The Institute for Peace and Unification Studies Seoul National University

IPUS HORIZON | No.14 (11 Jan 2023)

The Evolution of Cyber Security: A Complex Geopolitics Perspective

Sang-bae Kim

Professor, Department of Political Science and International Relations, Seoul National University

Not only cyber attacks have recently increased significantly in quantity, but also qualitatively. In the past, cyberattacks meant only hacking attacks for system disruption, but now they are connected to international political, economic, and military issues and have expanded to future cyber warfare. The biggest characteristic of cyber security is that it is different from the unique characteristics of traditional security issues. To sum up its characteristics in one word, it is "Virtual Spear and Mesh Shield", which is also the title of a book published several years ago. A merchant who sold spears and shields at the same time boasted of a spear, he said that there is no shield that cannot be pierced by this spear, but when he boasted of a shield, he said that there is no spear that this shield cannot block. This old idiom, widely known as contradiction, is particularly relevant to cybersecurity issues in the digital age. Cyber security is a situation where virtual (invisible) spears are attacking in very large numbers. The shield to block this is not a shield made of a solid plate, but a net with holes perforated. It is a mutual confrontation between an invisible spear that must be blocked and a very weak shield.

Since cybersecurity is a new issue, there is a need to analyze this issue through a geopolitical perspective in a classical sense. Nevertheless, due to the complexity of this nature, people are researching 'cyber security from the perspective of complex geopolitics' in a sense that we must invoke complex perspectives beyond geopolitics. Looking at the evolution of cyber security, in the beginning, there was a process in which the number of hacking activities by non-state actors, hackers, or terrorists increased and the patterns diversified. However, these early cyber security issues have emerged to the point of discussing war between countries. Emergence is a term used in complexity theory. It is a term that refers to the process of creating

a new order and pattern through complex interactions of various elements at the microscopic level or through the process of acting on various issues. The recent changes in the field of cyber security are taking place in a very complex manner to the extent that it must be seen by using the concept of emergence, a complex system theory. Accordingly, the need to take a complex look at not only traditional geopolitical or security issues, but also issues under the surface is being raised.

In discussing cyber attacks, it is first necessary to understand the unique characteristics of attacks based on a unique space called cyberspace. Security issues and attack and defense issues that occur in an environment with a complex and complex network structure called cyberspace need to be understood. Since the Internet itself is a vulnerable environment with many gaps, attacks are made targeting those gaps. Even if it is defended, it cannot be properly defended like a virtual spear and a mesh shield, and thus, attack is generally more advantageous than defense. In some cases, it is not easy to distinguish the victim. The attacking party does not end with the attack, but the attack itself returns to itself like a boomerang. It is a game of attack and defense that takes place in a complex network environment.

Next, given that cyberspace is a product of science and technology that creates computer networks, the space where cyber security takes place is significantly influenced by scientific and technological variables. Most cyberattacks, such as computer viruses and malware, can be viewed as software programs in some way. It is a method of attack created through science and technology, and the attack pattern is DDoS attack, or advanced persistent attack known as APT (Advanced Persistent Threat). Those like Stuxnet and Ransomware, which have been discussed recently, are being used as means by non-human actors. It is a game that occurs as these non-human actors have meaning as active actors with their own agency action ability. Other than that, the security game has traditionally been known as a game of threat and defense between state actors, but in the field of cyber security, private actors, not the states, are basically involved. Recently, state actors are manipulating private actors behind the scenes or directly attacking acts from behind the scenes, which is also a significant characteristic.

Lastly, cyberattack may be today's threat, but may be tomorrow's biggest threat. It is an invisible threat. For this reason, it has the characteristic of securitization

discourse, which assumes that security threats that exist objectively are present, but subjective judgments can become a greater threat. However, in cybersecurity, even the process of attributing responsibility after an attack occurs is taking place in a complex network environment in which it is impossible to strictly identify cause and effect. Thus, the storytelling of who attacked and how is important in the cyber security game that is taking place in reality.

In academia, cyber attack patterns are conceptually classified in various forms. In terms of the purpose or target of an attack, physical destruction, system disruption, and resource acquisition are put on one axis, and the subject of the attack is put on the other axis, such as a nation, a group, or an individual. Looking at it in this respect, they can be divided into various categories ranging from cyber warfare linked to physical attacks between countries to cyber terrorism to cyber disturbance, cyber espionage, and cyber crime. However, the recent characteristic is that there are situations where these distinctions are colorless and entangled with each other. A cyberattack seems to be a personal crime by private actors, but in some ways, the act of being a source of conflict at the national level or disrupting data or systems is itself linked to war in the physical space. Patterns of cyberattacks seem to be undergoing a transition on a historical level. Looking back over the past 10 to 15 years, in the early days, problems in international politics were attacks on national infrastructure, cyber attacks on public institutions, financial institutions, media institutions, and core infrastructure that are of great national significance. However, attacks on intellectual property rights, confidential data, or core technologies are now becoming a problem. Attacks are being made by targeting economically profitable parts of data or technology. Not only are ransomware planted to demand money, or hacking of cryptocurrency-related parts is taking place, but it is also evolving as a means of attack to obtain new things based on psychological defects called information psychological warfare. Another milestone in this process is the outbreak of COVID-19, and cyber attacks threatening the non-face-to-face environment created by COVID-19 are increasing. Currently, we are using many programs in a non-face-to-face environment. Interruptions or thefts are being made by infiltrating activities between individuals or between companies and countries that take place through these programs. Furthermore, regarding COVID-19, the theft of advanced core technologies for COVID-19 treatments and vaccines is also

a problem. A computer virus raids through a non-face-to-face environment, which has escaped the coronavirus, and a computer virus comes to the place where the coronavirus passed.

Recently, cyber attacks and defenses using AI are on the rise. Cyberattacks are becoming more intelligent and autonomous, moving beyond automation. Autonomous attacks follow program-automated mechanisms and algorithms, and the defense side also uses AI for predictive program that analyzes threat information and detects anomalies. At some point, a world in which autonomous cyber attack weapons that defend themselves against machines and AI-based defense networks that autonomously defend against them are exchanging battles in the absence of humans may come. Another recent trend is that it is connected to the phenomenon of geopolitical resurgence in international politics as a whole. In the past, private actors took the lead and the state hid behind attacks, but in recent years, state actors are taking the lead in cyberattacks. Signs of this were made known since the late 2000s, when cyber attacks by Russia against countries in Eastern Europe surfaced. Meanwhile, state actors are evident in the cyber battle between the United States (U.S.) and Israel against Iran in the early 2010s. Since then, in the mid-to-late 2010s, in the context of the hegemonic competition between the U.S. and China, cyber attacks and cyber security issues have become a key issue. In addition, on the Korean Peninsula, there have been several attacks, which are presumed to be North Korean attacks. State-sponsored cyberattacks are increasingly and explicitly disrupting and bringing systems down. However, they are not an attack with a sign of who made the attack, but rather a way to take a quick look at the key data or extract it, and thus, the sign for who did it is not visible. The U.S. intelligence authority claimed that attacks were carried out by Chinese hackers on the U.S. government system in the mid-to-late 2010s. Various types of hacking which North Korea has recently been perpetrating on major facilities in South Korea and other countries are linked to the theft of data installation, information technology, and financial purposes. Overall, cyberattacks are evolving. This is an important part to be noted in the response system of a complex national strategy.

In early 2021, discussions about growing cyberthreats were abuzz in the U.S. The newly launched Biden administration emphasized that Russian or Chinese hackers are increasingly attacking the U.S. system, and has a strong response posture. In July

2021, when President Biden visited the Director of National Intelligence (DNI), he took a strong stance, warning Russia that continuing cyberattacks against the U.S. could lead to a real war. Around the same time, the U.S. withdrew from Afghanistan and said it would reorganize its foreign policy around two main points. One of them was China, the other was cyber warfare. Accordingly, the U.S. government is employing experts with aggressive tendencies in the field of cyber security and taking measures to strengthen vigilance through various forms of executive orders, moving beyond the domestic level. At the international level, by pointing out these problems at European NATO or EU meetings, it forces NATO to issue a statement condemning China's cyber activities. Behind the Biden administration's tough stance, it is known that there have been many cyber attacks that can actually trace Russia behind it. In the late 2000s, an attempt was made to sabotage the U.S. presidential election, and an attack on SolarWinds, which is the largest security solution company in the U.S. was made in 2020. A ransomware attack on Colonial Pipeline, which is the largest oil pipeline company in the US, occurred in May 2021. There have been many other attacks on supply chains related to various types of daily necessities. Cyberattacks originating not only from Russia but also from China were controversial. The U.S. government claimed that the Chinese government is supporting hackers targeting U.S. laboratories developing a COVID-19 vaccine during the coronavirus phase, and ordered the closure of one of the consulates in the U.S. In addition, there have been cases where Microsoft's Exchange servers have been hacked.

North Korea is also known to be attacking not only South Korea, but also the U.S. and global systems. There were various types of DDoS attacks and APT attacks from 2009 to the early 2010s. The biggest known attack on South Korea was the March 2013 cyberattack on broadcasting companies and financial institutions. The scale of the damage was significant, but it received much attention from the media because it attacked the media. On the other hand, the 2014 hacking incident against Sony Pictures is known as an incident in which North Korea made a hacking attack against the U.S., causing the U.S. to respond proportionally, that is, to take a strong countermeasure. It was an attempt to hack Sony Films, which produced the 'Interview' movie about the assassination of North Korean leader Kim Jong-un, and disrupt the screening. Regarding this, U.S. defined it as cyber vandalism and announced that proportional countermeasures would be taken. As far as is known, economic

sanctions measures, including communication network disruption and financial sanctions, were considered against North Korea, and some of them have been implemented. A hacking attack on a private film company can be seen as an example of an international political incident. In addition, North Korea is being pointed out as behind attacks on some financial systems, such as the 2016 hacking of the central bank of Bangladesh. Even beyond the 2020s, North Korea is still known to hack into financial institutions around the world. As well as hacking the COVID-19 vaccine, it is known to have attempted to hack Korea's defense facilities and defense research facilities especially in 2021. As it made attacks to steal information from research institutes such as the Korea Atomic Energy Research Institute, Daewoo Shipbuilding & Marine Engineering, and Korea Aerospace Research Institute, it raised awareness at the domestic level.

What needs to be keep in mind here is that hacking attacks are often targeted in areas related to the supply chain. Even in the process of competition between the U.S. and China, the issue of supply chain supplementation is considered very important. In particular, as cyber security issues about Huawei's equipment, which makes China's 5G mobile communication equipment, were raised in the late 2010s, import and export regulations were enforced. It has emerged as a key issue in the conflict between China and the U.S. Most of the attacks on software companies, such as the aforementioned attack on the Sullivans security solution company, were attacks on the software system that manages the supply chain among the entire supply chain. This is also connected to the issue of economic security, that is, supply chain security, which has recently attracted attention. By targeting the system itself, which forms the supply chain, ranging from raw materials for daily necessities to intermediate goods and finished products, they may cause not only military damage but also economic damage in daily life. In particular, the supply chain issues and cyber encryption issues between the U.S. and China are also connected to cyber alliances, a traditional theme of international politics. When a controversy over Huawei equipment arose during the Huawei crisis, and the U.S. took steps to control Huawei imports, and pressured traditional U.S. allies, such as Canada, Australia, New Zealand and the United Kingdom, to ban Huawei products. Recently, 5G+ wires are expanding. Of course, there were cracks in the large front, but it shows a confrontation with China while the cyber alliance is generally maintained.

The cyber alliance is linked with the U.S. Indo-Pacific strategy, which has been passed down from the Trump administration to the Biden administration, and is reflecting an attempt to forge a new solidarity between the camps. China, which is trying to respond to this, is confronting it by emphasizing cyber security or data security in the frame of the so-called 'one belt, one road'. At the peak of this conflict, the U.S. put forward a 'Clean Network' in the end of the Trump administration in the 2020s, and in response, China put forward a 'Global Data Initiative'. In a broader sense, this is again connected to various negotiations and consultations in bilateral or multilateral diplomacy, or to the process of forming norms to restrict unjust acts at the international level. In 2015, then-President Obama and Chinese President Xi Jinping reached an agreement not to carry out attacks beyond a certain level and attempted to make a new breakthrough. However, attacks do not disappear even if the two leaders come forward and promise not to attack again due to the nature of cybersecurity. Still, the issue of attack and defense between the U.S. and China is an issue. Nevertheless, various kinds of bilateral diplomatic consultations are underway. Korea is also trying to solve this problem through the process of conducting cyber policy consultations with more than 20 countries. The UN attempted to create international norms through the Open Ended Working Group (OEWG). While some progress has been made in the past decade, it has also presented many challenges in itself. The fact that it is not the kind of problem that can be resolved by agreement between representatives of 190 countries in an international organization makes it difficult to form international norms in this area. What is more important is that there are many elements of conflict between the U.S. and China, Russia, or the Western camp and the non-Western camp, or developed countries and developing countries, which have different interests in the discussion. There is a wide range of views, ranging from discussion on whether the existing international law or the law of war can also be applied to acts of war in the field of cyber security to discussion on whether international law can be applied in the humanitarian dimension.

Regarding a phenomenon that has recently become more prominent because of the war in Ukraine, Cyberspace may be an act of physical attack or an act of attempting to steal information or data assets in it, but it can go further and create the psychological space of the actors involved in it or the effect that may provide false and manipulated information to the other party or cause some other cognitive

exchange, enabling to obtain what they want. A kind of information psychological warfare is taking place centering on cyberspace. The realm of cyber warfare, which we are aware of, is expanding. During the 2016 U.S. presidential election, information psychology warfare in cyberspace became an issue. Russia's involvement in the presidential elections of Hillary Clinton and Donald Trump became an issue. There was talk of unfounded speculation, but there was also a battle that Russia's intervention changed the outcome of the presidential election. As the distribution of various information, which were created using social media and the distribution of fake news are widespread, it moves beyond simply social and political conflict issues and is raised in the form of an act of war. In a way, at the transnational level, the online public sphere was expected to play a role as a space that could realize the ideal of participatory democracy and direct democracy. In fact, the space is becoming a space of war where false information is disseminated and weaponized.

Information warfare, which achieves information superiority and overwhelms opponents, is now being used in connection with psychology. In the era of the 4th industrial revolution, against the background of various technologies and data environments, it has begun to have the nature of communication warfare that affects the other party's cognitive system. There is a need to pay attention to the conceptual transformation of information psychological warfare in three dimensions. First, as a means of waging war, digital media such as SNS have become very important. The Internet world is a space we created for convenience, but it has become a tool for the environment that attacks oneself. Second, if traditional information psychological warfare was an aspect of military warfare at the national level, private big tech companies which control the computer environment, hackers at the passive level, and ordinary citizens are playing an important role. In the past, civilian actors were the target and subject of war, but they are emerging as the subject of war in the newly emerging information psychological warfare. Third, in terms of the goal of warfare, war itself may be the goal in information psychological warfare. While the goal of war in physical space was to subdue the opponent's hardware and seize lives, recently, the high level of achieving what one wants by spreading a persuasive and touching narrative to the other side to gain the other side's heart and consent or conveying the wrong situation emerged as another goal of war. The space where the war takes place expanded not only to cyberspace but also to outer space. Those who

emphasize the importance of information psychological warfare include the space of war in our cognitive space, that is, the brain space. As our cognitive space becomes an important war zone, it has the specific purpose of disrupting and manipulating the other person's cognitive systems, rather than simply producing and gathering information to be effective by passing it on. That is, it is not the message as being conveyed that is important, but that it hits the cognitive system of the messenger that consumes the message. Thus, creating a new system environment by finding out the vital points of messengers can be an important winning factor in the war. The key is that narrative wars or frame wars, where the ability to manipulate and weave frames which create stories and view problems is important, are emerging. As it is emerging as a new aspect of war, I think we need a more active response.

Even in the field of information activities conducted at the national level, the meaning of cyber security in activities using digital systems or in the process is being reexamined. If the core of espionage activities in the past analog era was to acquire and analyze information hidden in the so-called Small Data world, in the digital world, it is to bring and analyze a kind of open information big data. These changes are emerging one by one through the recent war in Ukraine. The war in Ukraine has a traditional warfare aspect, but also a new warfare aspect, which has not been seen before. There are elements intertwined that seem like war but also do not seem like war. The war in Ukraine can be cited as an example of complexity in terms of the means of war, its purpose, and the subject of execution. Another issue related to the recent war is whether cyber warfare will be conducted as a separate independent war or will become a multi-domain operation and become a complex aspect occurring in multiple spaces. It seems that the opinion is gradually leaning towards the latter. Attacks in cyberspace, which occur interlocked before, during and after the war are attracting attention. It is likely that in the future, how to wage war in cyberspace will be the key to winning or losing a war. Recently, unmanned weapons equipped with AI appeared. There is a discussion about a combat system, which combines manned and unmanned systems. The problem is that if a weapon programmed by humans for autonomous combat could be hacked and aimed at friendly forces, the risk would be amplified. In addition, autonomous weapon systems can be vulnerable not only to hacking vulnerabilities, but also to mechanical defects such as bugs and software glitches. As the size and scale of software increase and the complexity of technology

increases, the possibility of accidents or malfunctions increases even without malicious infiltration. Accordingly, it is necessary to prepare for this. Moreover, cyber attacks, which target the cognitive vulnerabilities of humans by using screen manipulation like deepfakes are considered cyber warfare in a broad sense.

Meanwhile, cyber warfare and electronic warfare are being combined. We are currently living using various types of information and communication systems. When war breaks out, the operations between those units become complex and important. If electromagnetic wave attack, energy directed attack, or energy laser weapon is used, it becomes electronic warfare. These elements of electronic warfare are being combined with cyber warfare. 'Left on Launch' is the most popular term. It means disabling missile bases or mobile launch pads in preparation for launch, which is the stage before launch (left). According to a British daily report, in the early 2010s, during the Obama administration, North Korea fired while continuously moving the missile launch site. Concern about North Korea's movement and launch of missiles were due to the U.S.'s electronic attack or cyber attack linked to electronic warfare. Next, these complex aspects of war lead to space warfare. The satellite's artificial intelligence system itself can be hacked, changing its trajectory and causing them to collide with each other. Scenarios in which space debris collides and destroys satellite systems are also being discussed. In fact, the current satellite navigation system, GPS disturbance is becoming a problem.

Cyberwarfare has recently been linked to nuclear weapons. In this context, the cybersecurity complex nexus has recently evolved into a trend in which cybersecurity is linked to various parts related to war. If the nuclear weapons system created in the Cold War era was a partially electronic system based on an analog system, now it is building a networked system as a whole, which can pose a greater risk in the event of a hacking attack. Even in the context of the Korean Peninsula, discussions on how aspects related to cyber warfare can be connected in the reality of North Korea's nuclear issue or missile launches are being carried out. In the context of truly asymmetric warfare, how to manage nuclear and cyberspace is becoming a major issue. Further, the capabilities of attack forces related to cybersecurity could change the face of the future international order today or tomorrow. In a way, the past order created in the Cold War era was centered on nuclear powers, but today cyber security issues are linked to nuclear weapons and are linked to various other issues.

The growing possibility of changing the face of the international order as we know it is raising the need for new norms to regulate it. If the discussion of nuclear norms was a major issue in the late 19th century, it is assumed that cyber norms linked to nuclear or other issues will become a major issue in the future. In conclusion, I think that the issues of international politics seen from the perspective of complex geopolitics are the current reality.

Author

Sang-bae Kim

Professor, Department of Political Science and International Relations, Seoul National University

Education

Indiana University
PhD in Political Science
Seoul National University
Master of International Relations
Seoul National University
Bachelor of International Relations

Experience

Seoul National University
Professor
Department of Political Science and International Relations
Seoul National University
Director
Institute of International Studies
President of the Korea International Political Science Association

BOOKS

『US-China Digital Hegemonic Competition: Complex Geopolitics of Technology-Security-Power』 (Hanwool, 2022)
『Virtual spears and mesh shields: Global politics of cyber security and South Korea』 (Hanwool, 2018)
『Arachne's International Politics: The Challenge of Networked World Politics Theory』 (Hanwool, 2014)
『Information Revolution and Power Transformation: Perspectives of Network Politics』 (Hanwool, 2010)
『Standard Competition in the Information Age: Wintelism and Japan's Computer Industry』 (Hanwool, 2007) et al.