Institute for Journalism, Media & Communication Studies, Keio University

KEIO MEDIACOM WORKING PAPER

NO. 3

RISK SOCIETY, CYBERTERRORISM, AND KOREA'S NETWORK CULTURE

DAL YONG JIN

OCTOBER 2016

Risk Society, Cyberterrorism, and Korea's Network Culture

Dal Yong Jin
Associate Professor
School of Communication
Simon Fraser University
djin@sfu.ca

Abstract

By employing Ulrich Beck's risk society and the critical approach on technology as analytical frameworks, this paper investigates negative aspects of digital technologies in tandem with cyberterrorism. It analyzes the ways in which the rapid growth of digital technologies has led to adverse effects, in particular, cyberterrorism and/or cybercrimes, by exploring the relationship between new technology and cyberterrorism. It critically raises the questions of technical values and ideas of digital technologies regarding cyberterrorism. It discusses the relationship between people and technology to develop a research framework that would help to expedite research on digital technologies by drawing insights from the analysis of risk society. It therefore aims to contribute to this ongoing debate of critical research on new technology by exploring rapidly growing digital technologies and their relationships with cyberterrorism and/or cybercrimes.

Keywords

Risk society; cyberterrorism; new technology; the Internet; informatization; information economy

Introduction

The swift growth of digital technologies, including the Internet and broadband services, has provided new opportunities because many people are able to enjoy their online activities and corporations develop new business models. The Internet, broadband services, and smartphones have greatly contributed to the development of the information economy and culture in the 21st century. However, new technologies are also blamed for the emergence of several negative effects on our information society. The rapid deployment of the Internet and broadband services has engendered a number of side effects from informatization, which is expected to become a greater challenge as people become more digitally sophisticated.

While there are several dystopian aspects of digital technologies, cybercrimes and/or cyberterrorism have become some of the most significant global issues in recent years. As Ulrich Beck (1999; 2002) argued, technological achievements, such as in genetics, biotechnology and reproductive technology, were producing new kinds of risk, because their unexpected side effects have created new risks as well as new opportunities in our society. What he emphasized was that the nature of risk had changed, from natural to man-made risks and from natural disease to science and technology involved risks. Digital technologies have especially brought about cyberterrorism, which is a new kind of risk. Long before computer communication and network technology were introduced, terrorism had been used to describe "criminal conducts" (Schjolberg, 2007, 1). With the swift growth of digital technologies, however, cyberterrorism has become one of the major threats and risks to our daily lives. Computer experts, security personnel and policy makers in many countries fear that cyberspace—referring to "the realm of computer networks in which information is stored, shared and communicated online;" and therefore, "cyberspace is not purely virtual," because "it comprises the computers that store data

plus the systems and infrastructure that allow it to flow" (Singer and Friedman, 2014, 13)—is a target for terrorists.

This anxiety, needless to say, came with the clear warning sent by the terrorists' use of and expertise in Internet and broadband services after the September 11 terrorist attacks on the U.S. in 2001. Since 2001, several theoreticians have identified cyberterrorism as including the possibility of physical attacks on information structure and functions. What they emphasized is that cyberterrorism could represent a new stage in the spread of terror, because it occurs in and via cyberspace. As Verton points out (2003a, xx),

> cyberterrorism is the execution of a surprise attack by a subnational terrorist group or individuals with a domestic political agenda using computer technology and the Internet to cripple a nation's electronic and physical infrastructures, thereby causing the loss of critical services, such as electric power, emergency 911 systems, telephone services, banking systems, the Internet, and a host of others.

Dorothy Denning (2002; 2003) has also put forward an admirably unambiguous definition in her testimony on the subject before the House Armed Services Committee in May 2000:

> Cyberterrorism refers to unlawful attacks and threats of attacks against computers, networks and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear. Attacks that lead to death or bodily injury, explosions, or severe economic loss would be examples. Serious attacks against critical infrastructures could be acts of cyberterrorism, depending on their impact. Attacks that disrupt nonessential services or that are mainly a costly nuisance would not (Weimann, 2004, 4)

Cases of cyberterrorism include the use of information technology (IT) to organize and carry out attacks. Forms of cyberterror, such as the dissemination of viruses and hacking as well as circulation of misinformation are on the rise (Misra, 2003). Government officers, computer and security experts, and ICT scholars have acknowledged that terrorists are using information infrastructure to bring havoc to computer systems and thereafter cyberspace and user safety (Sofaer et al., 2001, vii; Garfinkel, 2002; Schjolberg, 2007).

In the wake of the growing concern of cyberterrorism, many governments, corporations, and cybersecurity experts have paid attention to cybersecurity measures as a significant means to protect our society from cyberterrorism (Kizza, 2002). These experts and governments are keen about the nature of this kind of new risk, because the nature of the risks threatening our contemporary society, including cyberterrorism, is global (Beck, 1999; 2002).

This paper employs Ulrich Beck's risk society and the critical approach on technology as analytical frameworks for examining negative aspects of digital technologies in tandem with cyberterrorism. It analyzes the ways in which the rapid growth of digital technologies has led to cyberterrorism and/or cybercrimes, by exploring the relationship between new technology and cyberterrorism. It critically raises the questions of technical values and ideas of digital technologies regarding cyberterrorism. It discusses the relationship between people and technology to develop a research framework that would help to expedite research on digital technologies by drawing insights from the analysis of risk society. It therefore aims to contribute to this ongoing debate of critical research on new technology by exploring rapidly growing digital technologies and their relationships with cyberterrorism and/or cybercrimes.

Understanding Cyberterrorism and Risk Society

As digital technologies, from the Internet to broadband, and again to social media and smartphones, have substantially influenced our daily activities, several theoreticians critically analyze the dystopian nature of these new technologies. As Tsfati and Weimann (2002, 318) observed;

> Utopian visions of a virtual state in which citizens hold daily common discussions, communicate needs and demands to their representatives, and vote on various referenda (all using communication by computers) have been raised by thinkers and researchers…. However, with the enormous growth in the size and use of the network, it became clear

> that the realization of this ideal was premature. In addition to the fact that this utopian vision was challenged by pornographic and racist content on the Internet, it also became apparent that radical terrorist organizations of various kinds—anarchists, nationalists, separatists, revolutionaries, neo-Marxists, and fascists—were using the network to distribute their propaganda, to communicate with their supporters, to create public awareness and sympathy, and even to execute operations.

They argued that technology contributes to maintaining deeply rooted power inequalities in today's so-called information or knowledge societies (Saravanamuthu, 2002; Mansell, 2004). Dyer-Withefold (1999) also criticized hierarchical managerial and economic models and the type of technological innovation they breed because such technological innovation undermines democratic practices.

In addition, several scholars (Schiller, 2000; McChesney, 2000; Boyd-Barrett, 2006) elaborated on this analysis with detailed research into the operations of capitalist media. This suggests an examination of digital technologies to show how the structure of "global networks and digital information flows and their consumption are informed by predominant and alternative principles, values, and power relations" (Mansell, 2004, 99). As McChesney (2000) argues, the whole driving force behind the rapid growth of ICTs, including the Internet and broadband services, considers new technologies as profitable business and useful for the exploitation of society rather than as a public service. In fact, "technologies embody social choices made by those with power over their construction" (Dyer-Witheford, 1999, 52). As these theoreticians have argued, a technological process stimulates advances of general utility, but the concrete form in which these progresses are realized is determined by those in power over its construction (Hart et al., 2014).

More specifically, when the debate goes to cyberterrorism, which has rapidly become part of not only negative aspects of digital technologies but also the major part of risk society in the 21st century, many theoreticians express deep concerns. In particular, Ulrich Beck (2002, 39)

right after the September 11 attacks pointed out, "ever since that moment, we've been living and thinking and acting using concepts that are incapable of grasping what happened then…. No one has yet offered a satisfying answer to the simple question of what really happened." What Beck (2002, 41) claimed is that we are living in a 'world risk society' and that "we enter a world of uncontrollable risk and we don't even have a language to describe what we are facing." Beck clearly argued that world risk society does not "arise from the fact that everyday life has generally become more dangerous. It is not a matter of the increase, but rather of the de-bounding of uncontrollable risks" (41). He explained that this "de-bounding is three-dimensional: spatial, temporal and social:"

> In the spatial dimension we see ourselves confronted with risks that do not take nation-state boundaries, or any other boundaries for that matter, into account…In the temporal dimension, the long latency period of dangers, such as, for example, in the elimination of nuclear waste or the consequences of genetically manipulated food, escapes the prevailing procedures used when dealing with industrial dangers. Finally, in the social dimension, the incorporation of both jeopardizing potentials and the related liability question lead to a problem, namely that it is difficult to determine, in a legally relevant manner, who causes environmental pollution or a financial crisis and who is responsible, since these are mainly due to the combined effects of the actions of many individuals (41).

Of course, not everything changed after the September 11 attacks. Instead "it only accelerated patterns of the 1990s when Western policymakers understood the world in terms of globalization and risk. This trend raised significant questions about security and war. Ulrich Beck's *World Risk Society* offers important insights into the transformation of war debate. Globalization of risk has affected contemporary war" (Heng, 2006, 86). Security risks, including transnational terrorism, "figured prominently as spurs to war" (Heng, 2006, 86). This implies that as he clearly pointed out, modern risks are mainly transnational, and globalization has expedited the risks, while asking governments and businesses to work together beyond their national boundaries. These governments and businesses have to confront and control

cyberterrorism because "risk inherently contains the concept of control," which "presumes decision-making" (Beck, 2002, 40). They particularly understand that world risk society, in this case, driven by the possibility of cyberterrorism has been global in nature (Beck, 2002; Heng 2006), and they develop global cybersecurity measures. As Jarvis (2007, 32) points out, "in the global risk society, no one any longer knows with certainty the extent of the risks we face through our collective technologies and innovations." Therefore, the present study will shed light on the continuing debates on risk society in conjunction with cyberterrorism.

The Growth of Digital Technologies as the Tool of the Information Economy

From the Internet to smartphones, the swift advancement of infrastructure in the IT sector has expedited the growth of digital society. Most of all, the number of Internet users has soared globally, from 38 million in 1994 to 1 billion in 2005, then again to almost 3 billion users in 2014 (Computer Industry Almanac, 2006; Internet Live Stats, 2016). Until the very early 21st century, most Internet hosts were in Western countries because of their advanced technology, capital, and their aggressive government policies (OECD, 2001, 112). However, developing countries in Asia and Latin America have acknowledged the importance of the Internet and initiated its development in recent years, consequently the number of subscribers as well as Internet hosts in developing countries, including China and India, grew. In terms of Internet hosts, at the end of 2012, Brazil, China, Mexico, and Russia were all in the top 10 (World FactBook, 2013). The Internet is established as an important delivery channel, and broadband usage is playing a key role in the growth of the digital economy and society (Menon, 2006). Moreover, it is indifferent to distance and is quickly expandable. Together with a plethora of

other types of user equipment, information technologies are changing the way networks are used to transmit, receive and manage information (Frieden, 2001, 17-18).

In the midst of the rapid growth of the Internet, broadband service became a cutting-edge business for ICT companies in many countries because high-speed Internet was viewed as a significant part of the high-tech infrastructure of an information society. Broadband provided high-speed access and always-on connections, which resulted in a substantial change in patterns of Internet use. As the *New York Times* reported, a broadband connection typically changes people's Internet usage patterns, "making it much easier and more appealing for listening, viewing still photographs and watching video" (Kirkpatrick, 2003). Broadband services made significant progress, not only in infrastructural facilities but also in increasing the number of Internet users and the expanded application of the Internet. Broadband allowed for what several media and ICT corporations badly wanted: high speed access and always-on connections for a range of lucrative services, including telecommunications, entertainment, shopping and, education (Schiller, 2000).

For many countries, both Western countries such as the U.S. and Canada and developing countries, including China and Korea, how to develop broadband services was one of the most significant priorities on these countries' political-economic agendas (Jin, 2011). For example, former Federal Communications Committee (FCC) Chairman Michael Powell (2001) in the U.S. stated that broadband "has certainly become the central communications policy objective in America." John Chambers, CEO of Cisco, also pointed out that "broadband should be a national priority in this century just as putting a man on the moon was an imperative in the last century" (Papalardo and Martin, 2002, 8). Countries around the world, including the U.S., Canada, China,

Korea, and Hong Kong, and businesses such as AT&T, Verizon Communications, and SK Telecom are pitching broadband as the key to the future of economic growth.

Consequently, high-speed Internet connections have grown exponentially around the world. As one of the most active regions in the world, East Asia has shown the fastest growth in the Internet and broadband services in recent years. Korea had particularly become the global leader in terms of broadband penetration per 100 inhabitants between 2000 and 2005, although it has continued to drop its rank due to its market saturation in the 2010s. According to a report for the first quarter of 2014, for example, 36% of the broadband connections in the U.S. were considered high speed, at speeds of at least 10 megabits per second, which put the U.S. at seventh on the list of countries. In this category, Korea, which has been well known for its super-fast broadband speeds, topped the list at 77%, followed by Japan (54%), Switzerland (45%) and Netherlands (44%) (Fitzgerald, 2014).

As expected, the main reason for growing the number of broadband subscribers is for mega-profits. With the rapid growth of the Internet, online transactions, known as electronic-commerce (e-commerce) have increased over the last several years, from $54.9 billion in 2003 to as much as $1.672 trillion in 2015, and are expected to grow to $3.551 trillion in 2019 (Technology Briefing, 2004; Linder, 2015). The Asia-Pacific region is growing faster than any other at a rate of 35.2% year over year, because China, Japan, and Korea are included in the top 10 e-commerce countries in 2015 (Linder, 2015). The issue is that digital technologies cannot guarantee only economic growth. As Robins and Webster (1999, 122) pointed out, "information is thought to be the key to a new phase of economic growth, but it also causes severe damage for today's information society." While enhancing the quality of people's lives, new digital technologies have caused several social problematics, including cyberterrorism.

Critical Interpretation of Digital Technologies and Cyberterrorism

The threat of cyberterrorism has increased with the growth of the Internet and broadband services throughout the world because high-speed Internet communication allows terrorists to be decentralized, and thus it is harder to identify and observe their attacks (Bolz et al., 2001, 93). As Tsfati and Weimann point out (2002, 318), "it became apparent that radical terrorist organizations of various kinds—anarchists, nationalists, separatists, revolutionaries—were using the network to distribute their propaganda, to communicate with their supporters, to create public awareness and sympathy, and even to execute operations." In particular, broadband is a likely means of attack, because it can provide easy, always-on, and high-speed access to computer systems and data.

As broadband services have rapidly grown, the number of computer security breaches has been on the rise. While there are several different forms of cyber security issues, cyberterrorism has especially brought about tremendous financial losses throughout the world. For example, cyberattacks caused $12 billion in damage and economic losses around the world in 2001 alone (Squitieri, 2002). This trend toward rapidly more disruptive and economically damaging cyberattacks has continued throughout recent years. The British insurance company Lloyd's estimates that "cyberattacks cost businesses as much as $400 billion a year in the mid-2010s" (Cybersecurity Ventures, 2015). Several Asia-Pacific countries, such as Korea, Japan, Singapore, Australia and New Zealand are especially vulnerable due to the recent growth of digital technologies. Attacks on sensitive areas of government are growing more sophisticated in these countries (Lewis, 2016).

Due to the rapid growth of cyber terrorism, many governments and businesses throughout the world have started to pay much attention to cybersecurity in the 21st century. The U.S. government spent only $938 million in 2000 to protect federal computer systems. In the business sector, the situation was not far different (Lemke, 2002, 31). However, increased cyber security concerns after the September 11 attacks in 2001 have stimulated spending for cybersecurity (Jin, 2016). In his fiscal 2017 budget proposal, President Barack Obama of the U.S. asked for $19 billion for cyber security across the U.S. government, an increase of $5 billion over 2016 (Volz and Hosenball, 2016). President Obama (2016) believed that "networks that control critical infrastructure, like power grids and financial systems, are being probed for vulnerabilities. Cyber threats are among the most urgent dangers to America's economic and national security." As market research firm Gartner (2015) reported, global spending on IT security was set to increase 4.7% in 2015 to $75.4 billion, and the world would spend $101 billion on information security in 2018.

In the case of Korea, the methods of cybercrimes have become more diversified and sophisticated. Computer-related crimes in Korea have indeed increased. Although the rapid growth of broadband services has contributed to the growth of the national economy, the swift deployment of high-speed Internet has resulted in the growth of cyberterrorism and/or cybercrimes in Korea. According to the Korean National Police Agency (2016), computer-related crimes increased 87.6% over the period 2004-2015, from 77,099 cases in 2004 to 144,679 in 2015. What is interesting in the Korean context is that the PC bang (Internet café) has played a key role. For example, in 2002, when 104,888 computer-related crimes were caught, about 70% of cybercrimes primarily occurred in Internet cafes because cyberterrorists easily hide their

identities in public Internet cafes, which are connected to high-speed Internet (Korean National Police Agency, 2003).

Since the end of 2002, Internet cafes in Korea are equipped with high-speed leased lines and multimedia computers, and offer high-speed access to the Internet for almost one dollar per hour. Internet cafes were first introduced during the 1997 economic crisis with only 100 Internet cafes. However, the numbers rapidly increased and they became very popular, with 13,600 in 1999 and approximately 25,000 in May 2002, and still more than 20,000 in May 2006, although the number of Internet cafes has significantly decreased since 2010 and there were only 13,146 in 2014 (Hwang, 2002; Upgrade Business, 2003; Taylor 2006; Korea Creative Content Agency, 2015). These Internet cafes have played key roles in facilitating cybercrimes and cyberterrorism, because, again, cyber terrorists or criminals can easily hide their identities using computers in these cafes.

When we track cybercrimes by perpetrators' occupations, students (high-school and college) composed the largest group of suspects of cybercrimes at 40%. By age, teens made up 44% of suspects, followed by those in their twenties (33%) (Korean National Police Agency, 2002). Therefore, teens and 20-somethings accounted for 77% of total suspects of online crimes in 2001, which means the majority of cyber-related crimes and/or terrorism were committed by young high-school or college students, as a reflection of youth computer expertise. The proportion of teens has continuously decreased while the number of those in their twenties has continued to increase in the early 21st century. In 2013, teens consisted of only 16.4%, but those in their twenties accounted for 41.6% (Korean National Policy Agency, 2016). Two major reasons caused this new trend: one is the rapid increase in the number of smartphones since 2010 right after Korea introduced its own smartphones in 2009, and the other is the introduction of

large-scale Internet cafes with more computers. In particular, the emergence of the smartphone era has changed the patterns that Koreans enjoy, from online games to mobiles games, so that people go to Internet cafes less frequently than in previous years. As with in many other new technologies, high-speed Internet has been used not only by inventors but also by specific power groups. As the power group in cyberspace, the younger generation has rapidly increased its dominance and has used new technology to disrupt the information society. This means that only 10 years ago, teens consisted of the majority of cyber-related crimes and they, now, as people in their twenties represent the largest group of this particular cyber space issue in the 2010s.

The next generation of terrorists may grow up in the digital society, as several experts warned (Denning, 2002). "Cyber terrorism could also become more attractive as the real and virtual worlds become more closely coupled, with automobiles, appliances, and other devices attached to the Internet. Unless these systems are carefully secured, conducting an operation that physically harms someone may be as easy as penetrating a Web site is today" (Denning, 2003, 16).

Of course, another serious cybersecurity issue in Korea has been a potential cyberattack by North Korea in the wake of heightened inter-Korean tensions in recent years. North Korea has allegedly launched "multiple large-scale cyberattacks, targeting the websites of South Korean government offices, local banks, and media outlets." Therefore, "major banks and insurers as well as governments have taken steps to tighten their online security to guard against any attempt by North Korea to infiltrate their systems" (*Yonhap News*, 2016). The U.S. and Korean governments attribute a few recent incidents, including the March 2014 attacks against South Korean banks and media agencies and the November 2014 attack against Sony Pictures Entertainment, to North Korea. Prior to this, on 20 March 2013 North Korea initiated waves of

cyberassaults using malware called "DarkSeoul" against three Korean banks and three television broadcasters, including KBS and MBC, consequently paralyzing networks (Choe, 2013). Many people, including government officers and cybersecurity experts believe that "North Korea is emerging as a significant actor in cyberspace with both its clandestine and military organizations gaining the ability to conduct cyber operations" (Jun et al., 2015, 4). North Korea has taken "incipient steps toward an engagement with cyberspace whose future remains open, contingent, and largely unpredictable. Whether the internet will have similar effects to that in many other countries, including the development of social media and the cultivation of many-to-many ties, will depend largely on the country's policies and severity of censorship" (Warf, 2015, 117).

Korea is a test-bed for several digital technologies, because this small country has substantially developed several key areas, such as broadband services, Internet portals, online games, and smartphones; however, at the same time, the country has become a show window of the dystopian nature of digital technologies due to its unique socio-economic, cultural, and political milieu. The division of North and South Korea has intensified the concerns of the emergence of cyberterrorism, adding another risk to digitally networked Korean society.

Critical Discourse of Digital Technologies and Cyberterrorism

The relationship between cyberterrorism and new technology has been critical, as we need to understand its technological value and to institute appropriate security measures. In this regard, we should identify that cyberterrorism occurs when people who have technical expertise use potentially harmful sides of digital technologies; societies that apply digital technologies, including broadband services and smartphone technologies, are extremely vulnerable to cyberterrorism. Cyberterrorism happens because some people deliberate cyberspace as a zone of

unlimited freedom, a grid for free experimentation with no barrier (Robins and Webster, 1999, 91). As Barry Sandywell discusses (2006, 48), "the Net is frequently represented as a lawless zone undermining the solidarities of civil order." This unique and new space provides both utopian and dystopian environments. For many, cyberspace is not a place people rely on for the growth of our digital society. Many hackers enter computer systems by breaking through security measures. A few technical experts, in this case as a dominant power group, but with bad purposes, appropriate new technology to destroy the critical infrastructure of our society.

As Weimann (2004, 6) clearly points out, cyberterrorism is an attractive option for contemporary terrorists for various reasons: 1) it is cheaper than traditional terrorist methods, 2) cyberterrorism is more anonymous than traditional terrorist methods, 3) the variety and number of targets are enormous, 4) cyberterrorism can be conducted remotely, a feature that is especially appealing to terrorists, and 5) cyberterrorism has the potential to affect directly a larger number of people than traditional terrorist methods, thereby generating greater media coverage, which is ultimately what terrorists want.

Cyberspace is defenseless because it is "a geographically unlimited, non-physical domain, in which—independent of time, distance, and location—transactions take place between people, between computers, and between people and computers" (Hamelink, 2000, 9). Unlike traditional physical attacks, cyberattacks have been carried out from Internet cafes, and cyberattacks occur simultaneously on many occasions. Cyberspace enables terrorists to organize their attacks more easily on multiple targets and spread their own agencies over a larger geographic area (Robinson, 2001, 17-20). Unlike our physical world, people can hide their identity in cyberspace; and therefore, many people intend to conduct all kinds of cybercrimes and/or cyber terrorism. Due to the nature of cyberspace mention above, cyberspace has

especially become a ground for transnational terrorists to achieve their goals by disrupting the system and infrastructure in other countries.

Indeed, as the case of Korean broadband shows, a large potential exists for the majority of cybercrimes to occur primarily from PC bangs because cyber terrorists can easily hide their identities by using public computers. The structure of the network, its international character and chaotic structure, the simple access, and the anonymity furnishes terrorist organizations with an ideal arena for action (Tsfati and Weimann, 2002, 317). The new communication technologies—the Internet and broadband—provide cyber terrorists with "the ability to be halfway around the world instantly, in many places at once, and have an army of compromised machines to do their bidding" (Robinson, 2001, 17-20).

As Beck claimed, "risks arise from the actions and activities of individuals and society through conscious decision making." Beck especially saw "the generation of risk as indelibly connected with the rise of industrial society" (Jarvis, 2007, 31). In other words, cyberterror is a global risk, and as Beck (2002, 41-42) points out, "this should not be equated with a homogenization of the world, that is, that all regions and cultures are now equally affected by a uniform set of non-quantifiable, uncontrollable risks in the areas of ecology, economy and power. On the contrary, global risks are per se unequally distributed."

Space also intermingled with time, which is another key aspect of cyberspace. "Space and time are intertwined in nature and in society" (Castells, 1996, 407). In the age of digital and/or social media, people's information, including people's financial data, birthday, and family information, is easily accessed by the third parties. As people are able to communicate with each other on social media, this kind of new communication has been targeted as commodities by corporations and advertising agencies, but sometimes, people or organizations earn information

and appropriate them to fulfill their goas, either financial or political. This new trend creates a permanent virtual space in which space and time lose their authenticity (Jin, 2003; 2016). The problem is that the expansion of the network through the Internet and broadband services has brought about new forms of risk to our society. As Richard Clarke, chairman of the President's Critical Infrastructure Protection Board, argued, after the September 11 attacks, transnational terrorists began talking about destroying the information society and economy, which is increasingly dependent on networks (Verton, 2003b).

Of course, there is another form of space—national space—which means that in the 21st century, "national spaces have become de-nationalized, so that the national is no longer national….this entails that the foundations of the power of the nation-state are collapsing both from the inside and the outside, and that new realities are arising, a new mapping of space and time" (Beck, 2002, 53). As Edward Snowden's revelations in 2013 proved, in the early 21st century, several Western countries have practiced the far-reaching, seemingly unchecked global surveillance being conducted by the U.S. National Security Agency (NSA) alongside a few countries, including the U.K. and Canada ("Edward Snowden Interview," 2013; Hart, 2014, 2860). Both cyberterrorism and cybersecurity are beyond national boundaries; therefore, it is expected that governments throughout the world formulate alliances to protect their cyberspace from transnational cyberattacks.

However, Beck's notion of de-nationalization is not properly working in tandem with cyberterrorism and cybersecurity, mainly because the major players in cyberspace in this regard are nation-states. For example, after the September 11 attacks, the U.S. has established the Department of Homeland Security, which is the largest government agency. As the frontrunner of neoliberal globalization, the U.S. government has continued to demand other countries to open

their markets in actualizing a small government. On the contrary, the U.S. government had to develop the new agency, which focuses on national security, including cybersecurity. Although the Department of Homeland Security works with other countries, the major focus is domestic.

Most of all, it is not surprising to witness the corrupted use of Internet and broadband services in which cyberterrorism occurs because they do not arise by a sheer act of will. As Lia argues (2005), "modernization and technological breakthroughs are part of the ecology of terrorism in the sense that they inadvertently provide new opportunities for terrorists in terms of weaponry, targets, audiences and anonymity." Internet and broadband services have drawn attention to the commercial, political, and social interests from the beginning of their development. These new technologies have been invented and grown based upon complicated relationships between people, between people and technology, and between technology and technology (Wiener, 1954, 16).

New technologies are "not simply technical machines but communication forms that actively reconfigure social relations and public consciousness" (Sandywell, 2006, 40). Therefore, from its initial development, the Internet and broadband services could be used by a dominant few to disrupt the information society, because the always-on and high-speed service enables more people to exchange larger amounts of information, and terrorists utilize these new technologies. The Internet and broadband services are some of the most significant breakthroughs in modern history and the contemporary digital economy; however, with the rapid commercialization of digital technology, it has become possible for a cyber assault on the critical infrastructure of the information economy and society.

Conclusion and Discussion

This article has examined and discussed cyberterrorism through the lens of Beck's risk society. The swift growth of digital technologies, from the Internet to social media, over the last two decades has revealed both the delights and the dark side of the digital society. Newly developed digital technologies have quickened their pace in line with the evolution of other high-tech products. However, the rapid growth of the Internet and broadband services has also precipitated several negative impacts on our daily lives: new harmful effects such as cyberterrorism and cybercrimes (Drucker and Gumpert, 2000).

The Internet and broadband services are supposedly recognized as wonderful new digital media, which inspire equality in human communication and information sharing. However, with the help of anonymity, high-speed, and geographically unlimited space on the web (Robinson, 2001; Hamelink, 2000), cyberterrorism and cybercrimes are burgeoning in a digital age and are reaching more than alarming levels in many countries. "The dangers from terrorism increase exponentially with technical progress. Advances in financial and communication technology are what made global terrorism possible in the first place." (Beck, 2002, 45). As Jarvis (2007, 46) correctly observes, "Beck is alarmed by the fact of progress in almost every area of human endeavor amid a rampant disregard for ecological preservation, the use of technologies for nefarious purposes and the accelerated generation of unintended outcomes." The victims have been badly frightened by the enormous social costs and the crimes invisibility. Unfortunately, immature people with a poor sense of social responsibility, but possessing computer skills, have contributed to creating a digital nightmare over the Internet and broadband. They do not understand that "cyberspace is not a 'law-free' zone where anyone can

conduct hostile activities without rules or restraints" (Schmitt, 2012, 15). Cyberspace can blossom only if we understand it as a place that we nature and protect together.

At the end, what we have are not decisive solutions to cyberterrorism but guidelines for articulating the critical issues of broadband services and cyberterrorism. The power of those who own information and digital media skills—including cyber terrorists and cyber criminals—has expanded. In a digital capitalist society, where networks play a key role (Schiller, 2000), the distribution of power is concentrated, because fewer people possess high-level technical skills, as compared to those who possess only basic skills. Broadband, the new medium, is vital in this process, as it "works to legitimatize the existing distribution of power by controlling the context within which people think and define social problems and their possible solutions" (Jhally, 1989, 67). One of the major users of broadband is a highly educated younger generation and high school and college students, as well as technical experts who are willing to disrupt the information society and digital economy.

Unlike in many new technologies, in which inventors, producers, and corporations have expanded their power, in the case of the Internet and broadband services, a major consumer of these digital technologies has finally become a power group who uses it to distract the digital society, which is very rare. The Internet and broadband, as private entities owned by those seeking technological advantages, became tools for terrorists who have a vested interest in perpetuating the dominant ideology of cyber terrorists and cyber criminals to maintain or increase their power. In fact, cyberterrorism occurs when people use harmful aspects of digital technologies. One of the major characteristics of cyberspace is the impossibility of pointing to the precise place and time where an activity occurs or information traffic happens to be. The

spaces of the physical and the virtual world are closely interconnected, and it makes distance meaningless.

In sum, one must admit that technology is not universally rational nor a social and cultural force. Technology is an object, which is socially defined and organized. New technology is not a fate one must seek or avoid, but a challenge to political and social creativity and action. Technology is an important driving force in economic, social, and political change in modern society. However, technological improvements do not necessarily lead us to social progress (Christians, 1995). As with many other technologies, the Internet and broadband have their own values from design to product process, and their (adverse) value penetrates all technical activity. Cybersecurity cannot succeed without comprehending the relationship between people and technology, because another risk society in our modern society continues as members of tech-savvy young generation misunderstand cyberspace.

References

Beck, Ulrich (1999). *World Risk Society*. Cambridge: Polity Press.

Beck, Ulrich (2002). The Terrorist Threat World Risk Society Revisited. *Theory, Culture & Society* 19(4): 39-55.

Bolz, Frank. Jr., Kenneth J. Duponis and David P. Schulz (2001). *The Counter-terrorism Handbook: Tactics, Procedures, and Techniques*. New York: CRC Press.

Boyd-Barrett, Oliver (2006). Cyberspace, globalization and empire. *Global Media and Communication* 2(1): 21-41.

Castells, Manuel (1996). *The Rise of the Network Society*. Malden, MA: Blackwell Publishers.

Choe, Sang-hyun (2013). Computer Networks in South Korea Are Paralyzed in Cyberattacks. *New York Times*. 20 March. http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html?pagewanted=all&_r=1

Christians, Cliff (1995). Propaganda and the Technological System. In *Public Opinion and the Communication of Consent*, eds. Theodore L. Glasser and Charles T. Salmon, 156-176. New York: The Guilford Press.

Computer Industry Almanac Inc. (2006), January 4. Worldwide Internet Users Top 1 Billion in 2005 (press release).

Cybersecurity Ventures (2015). Cybersecurity Market Report. http://cybersecurityventures.com/cybersecurity-market-report/

Denning, Dorothy (2002). *Is Cyber Terror Next*? Available at http://www.ssrc.org/sept11/essays/denning.htm

Denning, Dorothy (2003). Information Technology and Security. In *Grave New World: Global Dangers in the 21st Century*, Michael Brown (ed.), 1-23. Georgetown University Press.

Drucker, Susan J. and Gary Gumpert (2000). CyberCrime and Punishment. *Critical Studies in Media Communication* 17(2): 133-158.

Dyer-Witheford, Nick (1999). *Cyber-Marx: Cycles and Circuits of Struggle in High-Technology Capitalism*. Urbana, IL: University of Illinois Pres.

"Edward Snowden interview: The NSA and its willing helpers" (2013, July 8). *Der Spiegel*. http://www.spiegel.de/international/world/interview-with-whistleblower-edward-snowden-on-global-spying-a-910006.html

Fitzgerald, Brian (2014). Data Point: U.S. Ranks Behind Latvia in Offering Top-Speed Broadband Connections. *The Wall Street Journal*. 27 June. http://blogs.wsj.com/digits/2014/06/27/data-point-u-s-ranks-behind-latvia-in-offering-top-speed-broadband-connections/

Frieden, Robert (2001). *Managing Internet Driven Change in International Telecommunications*. Boston: Artech House, 2001.

Garfinkel, Simson (2002). The FBI's cyber-crime Crackdown. *Technology Review* 105 (9): 66-74.

Gartner (2015). Gartner Says Worldwide Information Security Spending Will Grow Almost 4.7 Percent to Reach $75.4 Billion in 2015. 23 July. Press Release.

Hamelink, Cees (2000). *The Ethics of Cyberspace*. London: Sage.

Hart, Catherine, Dal Yong Jin, and Andrew Feenberg (2014). "The Insecurity of Innovation: A Critical Analysis of Cybersecurity in the United States." *International Journal of Communication* 8: 2860-2878.

Heng, Yee-Kung (2006). The 'Transformation of War' Debate: Through the Looking Glass of Ulrich Beck's World Risk Society. *International Relations* 20(1): 69-91.

Hwang, H. K. (2002). Broadband Internet. *Maeil Economic Daily*, 28 May, 19.

Internet Live Stats (2016). Internet Users. http://www.internetlivestats.com/internet-users/

Jarvis, Darryl S.L. (2007). Risk, Globalisation and the State: A Critical Appraisal of Ulrich Beck and the World Risk Society Thesis. *Global Society* 21(1): 23-46.

Jhally, Sut (1989). The Political Economy of Culture. In *Cultural Politics in Contemporary America*. eds. Jhally, Sut and I. Angus, 65-81. New York: Routledge.

Jin, Dal Yong (2003). Beyond Cyber-terrorism: Cyber-security in Everyday Life. *The Ellul Forum* 32: 8-13.

Jin, Dal Yong (2011). *Hands On/Hands Off: The Korean State and the Market Liberalization of the Communication Industry*. Cresskill, NJ: Hampton Press.

Jin, Dal Yong (2016). Cultural Interpretation of Cyberterrorism and Cybersecurity in Everyday Life. In Shaw, Jeffrey (ed.). *Jacques Ellul on Violence, Terrorism, and War,* 53-69. Eugene, OR: Wipf & Stock Publishers.

Jun, J., S. LaFoy, and E. Sohn (2015). *North Korea's Cyber Operations: strategies and responses*. New York: Rowman & Littlefield.

Kirkpatrick, David (2003). War images give new purpose to High-Speed Web. *New York Times*, 24 March, C1.

Kizza, Joseph Migga (2002). *Computer Network Security and Cyber Ethics*. London: McFarland & Company, Inc.

Korea Creative Content Agency (2015). *2015 Game Whitepaper*. Naju: KOCCA.

Korean National Police Agency (2006). *2005 Policy White Paper*. Seoul: National Policy Agency. Available at http://www.police.go.kr/index.jsp?_page=2281.

Korean National Police Agency (2003). *2003 Policy White Paper*. Seoul: National Policy Agency.

Korean National Police Agency (2002). *2002 Policy White Paper*. Seoul: National Policy Agency.

Korean National Policy Agency (2016). Cyber Security. Seoul: KNPA. http://www.police.go.kr/portal/main/contents.do?menuNo=200311

Lemke, Tim (2002). Cyber-terror a certainty, and government is most vulnerable. *Insight on the News* 18 (1): 31.

Lewis, Lee (2016). Asia cyber vulnerability gap leaves richer nations exposed. *Financial Times*. 23 February. http://www.ft.com/intl/cms/s/0/3ceb2a98-d9e5-11e5-98fd-06d75973fe09.html#axzz4AA1kiF1i

Lia, Brynjar (2005). *Globalization and the Future of Terrorism: Patterns and Predictions*. London: Routledge.

Linder, Matt (2015). Global e-commerce sales set to grow 25% in 2015. Internet Retailer. 29 July. https://www.internetretailer.com/2015/07/29/global-e-commerce-set-grow-25-2015

Mansell, Robin (2004). Political Economy, Power and New Media. *New Media & Society* 6(1): 96-105.

McChesney, Robert (2000). *Rich Media, Poor Democracy: Communication Politics in Dubious Times*. New York: The New Press.

Menon, Rekha (2006). Paying bills at the click of a mouse Online Banking: Broadband has expanded the range of services available. *Financial Times*, 10 May, 4.

Ministry of Information and Communication (2006). *2006 Korea Internet White Paper*, Seoul: MIC.

Misra, Sunil (2003). High-tech Terror. *American City & Country* 118 (6): HS 6.

Obama, Barack (2016). Protecting U.S. Innovation From Cyberthreats (commentary). *The Wall Street Journal*. 9 February. http://www.wsj.com/articles/protecting-u-s-innovation-from-cyberthreats-1455012003

OECD (2001). *Communication Outlook 2001.* Paris: OECD.

Papalardo, Denise and M. Martin (2002). Lobbying Group Outlines Big-Pipe Dream. *Network World*, 21 January, 8.

Powell, Michael (2001). Remarks of Michael K. Powell Chairman Federal Communications Commission At the National Summit on Broadband Deployment. Washington, D.C. 25 October.

Robins, Kevin and Frank Webster (1999). *Times of the Technoculture: From the Information Society to the Virtual Life*. London: Routledge.

Robinson, Clarence (2001). Physical Disaster Propels Cybersecurity Initiatives. S*ignal* 56 (3): 17-20.

Sandywell, Barry (2006). Monsters in Cyberspace: Cyberphobia and Cultural Panic in the Information Age. *Information, Communication & Society* 9 (1): 39-61.

Saravanamuthu, Kala (2002). Information Technology and Ideology. *Journal of Information Technology* 17 (2): 79-88.

Schiller, Dan (2000). *Digital Capitalism: Networking the Global Market System*. Cambridge, MA: MIT Press.

Schmitt, Michael (2012). International Law in Cyberspace: The Koh Speech and Tallinn Manual Juxtaposed. *Harvard International Law Journal* 54:13-37.

Schjolberg, Stein (2007). Terrorism in Cyberspace – Myth or reality? http://www.cybercrimelaw.net/documents/Cyberterrorism.pdf

Singer, P.W. and A. Friedman (2014). *Cybersecurity and Cyberwar: what everyone needs to know*. New York: Oxford University Press.

Sofaer, Abraham and Seymour E. Goodman (2001). *The Transnational Dimension of Cyber crime and Terrorism* (ed.). Stanford, CA: Stanford University Press.

Squitieri, Tom (2002). Cyberspace full of terror targets. *USA Today*, 6 May, 11A.

Taylor, Chris (2006). The future is in South Korea. 14 June, *CNN*. http://money.cnn.com/2006/06/08/technology/business2_futureboy0608/index.htm

Technology Briefing E-Commerce: Sales Rise 25% To Record (2004). *New York Times*, 24 February, C10.

Tsfati, Yariv & Gabriel Weimann (2002). www.terrorism.com: Terror on the Internet. *Studies in Conflict & Terrorism* 25: 317-332.

Upgrade Business Era: PC Bang. (2003). *KyungHyung Shinmun*, 30 September, 30.

Verton, Dan (2003a). *Black Ice: The invisible threat of Cyberterrorism*. New York: McGraw-Hill.

Verton, Dan (2003b). Cyberthreats not to be dismissed, warns Clarke. *Computerworld* 27(1): 6 January, 10.

Volz, Dustin and Mark Hosenball (2016). Concerned by cyber threat, Obama seeks big increase in funding. 10 February. Reuters. http://www.reuters.com/article/us-obama-budget-cyber-idUSKCN0VI0R1

Warf, Barney (2015), The Hermit Kingdom in cyberspace: unveiling the North Korean internet. *Information, Communication & Society* 18 (1): 109-120.

Weimann, Gabriel (2004). Cyberterrorism How Real Is the Threat? United States Institute of Peace- Special Report 119: 1-12.

Wiener, Norbert (1954). *Human Uses of Human Beings: Cybernetics and Society*, 2nd ed. Boston: Houghton Mifflin.

The World FaceBook (2013). Internet Hosts. Washington, D.C.: The Central Intelligence Agency. https://www.cia.gov/library/publications/the-world-factbook/rankorder/2184rank.html

Yonhap News (2016). S. Korea beefs up security against North Korea cyber attack. 15 February.

Institute for Journalism, Media & Communication Studies (MEDIACOM), Keio University publishes MEDIACOM Working Paper Series electronically.

Editor of the MEDIACOM Working Paper Series

Professor YAMAMOTO Nobuto (2015-)

Institute for Journalism, Media & Communications Studies

Keio University

108-8345

Tokyo, Minato-ku, Mita 2-15-45

http://www.mediacom.keio.ac.jp/english/

KEIO MEDIACOM Working Paper Series

1	Can Nationalism (in Asia) Still Change? *Benedict Anderson*	(2015)
2	IPT 1965: Fifty Years Fighting for Justice *Evi Sutrisno*	(2015)
3	Risk Society, Cyberterrorism, and Korea's Network Culture *Dal Yong Jin*	(2016)