https://doi.org/10.33778/kcsa.2023.23.5.199

Measures to Strengthen Korea-Japan Cyber Security Cooperation: Focusing on Joint Response to North Korean Cyber Threats

Tae Jin Chung*

ABSTRACT

South Korea and Japanese governments have never responded cooperatively to North Korea cyber threats in the past 10 years or even before that. There are two reasons: First, The historical and political conflicts between the two countries were so deep that they did not discuss their mutual needs. Second, officially, Japan had not been subjected to a North Korean cyberattack until 2022 . In particular, the issues of comfort women and forced labor during World War II were holding back the reconciliation between the two countries. With the inauguration of the Yoon Seok-yeol administration, Korea-US relati ons improved dramatically. Tensions in Northeast Asia reached their peak due to the conflict between the US and China. It has become a situation where peace cannot be garaunteed without close cooperation between Korea and Japan led by the United States.

북한 사이버 위협에 대응하기 위한 한일사이버 안보협력 강화방안

정 태 진*

요 약

한국과 일본 정부는 지난 10년 동안, 심지어 그 이전에도 북한의 사이버 위협에 협력적으로 대응한 적이 없다. 두 나라 사이의 역사적, 정치적 갈등이 너무 깊어서 서로의 필요를 논의하지 않았습니다. 특히 제2차 세계대전 당시 위안부 문제와 강제노동 문제는 양국의 화해를 가로막는 요인이었다. 윤석열 정부가 출범하면서 한미관계는 극적으로 개선됐다. 미국과 중국의 갈등으로 동북아 긴장이 최고조에 달했다. 미국이 주도하는 한·일·대만 간 긴밀한 협력 없이는 평화를 긍정할 수 없는 상황이 됐다. 한일 사이버안보 협력은 안보협력에 있어 가장 기본적이고 중요한 부분이다. 사이버안보는 적의 군사작전을 감시하고 안보상 이상행위를 탐지하는 역할을 담당하는 만큼 한·일 협력도 미국 정부의 가장 중요한 관심사다. 한일 정부의 관계 개선은 한반도와 동북아의 평화를 위해 필수적이며, 세계 안보와 평화 유지를 위한 가장 중요한 초석입니다. 사이버 안보 측면에서 지난 20년은 가장 중요한 시기로, 정치적 갈등으로 인해 북한의 사이버 위협에 한·일이 공동 대응하지 못한 점을 따라잡아야 할 때이다. 이번 연구에서는 한·일 정부가 북한의 사이버 위협에 공동 대응하기 위해 사이버 안보 협력 강화 방안과 필요한 법적 조치를 모색하고 한계점을 논의할 예정이다.

Key words: Korea Japan cyber security cooperation, North Korea Cyber Threats, Global and North East Asia Peace, Political & historical disputes, Counter-measures.

접수일(2023년 11월 09일), 수정일(2023년 11월 27일), 게재확정일(2023년 12월 11일)

* Professor, Pierson College, Pyeong Taek University

1. Introduction

Cyber security is no longer a matter of one country, but a major pillar of global security. And without the cooperation of our allies, we cannot expect the best possible results in defe nse and response. Until recently, due to histori cally deep-rooted conflicts, South Korea and Japan have always held joint military exercise s with the United States at the center when it comes to security in Northeast Asia. But amid the U.S.-China competition for technological hegemony and the crisis in Northeast Asia, No rth Korea's cyberattacks are no longer just a threat to South Korea. Therefore, cyber security cooperation between South Korea and Japan is a joint task that can no longer be postponed. The "cybersecurity cooperation" we are discus sing here does not mean cooperation that is only discussed at conferences, but practical co operation between working-level officials. Alth ough South Korea and Japanese governments are aware of North Korea's cyberattacks and cybercrimes that have been reported through the media, there has been no exchange of info rmation on the exact damage or threats in each country. Previous study reported that the impo rtance of cooperation between or among ASEAN countries. However, it is difficult to find papers on cybersecurity cooperation between Korea and Japanese governments. This appears that there no prior research coducted for this reseach topic. Among the previous studies, the most re ported about part is the enactment of Japan's Cyber Security Act and the introduction of cy ber security agencies.

During the pandemic, North Korea hackers illegally accessed the national networks of Sou th Korea and Japan to steal information or da mage networks, and socially engineered to pinch crypto currencies by approaching victims under disguise to scam crypto currencies[1]. It seems that they are devising a strategy to differentiate between Korea and Japan and between Korea and China through cyber psychological warfare. Cyber psychological warfare will someday infl uence the fate of the country through election manipulation. As there is already evidence that Russia intervened in the US presidential electi on in 2016, South Korea must also respond to North Korea's intervention in the election usin g cyber psychological warfare. In fact, Chinese hackers conducted cyber psychological warfare to divide South Korean people over the deploy ment of THAAD[1] in South Korea[2]. South Korea and Japan are still historically undissolved, and there is an issue of discharge of contamin ated water from Fukushima, so it is easy for third forces to interfere or separate them.

As the competition for supremacy between the US and China is intensifying, peace in the region cannot be guaranteed unless Korea and Japan closely cooperate to maintain peace on the Korean Peninsula and in Northeast Asia. We cannot rule out the possibility of North Korea's provocation aiming for a military vacu um on the Korean Peninsula that may occur as China invades Taiwan. Cyber security coopera tion between South Korea and Japan has more important strategic value than the operation of the existing military hotline. While the U.S.- Japan

1) Terminal High Altitude Area Defense(THAAD), formerlyTheater High Altitude Area Defense, is an Americananti-ballisticmissile defensesystem designed to shoot downshort,medium, andintermediate-range ballistic missilesin their terminal phase (descent orreentry) by intercepting with ahit-to-killapproach. THAAD was developed after the experience of Iraq'sScudmissile attacks during theGulf Warin 1991. The THAAD interceptor carries no warhead, instead relying on its kinetic energy of impact to destroy the incoming missile.

and U.S.-Korea cybersecurity cooperation has been focused on countering hostile countries such as North Korea so far, South Korea and Japan must become close allies not only in ph ysical space but also in cyberspace to actively respond to cyber threats from North Korea. So uth Korea is still considering joining the Inter national Cyber Crime Convention, but Japan has already joined and has maintained cyber s ecurity partnerships with the United States and European countries. Therefore, Japan's ability to collect and analyze cyber security informati on will not be inferior to that of Korea.

Recently, President Yoon Seok-yeol and Prime Minister Kishida visited the two countries and agreed to restore the relationship that had been solid so far and to make joint efforts for peace on the Korean Peninsula and in Northeast Asia[3]. This includes National Cyber Security. However, specific cooperation measures have not yet been presented. So, we look into what measures are specifically needed for cyber security cooperati on between South Korea and Japan. In this st udy, the conceptual framework for examining South Korea-Japan cyber security cooperation by reviewing existing literature and partnership model theories were utilized. In addition to exi sting research papers, Korea and Japanese gov ernments, international organizations, think tan k reports, and major foreign media were consu lted for literature analysis. Chatham House, Lexus, Nexis, and other online academic infor mation databases were also utilized. We have found that there is lack of academic research about the cooperation of cybersecurity between Korea and Japan. Although few existing resea rches are available, we have to analyze why there was no noticeble progress between two nations and what kind of factors hinder Korea and Japan relationship in terms of cyber security cooperation. Lastly, we will present solutions on how the two countries can better cooperate for cyber security against North Korea cyber atta cks. The next section examines previous resea rch and the progress made in the development of cybersecurity cooperation between Korea and Japan.

2. Development of Cyber Security Cooperation between Korea and Japan

In the era of the Fourth Industrial Revoluti on, Korea and Japan, leaders in advanced infor mation and communication technology, should contribute substantially to improving cybersec urity in Northeast Asia and the Global through strengthening cybersecurity cooperation. In this section, we examine the evolution of cybersecu rity cooperation between Japan and South Korea. Although there is not much prior research, it will be a good opportunity to give a new start ing point. Existing research has mainly focused on 'Changes of Cybersecurity Legal System in East Asia: Focusing on Comparison Between Korea and Japan'. This study compares 'Natio nal Anti-Cyberterrorism Act' of Korea with 'Basic Act on Cybersecurity' of Japan [4]. Ho wever, they did not see how to enhance the c ooperation between two nations. There are few other studies related to Cyber Capacity Building (CCB). Bimantara(2022)[5] reported that compa rative analysis between Korea and Japan. How ever, this study also limited to the The Norma tive Enactment of International Cybersecurity Capacity Building Assistance. Yoo, IT(2022)[6] study indicates that cybersecurity capacity buil ding (CCB) between Korea and Japan. This st udy found that Japanese CCB efforts are aligned

with Japan's national strategy wheras the ROK has approached CCB largely from the perspective of developmental assistance. In similar context, Kim, Yu-Kyung, et al.(2023)[7] reported that " Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis." This study analyzes cybersecurity cooperation in ASEAN Plus Three, explores fa ctors that influence cooperation. this can be a good reference to design the cooperation of cy ber security between Korea and Japan. From the commercial perspective, Pei, Y and Kim, SK(2023)[8] reported that Korea, Japan and Ch ina cooperation about digital trade. This study does not mention about the cyber security coo peration. It focuses on the possibility and impa cts of digital trade cooperation among the three countries in the Fourth Industrial Revolution.

Until now, South Korea and Japan have been the closest and distant neighbors. Regarding n ational security, only Dokdo[9], territorial seas and hukushima nuclear water release were of i nterest to each other[10]. In relation to North Korea, Japan has been interested in the abduct ion of Japanese citizens[11], but recently North Korean missiles and cyber threats have become a major concern. North Korea's missile and cy ber threats are straining the governments of South Korea, Japan and the United States. It remains to be seen whether North Korea's int ercontinental ballistic missiles reach the mainla nd[12], but cyber threats impend South Korea, Japan, and the entire United States. South Kor ea and Japan have established laws and cyber security agencies that are appropriate to their respective circumstances for cybersecurity. Korea government opened and operated the Na tional Cyber Security Center under the Nation al Intelligence Service in 2004, and under the current law, it is in charge of cyber security for government agencies and the public sector. As recent cyber threats and crimes are more c oncentrated in the private sector, the National Intelligence Service has tried for more than 10 years to enact the "National Cyber Security Act" that can be in charge of both the public and p rivate sectors, but the law has not been enacted due to opposition from the dissendant party[13]. In 2014, Japan enacted the Cyber Security Basic Act and started national-level cyber security a ctivities, and in 2015, the Cyber Security Strat egy Headquarters led by the Chief Cabinet Se cretary was established. National center of Inc ident readiness and Strategy for Cybersecurity (NISC) in charge of the strategic headquarters. With NISC as the command tower, the Nation al Police Agency, Ministry of Foreign Affairs, Ministry of Defense, Ministry of Internal Affairs and Communications, and Ministry of Economy, Trade and Industry, etc. are showing a full-fle dged and active appearance in response to incr easing cybersecurity threats under close coope ration[14][15].

Dialogue between South Korea and Japan on cyber security cooperation began only less than 1 year ago. In order to strengthen cyber securi ty cooperation between South Korea and Japan, it is necessary to understand the cybersecurity cooperation between South Korea and the Unit ed States. Yoon Suk-yeol government underst ands security cooperation with the United Stat es as a top priority[16]. At the Korea-US su mmit on May 21, 2022, there was a consensus among the leaders on strengthening cybersecu rity cooperation between South Korea and the United States [17]. On June 29, 2022, at IFEM A[2] in Madrid, the leaders of South Korea, the

2) Ifema(short forInstitución Ferial de Madrid; "Fair Institution of Madrid") is an entity charged with the organisation of fairs, halls and congresses in

United States, and Japan met for the first time in five years for a summit. The importance of the security alliance between South Korea, the United States, and Japan on the North Korea, China, and Russia war front-line and the impo rtance of cybersecurity cooperation was also mentioned[18]. On August 4, 2022, the first cy bersecurity meeting between South Korea, the United States, and Japan was held. It dealt wi th countermeasures to break the vicious cycle in which North Korea uses illegally stolen virt ual assets to fund the development of WMD (weapons of mass destruction). To this end, South Korea, the United States, and Japan est ablished a high-level consultative body and ag reed to actively cooperate on North Korea's m alicious cyber activities, including close inform ation sharing among the three countries, the is suance of joint security advisories, and measures against mixers that are used as virtual asset l aundering techniques[19].

Prior to this, Japan identified North Korea, Russia, and China as cyber threat countries at the Cyber Strategy Headquarter Meeting held in July 2021. Ironically, Japanese government had never disclosed the fact of a cyberattack by North Korea until October 2022[20].
However, in early October 2022, the Cabinet's Cyber Security Center, the Metropolitan Police Department, and the Financial Services Agency announced that North Korea's Lazarus hacker group had carried out attacks targeting Japane se crypto- currency companies and exchanges [21]. North Korea did not attack the Japanese government in cyberspace until October, 2022. Presumably, the reason for this is that they do not want to provoke Japan and provide an opp ortunity for cyber cooperation between South Korea and Japan. Although it is not officially disclosed, the strength of the Japan Self-Defense Forces exceeds that of most countries[22]. The refore, it is assumed that Japan's cyber power is also at a considerable level. However, after the US, Korea and Japan summit on June 29, 2022 in Madrid, North Korea has become hostile to Japanese government including cyberspace. No matter how much the goal was to steal cr yptocurrency, it is an important event that Jap an has been placed as an enemy in cyberspace. Such a trigger event was necessary to set the stage for strengthening cybersecurity cooperati on between South Korea and Japan. It is a fact that North Korea officially attacked Japan in c yberspace. As North Korea's cyberattacks incr ease, Japanese government will become more aware of the need for cyber security cooperati on with South Korea. In the following sections, we will discuss the possible types of cyberatta cks in North Korea.

3. Possible types of cyber attacks by North Korea against Japan

With the new strengthening of security coop eration between South Korea, the United States, and Japan, North Korea is likely to launch a f ull-scale cyberattack against Japan. Japan is c apable of responding to cyberattacks with force, according to “the 2021 Cyber Security Strateg y”. Rather than cyber attacks that destroy net works through technical attacks, North Korea will use cyber psychological warfare to disrupt the two countries' societies and distract public opinion through fake news. North Korea's cyber attacks that we can predict are as follows.

a) Wedge strategy

North Korea will attempt to reignite the issues of the past, especially the issue of Comfort

their facilities inMadrid.

Women and forced recruitment, in order to divide South Koreans and Japanese in an attempt to undermine the security cooperation system. The release of radioactive contaminated water from Fukushima will be a very good theme for separating the people of the two countries. Japan and South Korea have never been friends in history. However, in recent years, the situation in Northeast Asia has become difficult due to the hegemonic competition between the United States and China, and the triangular security system of South Korea and Japan led by the United States has been established. Since it is still in its early stages, we cannot rule out the possibility that North Korea's cyber-psychological warfare will lead to an estrangement in relations.

b) Cybercrime impersonating Japanese

North Korea's cyberattacks on Japan are more likely to occur in cyberspace as a means of social engineering. Recently, there have been many females pretending to be Japanese women on Facebook and other social networking services. They mainly aim to extort money from the victim men by using romance scam. South Koreans who have been victims of cybercrimes using social engineering techniques by North Korean cyber agents posing as Japanese women may be misled into believing that they have been victimized by the Japanese. Such misunderstandings will hinder the development of relations between the two nations.

c) Cyber attack via South Korea

In the past, when North Korea attacked South Korea, it was based in Shenyang, China.When attacking Japan, South Korea could be used to adversely affect bilateral relations. Cyberattacks could also use North Korean spies in South Korea. Using state-of-the-art IP laundering technology, it can be pretended that an attack was carried out in South Korea. Because of North Korea's deceitful tactics, we need concrete cooperation measures to prepare for this. In the next section, we will discuss what kind of cooperation between South Korea, Japan, and cyber security agencies is needed in the event of a North Korean cyberattack.

In the next section, we will discuss ways to strengthen cooperation between the cyber security agencies of Korea and Japan.

4. Strengthening Cybersecurity Cooperation between NCSC and NISC

On August 4, 2023, at a high-level meeting on cyber security cooperation between South Korea and the United States and Japan. In particular, cyber security cooperation between South Korea and Japan is important. If the security of Northeast Asia has been carried out under the leadership of the United States, from now on, South Korea, the United States, and Japan must all take responsibility together. Cyber security also requires joint action by the three countries. Cooperation between the NCSC and NISC is important for cybersecurity. While it is already in some stages of implementation, the following requirements will advance practical cybersecurity cooperation between the two countries.

a) Dispatch of Liaison Officer

Between National Cyber Security Center(NCSC) of Korea and National center of Incident readiness and Strategy for Cybersecurity(NISC) of Japan, cooperation officers should be dispatched to each other so that they can immediately

and jointly respond to urgent matters. Considering the immediacy that is one of the characteristics of cyberattacks, the role of the cooperation officers dispatched to the two countries will contribute to reducing the response time. In terms of cybersecurity, HUMINT through the Cyber liason Officer is also a necessary step for both countries.

b) Real-time cyber threat information sharing

Sharing cyber threat information is an essential requirement for cybersecurity cooperation. And it must be done in real time. Cyber evidence is volatile and must be judged and responded to immediately. It will require the same level of cooperation with the United States as cyber threat intelligence sharing. Mimicry cooperation does not build trust. Only by building a new security cooperation relationship based on cyber security cooperation can we effectively respond to North Korea's cyberattacks.

c) Joint Cyber Security Drills

Joint cyber security drills should be held on a regular basis so that both countries are always prepared for cyberattacks from North Korea. At the heart of the joint cyber security drills is the support of a country in the event of a cyberattack by North Korea. You need to define the scope of your support for each other. However, even allies are not allowed access to all areas. The more you train, the better outcome. It is necessary to prepare thoroughly for the actual cyber warfare.

d) Regular training and seminars

Geographically, they are the closest and farthest countries, but they should start their relations with the countries closest to each other through cyber security cooperation. For cybersecurity, experts from the two countries should meet frequently to exchange information and discuss each other's information through regular training sessions and seminars. As previous research has shown, not much information is known outside of the cyber laws of both countries. Because of the lack of information about each other, it is impossible to know exactly what is most effective for cooperation.

e) Establishment of a hotline

There should be no delay in establishing a hot line between the highest levels to carry out joint operations between the two countries in case of emergency. The hotline can be used to make important decisions that cannot be decided at the working level or when misunderstandings arise between the two countries. The symbolism of the hotline itself is to signal the commitment to strengthening Korea-Japan Cyber Security Cooperation.

5. Conclusion

This article has focused on strengthening cybersecurity cooperation between South Korea and Japan. The central argument of this research and main answer to the research questions is that there has been no full scale cooperation between Korea and Japan last two decades. The recent U.S.-led strengthening of security cooperation between South Korea and the U.S. and Japan has led to the strengthening of South Korea-Japan relations. In particular, as North Korea, China, and Russia are in tension with the United States, Japan, and South Korea, security cooperation between South Korea and Japan is essential including cyber security. This study receommended that close cooperation bet

ween NCSC of Korea and NISC of Japan at t he working level. It also emphacized that three possible type of cyber attacks by North Korea such as wedge startegy, impersonating Japanese and cyber attck via south korea. In order to i mprove the partnership between NCSC and NI SC, five suggestions introduced: Dispatch of L iaison Officer, Real-time cyber threat informati on sharing, Joint Cyber Security Drills, Regular training and seminars and Establishment of a hotline. Cybersecurity requires close cooperation between and among the three countries, along with South Korea, Japan, and the United States. Just as the five Anglo-American countries org anized and operated the Five Eyes, the United States, Japan, and South Korea should conduct similar cyber surveillance operations. When it comes to cybersecurity, prevention is the most important thing. It's best to detect it first and take a proactive response. In order to do so, t hey must have something like an echelon[3] sys tem that can monitor the movements of their enemies. So, it is necessary to form a "Triang ular Cyber-Surveilance System " by South Korea, the United States, and Japan, comparable to the Anglo-American Five Eyes, to monitor the mo vements of North Korea, China, and Russia.

An additional issue that can be explored in the future is to identify any obstacles to interrupt the cooperation or partnership of cybersecurity between two nations with its focus on organiz ational structure and culture, except the past i ssues.

3) ECHELON, originally a secret government code name, is a surveillance program (signals intelligence /SIGINT collection and analysis network) operated by the five signatory states to the UKUSA Security Agreement: Australia, Canada, New Zealand, the United Kingdom and the United States, also known as theFive Eyes. Created in the late 1960s to monitor the military and diplomatic communications of the Soviet Unionand its Eastern Blocallies during the Cold War, the ECHELON project became formally established in 1971. By the end of the 20th century, the system referred to as "ECHELON" had greatly expanded.

References

[1] Bartlett, J. (2020). Exposing the Financial Footprints of North Korea's Hackers.Center for a New American Security: Washington, DC, USA.

[2] Ernst, M., & Lee, S. (2021). COUNTERING CYBER ASYMMETRY ON THE KOREAN PENINSULA: SOUTH KOREA'S DEFENSE AGAINST CYBER ATTACKS FROM AUTHORITARIAN STATES.Journal for Intelligence, Propaganda & Security Studies, 15(1).

[3] Nishino, J. (2023). Japan's New Plan for a" Free and Open Indo-Pacific" and Its Challenges. Asia Policy,30(3), 17-25.

[4] Kim, K., Park, S., Lim, J. (2016). Changes of Cybersecurity Legal System in East Asia: Focusing on Comparison Between Korea and Japan. In: Kim, Hw., Choi, D. (eds) Information Security Applications. WISA 2015. Lecture Notes in Computer Science(), vol 9503. Springer, Cham.

[5] Bimantara, A. (2022). "The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices", Global: Jurnal Politik Internasional: Vol. 24: No. 1, pp.109-142.

[6] Yoo, I. T. (2022). Cybersecurity Crisscrossing International Development Cooperation: Unraveling the Cyber Capacity Building of East Asian Middle Powers Amid Rising Great Power Conflicts.Korea Observer,53(3).

[7] Kim, Y. K., Go, M. H., Kim, S., Lee, J., &

Lee, K. (2023). Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis.Journal of Internet Technology,24(2), 495-505.

[8] Pei, Y., & Kim, S. K. (2023). Digital trade: a new chance for China-South Korea-Japan trilateral cooperation?.Asian Affairs: An American Review,50(2), 120-137. Security Applications. WISA 2015. Lecture Notes in Computer Science(), vol 9503. Springer, Cham.

[9] Kim, S. (2010). Understanding the Dokdo issue: A critical review of the liberalist approach.The Journal of East Asian Affairs, 1-27.

[10] Liu, D., & Hoskin, M. (2023). Contemporary international Law: Regulating the upcoming fukushima radioactive wastewater discharge. Ocean & Coastal Management,234, 106452.

[11] Yamamoto, T. (2009). Abduction: Japan's Blunders in Negotiations with North Korea.North Korean Review, 34-42.

[12] Kristensen, H. M., & Korda, M. (2021). North Korean nuclear weapons, 2021. Bulletin of the Atomic Scientists,77(4), 222-236

[13] Yang, J. Y., Kim, S. J., & Oh, I. S. (2017). Analysis on south Korean cybersecurity readiness regarding North Korean cyber capabilities. InInformation Security Applications: 17th International Workshop, WISA 2016, Jeju Island, Korea, August 25-27, 2016, Revised Selected Papers 17(pp. 102-111). Springer International Publishing.

[14] Carapeto, R. (2021). The Japanese Basic Act on Cybersecurity and the historical development of the Japanese legal frame-work for cybersecurity.Int. Cybersecur. Law Rev.2, 65 - 76 (2021).

[15] OGAWA, H., & TSUCHIYA, M. (2021). Cybersecurity Governance in Japan. International Journal of Cyber Diplomacy, 7-31.

[16] Park, H. (2022). Changes and Continuities in South Korea's Major Foreign and Security Policies under the Yoon Suk-yeol Administration.East Asian Policy,14(04), 71-90.

[17] BBC News Korea (2022). 한미 정상회담서 죽한 '완전한 비핵화' 재확인...'전략적 경제안보 동맹'강화, BBC News Korea, 2022.05.21, https://www.bbc.com/korean/news-61532951, Viewed on October1, 2023.

[18] BBCNews Korea (2022). 한 미 일 정상회담 개최, 북 중 러 대응 전선 본격화, BBC News Korea, 2022.06.30, https://www.bbc.com/korean/news-61532951, Viewed on October 2, 2023.

[19] Bae, Gyung Hwan(2023). 한미일, 고위급 사이버안보 첫 회의… 北 대량살상무기 자금 차단 논의, 아시아경제, 2023.08.04, https://view.asiae.co.kr/article/2023080411232280718. Viewed on October 2, 2023.

[20] Consular officer, Japanese embassy in Korea. Interviewed on September 27, 2023.

[21] Park, Sang Hyun(2022). 일본경찰 "北연계 해킹조직, 日 가상화폐 기업 공격", Yonhap News, 2022.10.15, www.bbc.com/korean/news-61992344, Viewed on October 2, 2023.

[22] Akimoto, D. (2021). Japan's Multi-Domain Defense Force: The Space, Cyber, and Electromagnetic Domains.

〔저자소개〕

정 태 진(Tae Jin Chung)
평택대학교 피어선칼리지 교수
미시간주립대 정보통신학 학사
미시간주립대 형사사법학 석사
영국 리즈대학교 법과대학 박사
전) 국제기구(IVI) 보안기획관
현) 국가정보원 사이버안보센터 자문위원
현) 경찰청 안보수사국 사이버안보 자문위원
현) 대통령 경호처 인사심의위원
email :cyberpolicing@gmail.com