A Study on Changes in the Digital Hybrid Risk Paradigm in the Hyper-Connected Society

Ji-Yeon YOO
Associate Professor
Department of Information and Security Management
Sangmyung University
Seoul City 03016
Republic of Korea

Abstract

The rapid development of an increase in the complexity of information technology and associated networks has raised the possibility of sudden risks and widespread adverse effects. Moreover, new combinations and evolutions in information technology and network arrangements, from recent networked control systems to combinations of traditional business and information technology, cloud computing, and the Internet of Things, are increasing the severity of risk, and there is now a significant possibility of a national disaster. With this focus, this study provides a comprehensive review of information technology risk beyond the technical to the socio-theoretical dimension. Within this framework, this study examines the paradigm shift to a digital hybrid risk society.

Keywords: Digital Hybrid Risk Society, Swift of Risk Paradigm, New Risk Paradigms, Digital Risks, Hyper-Connected Society

1. Swift Risk Paradigm

Throughout the ages and in all societies there has always been risk. The first risk faced by mankind was probably from nature. Natural disasters, climate change, disease, and animal attacks have threatened the survival of people, who have been constantly responding in attempts to protect themselves.

However, risk does not always come from the outside. Since people formed communities to satisfy social desires, there have been consistent risks of social conflicts and misunderstandings, which have often led to violence.
To keep themselves safe, people have found ways to protect themselves. The Industrial Revolution, development of scientific technology, and medical advances could all be seen as effective risk responses. However, these achievements at the same time generated new risks (Dietz et al., 2002); that is, as the world modernized, entirely different technical risks from the previous natural or social risks arose (Jones, 1993). Technical risks are risks that have been brought about by technological developments or the natural or artificial use of such new technology.
Risks can be categorized into natural, societal, and technical, depending on the cause (Jones & Hood, 1996)(see Figure1). Natural risks are events that occur from rapid changes in natural phenomena or from natural disasters such as floods, droughts, or earthquakes, which are unrelated to human activity or artificial technology. Societal risks are incidents caused by human behavior, such as fraud, theft, and violence. Technical risks arise from human error or technical system failures, such as the collapse of a building or bridge, an explosion at a plant, or contamination.

As modern society evolves with rapid achievements in technological development and improvements in society, risks and the associated assessment of risks are going through a paradigm shift (Jones, 1993; Jones & Hood, 1996; Sim, 2000). Scientific technology and new information technology are providing people with a rich, convenient life, far from the traditional risks that have previously plagued society. However, these same scientific and information technology advances have created a new epicenter for technical risks. While the proportion of the disasters caused by naturally occurring risks is decreasing, disasters related to the use of technology have been rapidly increasing (Kim, 2009). In other words, while naturally occurring and societal risks have decreased, as technological development expands, so too does the level of technical risk (see the right side of Figure 1).

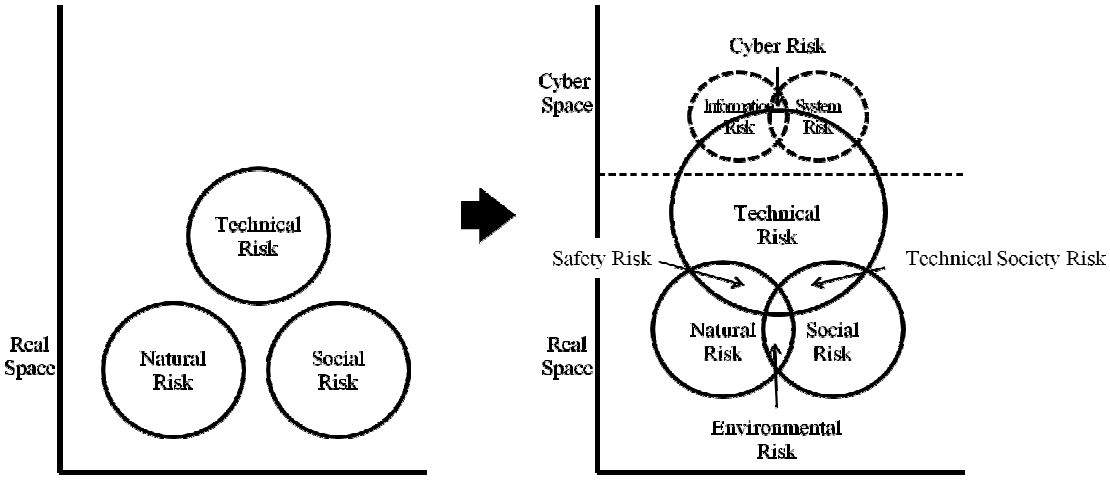

Figure 1: Risk Paradigm

Specifically, the risk paradigm shift has three main characteristics. The first is the appearance of a hybrid risk caused by the interaction between the risks; that is, natural, societal, and technical risks now have a dual nature as they overlap within the risk paradigm. For example, natural disasters such as desertification and global warming are new phenomena rather than genuinely naturally occurring risks, as these are risks that have been created or worsened by human-caused changes to the natural environment. Therefore, environmental risks are a different concept to natural disasters. There are also safety risks that are the result of technical risks, such as flooding resulting from errors in a dam management system caused by the information system used to manage the natural environment. Other technical risks can be intentionally generated by humans using advanced technology, such as terrorism, anthrax, or the collapse of buildings (Sim, 2000).

The second characteristic of the risk paradigm shift are the new technical risks created by the growing dependence on cyberspace. The development of information technology has led to an increase in system risks such as system errors and failures, database information exposure, and the possibility of remote access to vital information. There are also cyber risks that intentionally trigger information overload, privacy infringements, computer crime, and system errors through hacking, virus distribution, and information control and misuse beyond the system or information risks (Ferrell, 1996). These risks are causing increasing concern as they are new risks quite separate from natural disasters caused by natural phenomena, such as floods or earthquakes (Kim, 2008).

The third characteristic of the risk paradigm shift is the expansion of the technical risk realm. For instance, in cases of apparent natural risks such as unusual rainfall, global warming may be the cause. In this light, such a risk can be seen connected to societal risks because of society's rapidly increasing use of fossil fuels and to technical risks because the unusual rainfall is the result of the technical developments that led to the sudden upsurge in fossil fuel use (Lim et al., 2003; Yoon, 2003).

It is also expected that there will be a new risk paradigm shift as technology advances and becomes the essential infrastructure underpinning the whole society. This means that most risks are expected to be related to system errors or the technical system design management (Yoon, 2003). Risk structures are changing as the risks directly or indirectly associated with technology interact with socioeconomic systems (Yoon, 2003). With these ever present risks, security deficits are also becoming more obvious due to unexpected or unprepared-for crises and disasters (Kim, 2000).

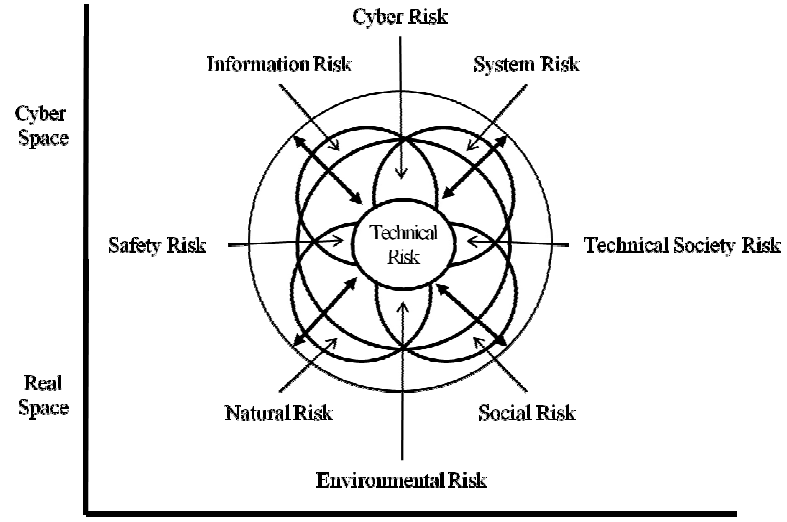

Figure 2: New Risk Paradigms

As shown in Figure2, as information technology and the network are coupled with a majority of the systems that directly or indirectly affect all society, the risks expand, reproduce, and are clustered around the centrally placed technical risks. Therefore, of all the technological achievements, information technology in particular is causing a resonance through its interactions with the political, economic, and societal systems. Genuine natural risks, such as floods or earthquakes, can be controlled and managed by information technology, but new risks arise from errors within the information technology network. Societal risks such as violence and fraud can be reduced by the correct application of information technology, such as psychological therapy or imprisonment, but new risks that utilize the information system network, such as cyber violence and cyber fraud, are emerging in their place.

Risks are sometimes intensified by the highly sophisticated networks and interactions between environmental risks, safety risks, and techno-social risks. At the same time, there is an increase in cyber risks that attack the network in the form of viruses, malicious codes, or inappropriate access. Cyber risks used to be restricted only to cyberspace but the range of information risks, such as the exposure or release of information and system risks caused by system errors, has expanded to the risk of physical damage to social sectors that are now connected to the Internet.

The aforementioned new risk paradigms have three characteristics. First, the essence of the risks in the new risk paradigms are hybrid risks centered around technical risk. There have always been technical risks, but these tended to be personal, local, unstructured, and static. On the contrary, in the future, when all society is digitally integrated, widespread technical risks are expected to be the foundation of risk as information technology will be the structural base of society. These technical risks are dynamic and manifest comprehensively, globally, and structurally, and can occur in any place, at any time (Yoon, 2003; Kim, 2009).

Second, risks happen simultaneously in cyberspace and real space, and are global. The various elements of the risks dispersed in cyberspace and across real space combine and enlarge globally, leading to unexpected results (Lee, 2005). There are many elements that may incite this hybridization and globalization of risk but the root cause is information technology and the extensive network. Most systems in today's social sectors, such as transportation, flight, electricity, medical treatment, and businesses, are directly or indirectly related to information technology. Because of this, if a risk occurs on one side, it becomes the epicenter of the technical risks that can instantly cause a tremendous ripple effect in many different places, the so-called "network domino effect" (Kim, 2009).

Third, the unpredictability and uncertainty of the risks are increasing. Previous risks tended to occur regularly and repeatedly, but as risk becomes hybridized and generalized it is difficult to identify when and in what forms it will arise. As new risks overcome existing risks and contribute to the technical development that improves social benefits, it is also difficult to decide if they need to be confronted or if they can be endured.

This study defines the risks in this new risk paradigm as digital risks. Digital risk means the possible threat from a malicious effect on the human safety and social environment as the systems in social sectors are linked to information technology and the associated networks.

2. Types of digital risks

Based on Perrow's risk model, digital risks can be classified into four types. Perrow argued that the risks in the modern society were caused not by an individual unit but by a system paired at a hybridized and diverse level (Perrow, 1984; Yoon, 2003; Lee, 2005). Moreover, as Perrow saw these risks not only as a problem of technology but as being able to lead to further expansion and stimulation, he provided a theoretical foundation for the digital risks that would arise when social sector systems became coupled with information technology and networks.

Perrow's risk model is based on the level of interactions and dynamics in the coupling method between the risk elements. Interactions can be divided into linear interactions and complex interactions. Linear interactions, although unplanned, occur visibly and in a predictable order. The coupling between elements is loose and each element is physically separated and has its own unique characteristics. Complex interactions, however, are difficult to predict and occur on impulse or invisibly in an unplanned and chaotic order. These interactions have tense coupling with no gaps, margins, or buffers between two elements (Perrow, 1984; Yoon, 2003).

Considering the interactions and the coupling methods between these risk elements in the information technology network, and the influence caused by the degree of coupling with other sectors, digital risks have been classified into simple and exploding, simple and amplifying, complex and exploding, and complex and amplifying, as shown in Figure 3.

Type 1 simple-and-exploding risks are caused by local and predictable weak points, and have less interaction between the elements and a loose coupling in which the elements are physically separated. These risks include the various adverse effects of cybercrime related to the exposure or release of information and information services through errors in information software, the information system, or by intentional low-level access.

Interaction \ Coupling Method	Loose	Tense
Linear	**Type 1. Simple-Exploding** Risks caused by local and predictable weak point e.g.: Information release, cyber crime	**Type 2. Simple-Amplifying** Dreadful risks caused by individual system failures e.g.: Y2K etc.
Coupled	**Type 3. Complex-Exploding** Networked unpredictable risks e.g.: Viruses, malicious codes, hacking	**Type 4. Complex-Amplifying** Dreadful unknown risks networked beyond the space e.g.: Accidents in main infrastructure control system

Figure 3: New Risk Paradigms

In the Type 2 simple-and-amplifying risks there is less interaction between the elements and they occur when these complex risk elements are coupled. These risks cause failures in an individual system and may be intentional or unintentional, but have the significant possibility of expansion and reproduction as they can spread from an individual system through cyberspace and into real space. The Y2K issue was an example of this type of risk as it started from a simple system failure and spread toall information systems and social sectors.

The Type 3 complex-and-exploding risks are local, networked, have a loose coupling but a greater level of interaction between the elements, and are unpredictable. Intentionally spread viruses, malicious codes, and hacking are examples. However, they often arise in a target subject area or within a service, but also expand gradually through the network. Generally, they are unidentifiable at a personal level due to the complexity of interactions andnetwork expansion, but become noticeable as they spread across a larger region of the network.

In the Type 4 complex-and-amplifying risks, there are many interactions between the complex coupled risk elements, which can cause catastrophic and unknown risks beyond individual system failure. The main infrastructure coupling with the information technology network is an unpredictable potential threat in cyberspace as well as in real space. A good example of these risks are control system errors in the main infrastructure. Only information technology failures or small errors in real space can damage social infrastructure such as electricity, energy, transportation, and communications, any damage to or destruction of which can lead to societal chaos. If a small, unanticipated accident occurs in this complex tightly coupled system, it is highly likely that it will accelerate and lead to a catastrophic disaster (Kim, 2004).

In other words, the combination of complexity and tight coupling makes the occurrence of accidents inevitable and at the same time stimulates expansion. Systems composed of highly complex subsystems have millions of interactions every minute, making it extremely difficult to foresee and/or prevent the risks. The definitions for the concepts and the types of digital risks summarized above are significant as this is not just a conceptual discourse but a way to acknowledge the differences so as to develop adequate plans for each scenario, to plan against the risks, as well as to determine their causes. In short, since the interactions and the coupling of digital risks are becoming more complicated as they become more networked, they can be classified by increasing magnitude; Type 1–simple and exploding <Type 2–simple and amplifying <Type 3–complex and exploding<Type 4–complex and amplifying; and therefore proper risk management is required to address each type.

3. Digital hybrid risk society

German sociologist Ulrich Beck was an early proponent of the recognition of the risk society and promoted dynamic discussions in this area. Basically, he asserted that modern systems knowledge and the advanced technologies and behavioral patterns that developed to overcome the pressures and deficiencies of the premodern era are now, paradoxically, functioning as the main sources of risk (Beck, 1992). He then named this so-called "modern paradox" the risk society (Lee, 2005). He saw the risk society as one where unpredictable risks increase as the development of more and better scientific technologies advance affluence in the postmodern society. People in the risk society are exposed to risks induced by scientific technologies, but at the same time they enjoy the material richness from unlimited technological development.

Further, as society continues to advance its information network, the possibility of becoming a risk society is growing (Lee, 2005), with this intensification moving society toward the hyper risk society (Lee, 1998) or the information risk society (Korea Internet & Security Agency, 2008; Choi, 2009).

With the movement into the information society, where information technology, information systems, and information networks become the centers of production and services, the threats produced from secondary, non-natural, artificial uncertainty, and structural or uncontrollable potential risks broaden even further. Information systems, software, and automated systems can be found in all corners of society, from office computers to medical equipment and nuclear plants, thus creating a network of complex interactions never experienced before. Therefore, if these risks are realized due to failures and errors or intentional and malicious access to information technology, the reaction is often chaotic and disorganized. Classic examples are the Chernobyl disaster in Ukraine, the Patriot missile crash in the Gulf War, and the excessive radiation from cancer treatment equipment in Canada.

As the information society becomes highly sophisticated, the environment becomes increasingly controlled by information technology systems, which become larger and more complex as dependence increases. This growth in complexity is in inverse proportion to trust ininformation technology systems, so the probability of system error increases. This is the dilemma of the developed information society.

The dilemma of the developed information society will intensify with the movement into the hyper-connected society, which is the point at which the entire society digitally converges. When examining the social and technical changes expected in the hyper-connected society, the dilemma of the developed information society intensifies. The digital features that will categorize the hyper-connected society are ubiquity, generalization, convergence, intellectualization, and individualization, which will cause the following digital risks.

Ubiquity and generalization. As digital devices and systems become highly multifunctional and have increased storage space, there is the possibility of increased attacks. Therefore, as sophisticated information technology begins to influence every corner of human life, the risks become ubiquitous and there is higher uncertainty as the digital risks can occur anywhere, at any time. Recent optimized multifunctional personal devices, such as national infrastructure control systems, cloud computing, and smart offices, face digital risks every day. The convergence between cyberspace and real space thus increases the risk of threats against people, as objects can be controlled that affect people in the real space. As the degree of coupling and dependence between people and information technology rises, the U-medical service, for example, could directly and critically threaten the life of a person through weak points and information technology errors.

Convergence. The complexity of digital risks intensifies as information systems become integrated into the ALL-IP network.

This means that everyone is connected through telecommunications systems and all social sectors and systems are interlinked by the network and interact using a combination of traditional business and information technology. Therefore, through the national IT infrastructure, the border between cyberspace and the real world dissolves. This societal digital convergence means that any attacks or technical errors affect the entire society, causing unpredictable risks. The coupling of the national infrastructure such as transportation, telecommunications, broadcasting, medical treatment, energy, and finance with information technology creates a risk that can paralyze cyberspace and the real world through attacks on information technology's weak points. The cyberterrorism case in Estonia in 2007 actually proved that information technology security can become a risk at the state level.

Intellectualization and individualization. Due to the nature of intellectualized digital devices, the risk of malfunctions by technologies connected directly to people's daily lives as humans can become a threat to human life. Because of the increased complexity of intellectualized and individualized information technology, the probable risk of malfunction increases, as the potential risks are spread over organizations, through society, to the state level.

Because individualized digital devices and systems are not limited to an individual but are connected with organizations, society, and the state to which the individual belongs, it is more likely that even small risks can result in catastrophic social and national risks. Through ubiquity, generalization, convergence, intellectualization, and the individualization of information technology in the digital age, uncertain, complex, and unpredictable risks reside everywhere. In the coming hyper-connected society, any attack on a weak link can cause a domino effect, intensifying the probability of greater potential risks.

This study defines the intensified risk society arising from the advanced hyper-connected society as the digital complex risk society. A digital complex risk society is a "society where the risks induced by information technology as the social infrastructure are expanded and reproduced over social systems and complexly exposed to cyberspace and the real space as the entire society is digitalized and the borderline between the cyberspace and real space becomes ambiguous."

Two characteristics of the digital complex risk society within the hyper-connected society are the maximization of network risks, and the expansion of the risks beyond the border between cyberspace and real space (Lee, 2005).
A maximization of network risks results from the intensified interdependence of the information technology network, as a minor impact in one section can spread over the network within a short time, creating a critical threat. The maximization of network risks is a new type of risk caused by qualitative changes in the network. The network goes through a phase transition when the average number of the connected links of an individual to the network exceeds a certain critical level. In other words, the individual is connected to the network, meaning, conversely, that the entire network is also connected to the individual.

Secondly, the maximization of network risks can cause a network domino effect. The instant spread of the risk elements from the individual domain can cause overall system collapse across the world in a short time. Even a trivial matter can lead to an unprecedented new type of risk when delivered through the qualitatively modified network, thus causing entire system failure. For example, if someone knowledgeable about Internet structure attacks 1% of an important node, this action can paralyze one half of the entire Internet function, and a 4% attack can completely fragment the Internet (Albert et al., 2000). Third, the maximization of network risks could be seen as a tipping point. One small weak point in an individual network can destroy the whole the moment it enters the network. The higher the level of networking, the stronger is the power of the influential risks and the larger the potential destruction.

All these aspects of the maximization of network risk expand the risk possibilities beyond the border between cyberspace and real space. A space in the digital society becomes integrated with the network-connected space.
With enhanced integration between logic networks and physical networks, the development of information technology has led to a coordinated relationship transcending the border between cyberspace and the real world. The reciprocity and real-time response of information technology has created a space that responds to human behavior and movement to the extent that risks in real space are immediately reflected in cyberspace, while information technology risks materialize in the real space. These shifts in the digital society space paradigm amplify risks as the digital hybrid risk society begins to interact with the real space beyond cyberspace. That is, future digital risks will possibly expand and aggravate the damage from disasters resulting from the risks, as they will interact simultaneously, directly, and indirectly in both cyberspace and the real world.

References

Albert R., Jeong H., Barabási A.L. (2000). "Error and Attack Tolerance of Complex Networks." *Nature 406*: 378-482.

Beck, Ulrich (1992). *Risk Society: Toward a New Modernity*, London: Sage Publications.

Choi, H. S. (2009). "A Study on the Policy Response Measures to Digital Risk Society." *Korea Agency for Digital Opportunity and Promotion:Research Series 08-14*.

Ferrell, Jeff (1996). *Crimes of Style*, Boston: Northeastern.

Jones, D. K. C. (1993). "Environmental Hazards in the 1990s: Problems, Paradigms andProspects."*Geography*, Vol.78. No.339: 161-165.

Jones, David K.C. and Hood, Christopher (1996).*Accident and Design: Contemporary Debates in Risk Management*. London and Bristol: UCL Press.

Kim, D. G. (2000). "A New Perspective on Popularization of Scientific Technology." *Science and Technology Policy*, Vol.122.

Kim, J. G. (2008). *Cyber Trend2.0*. Seoul: Jipmoondang.

Kim, J. G. (2009). "Cyberization of Technical Risk and Privacy Rights." *Social Theory*.Vol.35.

Korea Internet & Security Agency (2008). "Information Security Policies in Ubiquitous Environment." *Information Technology Policy Development 07-policy-74*.

Lee, J. Y. (2005). "Changes in Risk Structure in Korean Society." *Korea Information Society Development Institute: Megatrend Korea 21 Century Series(Ⅲ) 05-32*.

Lee, Y. S. (1998). "Risk Society is Also Named as the Hyper Risk Society." *Hankyoreh 21*, Vol.202.

Lim, H. J., Goo, D. W., Kim, J. Y., Seo, M. G., Seo, Y. J., Sim, S. W., Lee, S. Y., & Lee, J. Y. (2003). *Risk and Safety in Korean Society*. Seoul National University Press.

Perrow, C. (1984). *Normal Accidents: Living with High-Risk Technology*.Basic Books.

Sim, S. W. (2000). "Possibility of Patience of Risk and Rational Practicability of Risk Management." *Journal of Sungkonghoe University*, Vol.15.

Thomas Dietz, R. Scott Frey, and Eugene A. Rosa.(2002). "Risk, Technology, and Society." Riley E. Dunlap and William Michelson (eds.). *Handbook of Environmental Sociology*. Westport, CT: Greenwood Press: 329-369

Yoon, J. H. (2003). "Structure and Procedure of Technical Risk." *Science & Technology Studies*, Vol.3.