology, it is necessary to develop improved and cultivated crops with high value added crops that meet the subtropical and temperate climate. Seventh, the development of disaster disease control technology that threatens food security is needed. It is also necessary to establish countermeasures to prevent the reoccurrence of the food crisis in 2007-2008 by paying attention to the mechanism of characteristics in which food security is linked to energy security in a complex manner. And it is also necessary to promote the establishment of the national food system, the promotion of private investment, and the training of outstanding talent.

REFERENCES

Book

FAO, (2003), Trade Reforms and Food Security: Conceptualizing the Linkages. FAO.

Filder, D.P., and Gostin, L.O., (2008), Biosecurity in the Global Age: Biological Weapons, Public Health, and the Rule of Law. Stanford Univ. Press.

Maxwell, S., and Smith, M., (1992), Household Food Security: Concepts, Indicators, Measurements: A Technical Review. UNICEF and IFAD.

Ministry of Science, ICT and Future Planning, (2016), Biotechnology in Korea 2016. MSIP.

National Academy of Sciences (NAS), (2010), Understanding Biosecurity: Protecting Against the Misuse of Science in Today's World. NAS.

National Science and Technology Council, (2016), A 21st Century Science, Technology and Innovation Strategy for America's National Security.

NIAID, (2007), NIAID Strategic Plan for Biodefense Research 2007 Update.

OECD, (2009), The Bioeconomy to 2030: designing a policy agenda.

United Nation, (2011), State of the Future.

WHO, (2006), World health report 2006.

WHO, (2007), World health report 2007: A safer future, global public health security in the 21st century.

World Economic Forum, (2016), Global Risks Report 2016.

World Economic Forum, (2017), Global Risks Report 2017.

Journal Article

Katherine F. S., et al., (2014), Global rise in human infectious disease outbreaks, *Journal of the Royal Society Interface*, 11: 20140950.

Kim, Sangbae, (2016), Emerging Security and Meta-governance: Theoretical Understanding of the New Security Paradigm, *Journal of Political Science Studies*, 50(1), 75-104.

Min, Byoung Won, (2007), Extending the Concept of Security in the Post-Cold War Era and the Network Paradigm, *Journal of National Defense Studies*, 50(1), 23-55.

Online Material

Belfer Center for Science and International Affairs of Harvard Kennedy School, https://www.belfercenter.org/project/managing-microbe.