*IOSR Journal Of Humanities And Social Science (IOSR-JHSS)*
*Volume 24, Issue 2, Ser. 9 (Feb. 2019) 27-31*
*e-ISSN: 2279-0837, p-ISSN: 2279-0845.*
*www.iosrjournals.org*

# A Study on the Environmental Approach to Digital Risk Response Policy

Ji-Yeon Yoo*
** Department of Intelligent Engineering Informatics for Human in Sangmyung University, Republic of Korea*
*Corresponding Author: Ji-Yeon Yoo**

**Abstract:** Since these risks are not limited to the information technology and online environments, such as information systems and information networks, we must consider ways to approach and protect the ultimate problems, not just the system, but the problem of human survival, privacy, and happiness. In other words, we consider the environmental approach as a way to prevent multidimensional risk in the hyper digital risk society and to protect human fundamental rights. Environmental rights are the most modern solution to protect people from external factors and guarantee their rights.

**Keywords:** Digital Risk Response Policy, Environmental Approach, Hyper Digital Risk Society, Human Survival, Human Fundamental Rights

---

Date of Submission: 13-02-2019 Date of acceptance: 28-02-2019

---

## I. INTRODUCTION

The remarkable development of information technologies such as AI, IOT, Big Data, and Cloud has led to new changes to the digital environment and deepening human dependency on and coupling with information technology. These technological developments have created a hyper-connected society in which all areas are integrated into one through the integration of people and objects, the strengthening of networking abilities, and the acceleration and increase of industrial value through new applications (WEF, 2014). The emergence of this super-connected society is changing not only the digital social environment, but also the behavioral patterns of government, industry, and individuals (PRCST, 2014).

However, the rapid development of information technology and networking and the concomitant acceleration of hyper-connectivity are increasing the potential for complex and unexpected risks and dysfunctions. In other words, the development of artificial intelligence gave people the advantage of improving their quality of life by improving convenience and accessibility to knowledge, but on the contrary, presented various risks such as degradation of individual proficiency due to increasing dependency, and the effects differ according to individuals, industries, and governments. Personal autonomy of personal information has become difficult or impossible to guarantee, and the risk of infringement of personal information stored and transmitted through IT devices without impregnable security is increasing. There is a problem with personal information being processed through big data in a situation where the collection route of information such as use of social network services (SNS) and access to public data is expanded and diversified (Seon & Kim, 2014). Industry is increasing cyber threats that threaten or attempt to compromise the operation of connected objects in the network layer and wireless sensor network links (Korea Economy, 2016). An electronic device connected to an IoT network such as a security camera, a router, or a DVD can be used to introduce malicious code into the network. Cyberattacks can harm national security and diplomatic relations at the government level. As core infrastructures such as water, electricity, food supply, and public health move out of their closed domains and expand into the connectivity and vulnerability of the private sector, malicious infringements can cause tremendous social chaos and instability (Wright & Schaetzel, 2013).

Recently, the dilemmas of the development of the information society have become more and more intense as society as a whole becomes digital (Jeong & Yoo, 2010). Uncertain, complex, and unpredictable risks are scattered throughout ICT by its normalization, convergence, intelligence and personalization, and the danger that threatens a weak link poses a greater danger to society by causing a domino effect which could lead to widespread crisis and disaster. In particular, Cyber-Physical Systems (CPS), in which a variety of systems collaborate to achieve a common goal, are expanding the digital environment to the frontier between online and offline (X. Li, C. Qiao, X. Yu, A Wagh, R. Sudhaakar, and S. Addepal, 2012). In the CPS era, where the digital domain and the physical domain fuse and interact, the security liabilities of the cyber domain can be transferred to security and safety vulnerabilities in the real world (AhnLab, 2017).

Therefore, in this study, we define the hyper-digital risk society as a more profound risk society in which digital risk has fully expanded into the environment where cyberspace and physical space co-exist. I want to conduct basic research on this phenomenon. Digital risk society means a society threatened by the danger posed as information technology expands as a social infrastructure and reproduces itself throughout the social system as an entire society becomes digitized and the boundary between cyberspace and real space becomes ambiguous (Jeong & Yoo, 2010). In recognition of hyper-digital risk, we try to protect the digital security that protects people's lives, bodies, property and privacy as fundamental societal rights.

## II. FULL-SCALE EXPANSION OF DIGITAL RISKS

The increasing complexity and connectivity of the digital environment caused by the advent of the early connected society is foreshadowing risk premises where all elements, subjects, and environments are threats to security and stability. It is a simultaneous occurrence of a domino effect dynamic in which inanimate objects become sources of threat and individuals' risks becomes the state's risks both online and offline. For example, the university's set-top box for air conditioning management becomes a target of cyber threats (KISA, 2014), and personal infringement will soon threaten national infrastructure through targeted attacks. Cyberattacks have resulted in catastrophic consequences within 15 minutes of their occurrence (Clarke, RA, Knake, RK, 2010).

In recent years, consideration of advanced persistent threats (APTs), cyberattacks in which hackers gain access to a system or network and remain undetected for a prolonged period, have been on the rise in long-term planning of major national infrastructures such as key information systems, vulnerability analysis, and the systematic and continuous implementation of various technologies. This is because the utilization of general-purpose technology, networks, and media developed for business systems to optimize system operation, resource utilization and cost reduction has gradually increased while closed and independent control systems have been opened to the private sector. A new security threat to the control system will arise (Clarke, RA, Knake, RK, 2010).

Meanwhile, the development of autonomous vehicles (AVs) has brought benefits such as reduction of traffic congestion and fatalities, but technical, social and legal problems are emerging with the introduction of the new technology. The complexity and high connectivity of AVs makes the maintenance of security against cyberattacks very complicated (BCG, 2015). Autonomous vehicles' operational menu data, signal systems, and GPS systems can be exploited for crimes such as infiltration of information by hackers or kidnapping or killing vehicle operators.

As everyone and everything is connected to the network and the services provided through them have expanded to various areas, the risks that may arise in the hyper-digital risk society also extend to the entire function and safety of states, enterprises and individuals.

## III. LIMITATIONS OF CYBERSECURITY POLICY AND THE NECESSITY OF A NEW POLICY PARADIGM

In the second connection society, 'connectivity' is a characteristic which describes all areas' connection to a common network. Connectivity extends cyber threat to one element to all of society, the security of which must be maintained (WEF, 2014). However, the existing domestic cybersecurity response is being led by the state and private enterprises, and its focus is confined to the information system. Therefore, it is difficult to recognize the importance of the general public as well as effective response to the dangers currently threatening society.

Current security awareness is insufficient to effectively deal with escalating risks because it only addresses a portion of the threats to the digital risk society. In this regard, based on Liebig's law of the minimum, even if cyber security policy is well-institutionalized by the state, if the security of an individual victim of a cyberattack is insufficient and the environment for guaranteeing such security it is not established, it is difficult to effectively respond to digital risks and maintain a safe society. In other words, the existing national policy considers only the traditional ICT environment, and does not consider the connectivity, security threat transfer, and security response in all areas of the hyper-connected society, as is absolutely necessary.

In this paper, we propose a new methodology for risk assessment, considering a combination of risk factors and risky environments (Jeong & Yoo, 2010). In other words, it is necessary to supplement existing cyber security policies and establish a policy which takes macro, bureaucratic and global cybersecurity into consideration. As demonstrated by recent accidents in the national infrastructure, damage caused merely by the interruption of the information system has spread to individuals through connectivity. Therefore, it is necessary to recognize the importance of voluntary individual risk management in order to maintain individuals' daily lives. It is necessary to establish conditions which promote improvement and enhance response capability.

In other words, the following policy values should be set in order that security can be considered and implemented in all areas of the hyper-digital risk society to enable integrated and immediate response.

**Table 1.** Hyper-Digital Risk Society Response Policy Value

| concept | component |
|---|---|
| Security for Everyone | All people and objects are connected to the network and the services that utilize them are spreading throughout various public and private domains.<br>New technology and connectivity have allowed many to enjoy unprecedented convenience, but new dysfunction and cyber threats have emerged, and with them the hyper-digital risk society is coming.<br>Since all citizens are subject to cyber threats, it is necessary to deal with cyber security at the environmental level. Therefore, an environment in which all citizens actively participate in cyber security should be established. |
| Security of Everything | In a hyper-digital risk society, security should be considered across all objects, systems, facilities and areas connected to the network.<br>Existing security is confined to information system security and focuses mainly on response in the event of an accident, but future security should have connectivity with other systems, devices, and areas connected with it, not just one information system.<br>In this context, a series of processes should be organized to predict and prevent an occurrence rather than enacting a series of cyber incident responses and follow-up actions. We should aspire to conduct cybersecurity proactively rather than reactively. |

In other words, to realize a safe digital society, it is necessary to complete daily and integrated systematization of safety management through maintenance of preparedness against various types of disasters and accidents and cooperation among risk management authorities and related organizations (Ahn, 2010), as well as public awareness of digital environmental rights should be taken by each individual's own behavior, through which prevention is achieved.

## IV. THE HYPER-DIGITAL RISK-BASED APPROACH: A NEW POLICY PARADIGM IN RESPONSE TO SOCIETY'S VULNERABILITY

Environmental rights are basically the right to live in a healthy and pleasant environment. In the face of serious environmental crises, countries around the world are looking at environmental rights as modern human rights (third-generation human rights) for human survival (Park and Ham, 2015). In particular, the Constitution of Japan proposes protection of interests and the duty and role of protection of the state and individuals in the rights structure of environmental rights. It also explains environmental rights for the purpose of protecting the interests related to life, body, health, personality and property. In order to protect them, it imposes an obligation of infringement against the state and imposes a duty of protection from infringement by others.

Since 1980, the Republic of Korea has designated environmental rights as one of its basic rights in Article 33 of the Constitution. In 1987, the Republic of Korea made its commitment to environmental rights more concrete, saying, "All citizens have the right to live in a healthy and pleasant environment (Article 35, Paragraph 1), 'and' the matters concerning the contents and events of the environmental right shall be determined by Act (Article 35 (2))." In addition, direct mention was made of the so-called 'premise of basic rights' to support the dignity and value of human beings as set forth in Article 10 of the Constitution, the right to pursue happiness, the right to life, physical integrity, and protection under the conditions of the Constitution.

Thus, the right to life includes the right to survival, the right to security from infringement, the concept of security, and the concept of 'safety', meaning the maintenance of a safe state around 'me (each person)'. Therefore, the right to the environment is a right to freedom from the standpoint of preventing the destruction of the environment and enjoying a good environment.

In order to maintain human life and health, it is necessary to eliminate or reduce harmful pollution before actual damage is suffered by individuals or local residents due to environmental destruction. The constitutional position of the environmental right is required.

In general, maintaining a good environment based on the right to pursue happiness, which is a free right, is essential for personal survival. We claim and discuss environmental rights as 'new human rights' centered on conventional human rights. The existing environmental rights should be approved as 'new human rights' and included as constitutional legal rights. It is natural that new human rights are established as a result of changes in the era and a revised meaning has been granted. Therefore, the environmental right is intended to be established by applying it to the existing human rights regulations within the Constitution.

The Japanese Constitution explains the right of protection of the environment right by presenting protection interests and the obligations and roles of national and individual protection. It explains the environmental rights for the purpose of protecting the lives, bodies, health and legal interests related to a

personality or property. In order to protect it, it imposes an obligation of infringement against the state and imposes protection duty from infringement by others.

The right to personal values (life, body, and honor) encompasses the inviolability of the individual's living area (secrecy of the letter and protection of privacy) and freedom of general activity. Considering that the environment is part of the personality which embodies material and spiritual values, the pursuit of human happiness is only possible under certain circumstances and that maintaining and forming a certain environment is the goal of happiness, the destruction of the environment can also be said to be included in the pursuit of happiness. Therefore, it is possible to argue that the right to pursue happiness and personal values are at the same level, and that both rights are environmental rights. In addition, environmental rights have the nature of the moral rights that are established in relation to the natural environment, and their scope, both broad and narrow, is not constant, and is broadly comprised of history, culture, environment, and social and artificial environments.

## V. CONCLUSION

The risk of a digital society is an 'essential risk' incurred in the pursuit of social profit or benefit through the utilization of information technology, and this process is assumed as 'voluntary risk' by users' arbitrary choice (Siegrist et al., 2000). In other words, the risks of the digital society are not necessarily controllable, accidental, or exceptional events, but the inevitable threats posed by everyday products created by social systems and institutions. Therefore, the measures to protect the lives, bodies and property of citizens of the hyper-digital risk society should be considered more specifically.

## REFERENCES


[1] Ahn, Young-hoon (2010), "Activation of the National Disaster Risk Assessment System (NRA) to Enhance Disaster Response Capability", *World & Cities* Vol.7. No.3, pp. 26-33

[2] AhnLab (March23,2013), "The Fourth Industrial Revolution, Changes the Security Paradigm", http://www.ahnlab.com/us/site/securityinfo/secunews/secuNewsView.do?seq=26177

[3] BCG 2015. "The Make-or-Break Questions About Autonomous Vehicles: Revolution Versus Regulation". http://www.bcg.com.cn/en/files/publications/reports_pdf/BCG-Revolution-Versus-Regulation-Sep-2015.pdf

[4] Business Watch (Oct.5,2015), "Internet of Things Era.. 'Things were exposed to hacking'". http://www.bizwatch.co.kr/pages/view.php?uid=15607

[5] Choi, Heung-Suk (2009), "Digital Risk Social Policies", Korea Information Society Agency.

[6] Choi, Myung-gil (2013), "A Study on the Evaluation Method of Control System Security", *Journal of the Korea Institute of Information Security*, Vol. 23 No. 2

[7] Clarke, R. A., Knake, R. K. (2010). "Cyber War: The Next Threat to National Security and What to Do About It". HarperCollins Publishers. New York.

[8] Eun, Yongsun. Park, Kyungjun. Won, Myunggyu., Park, Taejun. And Son, Sanghyuk (2013), "Cyber Physical System Research Trends", *Information Science* 31 (12), pp. 8-15, Korea Information Science Society

[9] Jeong, Gughwan and Yoo, Jiyeon (2010), "A Study on Digital Risk Management for Advanced Information Technology". *Economics & Humanities Society Study Group*, 10-12-04, Institute of Information and Telecommunication Policy

[10] Jo, Hwasun and Park, Yura (2012), "Digital Risk Society and Digital Detox Movement", *Internet and Information Security*, Vol.3 No.4, pp. 3-20

[11] Khan S., L. Yufeng, A. Ahmad (2009). "Hydrological systems through a system dynamics approach". *Environmental Modeling & Software, Vol.*24, No.12. pp. 1363-1372.

[12] Korea Internet Promotion Agency (2014), "Basic Matrix for Cyber Attack Response". *INTERNET & SECURITY FOCUS*, pp. 15-38

[13] Lee, J aeyeol (2005), "Risk Structure Change in Korean Society", Korea Institute of Information and Telecommunication Policy 21st Korea Mega Trend Series (Ⅲ), pp. 05-32

[14] Lim, Jilhwan (2011), "A study on the status and countermeasures of security system vulnerability of control system".

[15] Park, Gyunseong and Ham, Taesung (2015), *Environmental Law* (7th edition), Park Young-sa

[16] Seon, Wonjin. Kim, Doo-Hyun (2014), "The Change of Society and Personal Information Protection", *Journal of the Korean Institute of Communication Sciences*, v. 31 no. 4, pp. 53-58

[17] The Korean economy (Oct. 23, 2016), "The Paradox of the Hyper Interconnection Society Era ... IoT, abused as a 'hacking host' ". http://www.hankyung.com/news/app/newsview.php?aid=2016102374841

[18] World Economic Forum (2014). "The Global Information Technology Report 2014", pp. 35-40.

[19] Wright. G. A. and Schaetzel.T.N. (2013). "Cyber Security: Designing and Maintaining Resilience". Georgia Tech Research Institute.

[20] X. Li, C. Qiao, X. Yu, A. Wagh, R. Sudhaakar, and S. Addepalli (2012). "Toward Effective Service Scheduling for Human Drivers in Vehicular Cyber-Physical Systems". *IEEE Transactions on Parallel and Distributed Systems*. Vol. 23, No.9. pp. 1775-1789.

Ji-Yeon Yoo. "A Study on the Environmental Approach to Digital Risk Response Policy". " IOSR Journal of Humanities and Social Science (IOSR-JHSS). vol. 24 no. 02, 2019, pp. 27-31.