Hindawi
Security and Communication Networks
Volume 2022, Article ID 9962029, 10 pages
https://doi.org/10.1155/2022/9962029

Research Article

Military Information Leak Response Technology through OSINT Information Analysis Using SNSes

Yong-Joon Lee,[1] **Se-Joon Park**,[2] **and Won-Hyung Park**[3]

[1]*Department of Hacking Security, Far East University, Chungbuk 27601, Republic of Korea*
[2]*Department of Information Security Group, SK, Seoul 06750, Republic of Korea*
[3]*Department of Information Security Protection, Sangmyung University, Chungnam 31066, Republic of Korea*

Correspondence should be addressed to Se-Joon Park; sjoon0912@naver.com

Received 29 October 2021; Revised 12 December 2021; Accepted 23 February 2022; Published 30 March 2022

Academic Editor: Ilsun You

Open-source intelligence (OSINT), an information gathering and analysis system that utilizes public information on SNSes, is a necessary information gathering activity to counter terrorism and cyberterrorism. Although it is not possible to patrol cyberspace directly, as in real space, cyberspace can be patrolled by collecting information using OSINT technology. In this study, OSINT information analysis activities related to military information leakage are presented to SNSes. In this study, two or more OSINT collection tools are used to search for military information keywords, for characters' names, and for personal identification information about the characters. The results of 100,209 cases of military information keyword search and 471 cases of name search are presented. It was also confirmed that personal identification information was not searched because of the strengthening of personal information protection.

1. Introduction

As the use of SNSes is allowed in the military, there are continuous cases of leakage of military information through SNSes. This study is to present practical experiments and countermeasures for the leakage of military information through SNSes [1]. Open-source intelligence (OSINT), which is the collection and analysis of information using public information on SNSes, is a necessary information activity to counter terrorism and cyberterrorism. Terrorism is the most important aspect of real space, where victims, witnesses, and law enforcement agencies recognize terrorism [2]. Terrorism and cyberterrorism in cyberspace are difficult to recognize from the reports of victims and witnesses. Many terrorist attacks in cyberspace are difficult to identify [3]. Recently, military information has been leaked through SNS. Accordingly, intelligence agencies around the world are investigating military information leakage cases using SNS information collection technology. Information gathering channels on physical terrorism and cyberterrorism are equally applicable in cyberspace. Although it is not possible to directly patrol cyberspace, as in real life, it can be patrolled by collecting information using OSINT technology. In this study, OSINT information analysis measures related to military information leakage are presented to SNSes. To respond to military information leakage, Institute for the Study of Violent Groups (ISVG) and Study of Terrorism and Responses to Terrorism (START) were searched in the database of OSINT public information collected from SNSes worldwide, and the characteristics of Cyber Threat Analysis and Sharing (C-TAS) were investigated [4]. To cope with substantial military information leakage, two or more OSINT collection tools were used to search for military information keywords, for person names, and for personal identification information. In this paper, studies that collected information from existing SNSes were analyzed. The performance of various OSINT tools for collecting information from SNSes was verified. It was conducted through an experiment to collect military information using OSINT technology on SNSes. An experiment was conducted on SNSes to collect military information with OSINT technology, and a countermeasure was suggested through this [5].

The rest of this paper is organized as follows. Section 2 presents related studies on collecting military information using OSINT tools. Section 3 presents various experimental results for actual military information collection through OSINT tools. Section 4 presents the results of collecting and responding to military information through OSINT tools for SNSes.

2. Related Work

To analyze the efficiency of OSINT information analysis to deal with military information leakage through SNSes, we investigated the collection of OSINT information on ISVG and START in the field of terrorism. Furthermore, the characteristics of Korea's C-TAS were analyzed through a research survey on cyber threat information collected on SNSes in response to cyberterrorism [6].

2.1. Purpose of OSINT Utilization. Since September 11, 2001, terrorist attacks on Islamic fundamentalism have led to the increasing importance of OSINT technology, and OSINT has been actively utilized by the United States and NATO. This is because terrorist organizations such as Al Qaeda, the Taliban, Hezbollah, and Hamas are active online. The U.S. and NATO recognize OSINT as important information collection channels along with existing information collection channels, Human Intelligence (HUMINT), and Technical Intelligence (TECHINT). OSINT is different from existing information activities, and interest in OSINT collection, database construction, and information analysis on SNSes is increasing. The application areas of OSINT for collecting SNS information are as follows:

(i) Intelligence: the collection of information from OSINT and the secondary analysis of published information are used to understand important security threats, terrorism, and cyberterrorism. In OSINT, data mining, statistical analysis, location analysis, network analysis, and time-series pattern analysis are important [7].

(ii) SNS background survey (internet vetting): activities related to background surveys and profiles of specific individuals or groups. Recently, activities mainly take place in cyberspace, so they are more likely to collect information about the characteristics, history, and tendencies of specific individuals and organizations in online space than in offline space [8].

(iii) Crime investigation is an online activity used to secure criminal evidence. This activity, in contrast to digital forensics, includes information about witnesses and witnesses online [9].

2.2. ISVG (Institute for the Study of Violent Groups). The US ISVG program is a research project that uses federal research funds to build databases related to terrorism. ISVG is responsible for Sam Houston State University's College of Criminal Justice. The ISVG program uses OSINT information that can be collected on SNSes to build a database of information about terrorist organizations, terrorist organizations, and major terrorists around the world. Since 2004, more than 150,000 terrorist databases have been built. As can be seen in Figure 1, the database consists of a series of incident identification numbers that collect OSINT information from various SNSes on related events and people and organizations. Comprehensive incident information can be obtained by searching for specific terrorist events, people, and organizations [11]. About 20 researchers searched SNS information in real time and built a database to collect information on terrorist attacks in continents and regions. In addition, 11 additional language-related materials were searched, and the database entry language was English [12].

2.3. START (Study of Terrorism and Responses to Terrorism). START is a program supported by the U.S. Department of Homeland Security and is being studied by the University of Maryland to collect information on terrorism. As shown in Figure 2, START builds a variety of databases, but the Global Terrorism Database (GTD) related to terrorist attacks collects information published on SNSes in an OSINT manner. Information on terrorist attacks around the world, including incident information, attack information, weapons information, and damage information, was compiled into a database [14]. It collects systematic data on terrorist incidents worldwide and has at present collected more than 110,000 pieces of information. For each terrorist incident, it provides the date, location, weapons used, nature of the terrorist, number of victims, and identification information about the terrorist. The GTD database is open to the Internet and can be used by anyone for browsing and research [15].

2.4. C-TAS (Cyber Threat Analysis and Sharing). It is necessary to immediately and preemptively respond to cyber threats and to build intelligence to prevent accidents. Cyber threat intelligence can be categorized according to the organization's expertise in collecting information, enabling OSINT to build databases [16]. As can be seen in Figure 3, the Korea Internet & Security Agency (KISA) has established a cyber threat analysis and sharing system (C-TAS) that shares information about threat IPs, malicious code, vulnerabilities, etc., among other types of information provided by registered agencies. In a way that shares information, Cyber Threat Intelligence (CTI) is divided into Threat Intelligence Service (TIS) and Threat Intelligence Platform (TIP) in the form of a service or platform [18]. FireEye iSIGHT Intelligence provides CTI services at different levels based on API and web-based information values. This service assists with attacker synchronization, background, development environment, security issues, etc. [19]. Symantec's DeepSightTM Intelligence provides analysis and reputation information on major breaches of accident indicators. The main information provided provides reputation information such as IP, domain, URL, malware history, regional information, industrial information, owner information, and behavior information [20]. IBM provides cyber threat intelligence services and products to various service

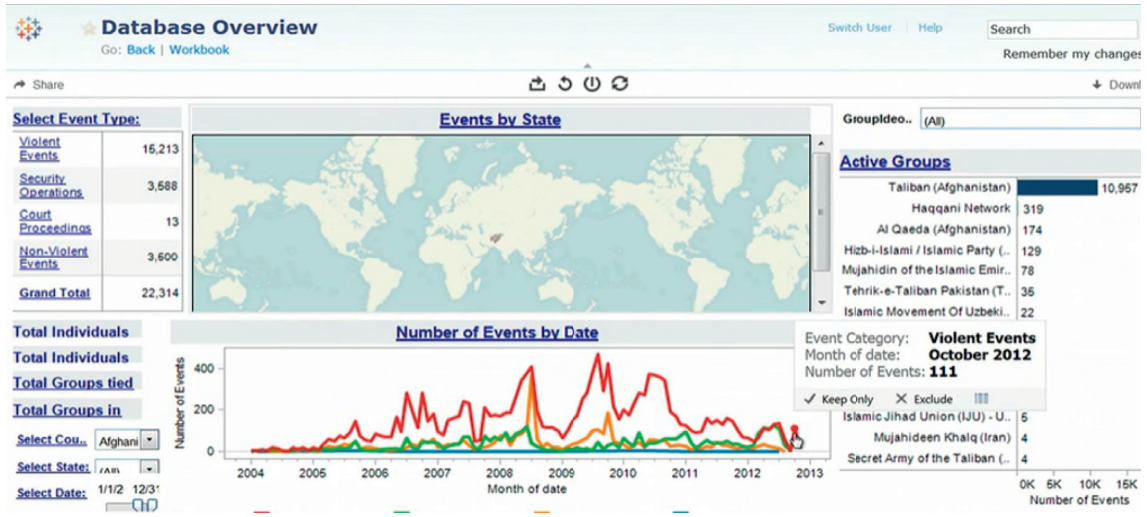


Figure 1: US Sam Houston State University ISVG database [10].

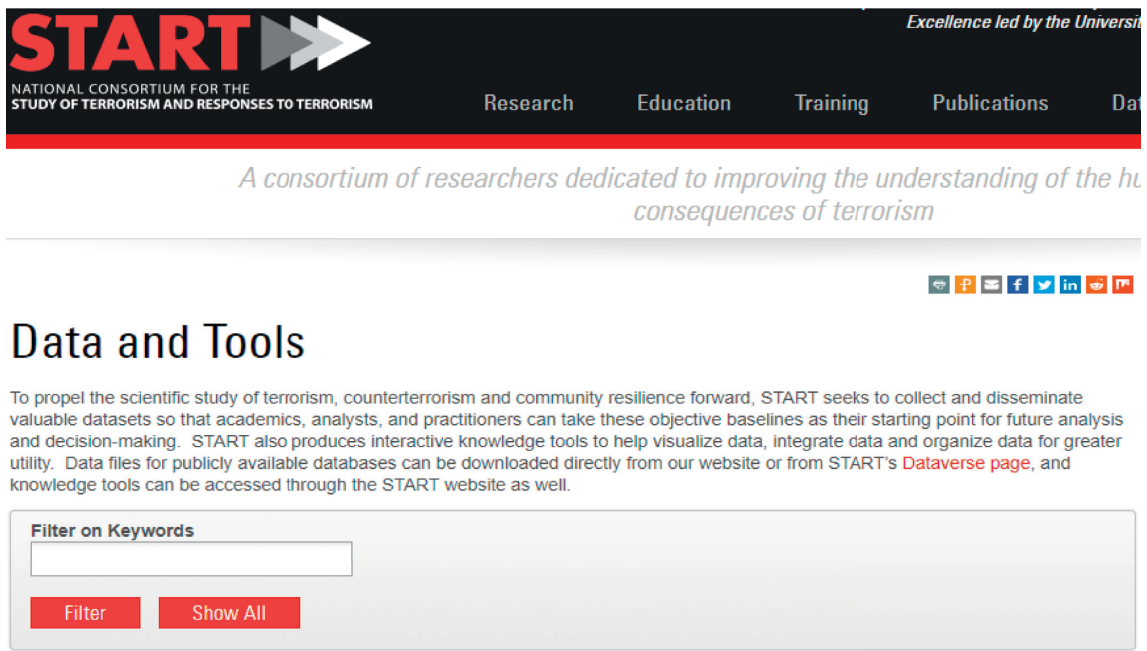


Figure 2: Maryland University START database [13].

subscribers through IBM i2 services, which previously expanded Watson for cybersecurity services [21].

2.5. Comparative Analysis of Terrorism and Cyberterrorism OSINT. This study investigates the construction of OSINT information published on SNSes and portal sites worldwide in response to terrorism and cyberterrorism [22]. As shown in Table 1, the anti-terrorism sector operates the ISVG and START databases in the United States. The purpose is to provide terrorist incidents, terrorists and organizations, sites of events, weapons used, and extent of damage to counterterrorism. In response to cyberterrorism, Korea's C-TAS has made cyber threat information, malicious code, and weaknesses unique to registered information security agencies. Researchers collect SNS information manually to counter terrorism, but information that is shared to counter cyberterrorism is characterized by automation [23].

3. Experiment

To cope with military information leakage, three experiments were conducted to analyze the efficiency of OSINT information analysis through SNSes. The SNS targets were Facebook and Instagram, and portal sites conducted OSINT information collection experiments on nine military information keywords, five military information names, and five military information personal identification numbers. In this paper, we presented the actual response results to the leakage of military information using SNS information

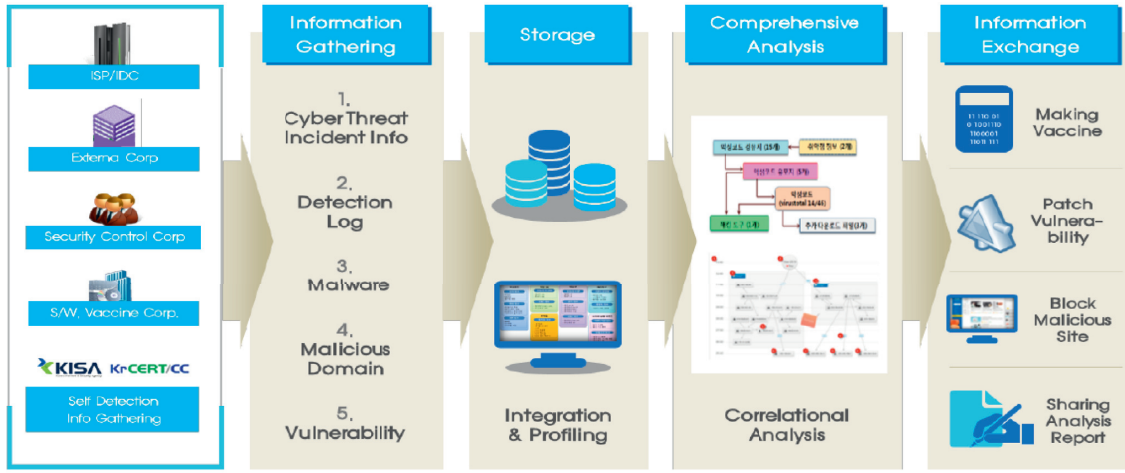


Figure 3: Korea KISA C-TAS database [17].

Table 1: OSINT information collection database via terrorism and cyberterrorism SNS.

OSINT database	Nation	Collection agency	Purpose	Collected information	Collection method	Amount of information
ISVG	United States	Sam Houston State University	Counterterrorism	(i) Terrorism (ii) Terrorist (ii) Organizations (iii) Location (iv) Weapons used	Passive (researcher)	150,000
START	United States	Maryland University	Counterterrorism	(i) Terrorism (ii) Terrorist (iii) Organizations (i) Location (ii) Extent of damage	Passive (researcher)	110,000
C-TAS	Republic of Korea	KISA	Cyberterrorism response	(i) Cyber threat information (ii) Malignant code, weakness	Automatic (information sharing)	Private

collection technology. Some of the SNS collection results can be used as collection technology for actual response.

3.1. Experimental Environment. Invisible Web, which is not displayed in relation to OSINT information collection, refers to websites that cannot be searched by search engines such as Google and Naver. Invisible Web and Deep Web cannot be searched through search engines, and less than 20 percent of websites are searched in cyberspace. To solve these problems, it is necessary to understand the characteristics, advantages, and disadvantages of various search engines for OSINT information collection. At least two or more search engines should be utilized to ensure the reliability and validity of OSINT collection materials, depending on the nature of the data required for a particular subject.

3.2. SNS Target Military Information Keyword OSINT Search Experiment. In this experiment, nine keywords related to military information leakage were collected from SNSes, and the amount of information collected and its accuracy were analyzed. The SNS targets were Facebook and Instagram, and the portal used four different OSINT search engines—Carrot2, WebSTAR, Biznar, and Imgur—on Google and Naver. Table 2 shows the characteristics of the OSINT search engines.

In this experiment, four OSINT search engines were used to collect information on nine keywords related to military information leakage on SNSes: military secrets, defense industry preferences, defense companies, defense capabilities, improvement projects, officers, weapons systems, and defense projects. Table 3 shows the results of the OSINT information collection experiments: WebSTAR (94,927 cases), Biznar (4,816 cases), Carrot2 (465 cases), and Imgur (1 case). The Imgur OSINT search engine mainly searched for images, so the amount of information analyzed was small. The search volume by keywords was 100,209, followed by officers (62,214), defense (25,197), reserve (8,148), defense industry preferences (1748), defense industry companies (725), weapons systems (629), military secrets (584), defense agency projects (552), and defense improvement projects (412). The level of information collection was high, and the speed of information collection was slow. However, owing to the large amount of information collected, the

Table 2: Characteristics of OSINT search engine for SNS target military information keywords.

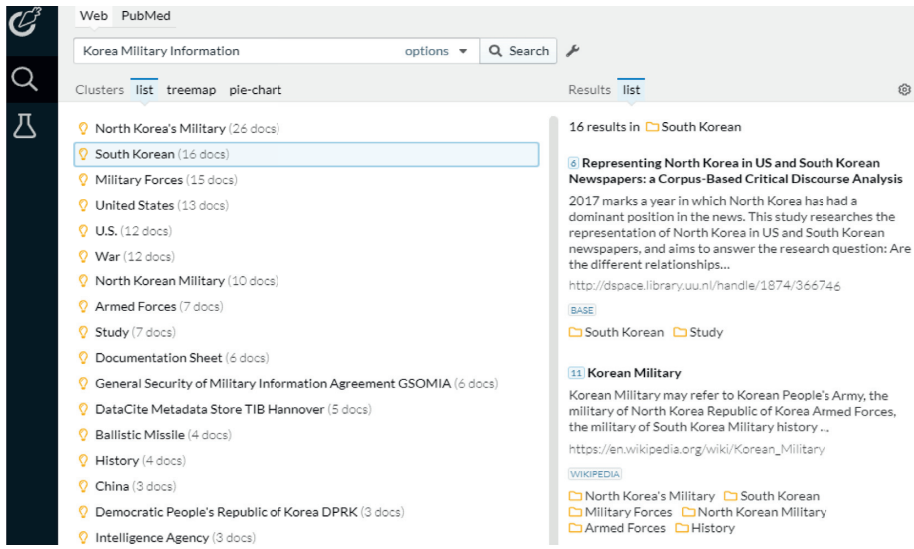
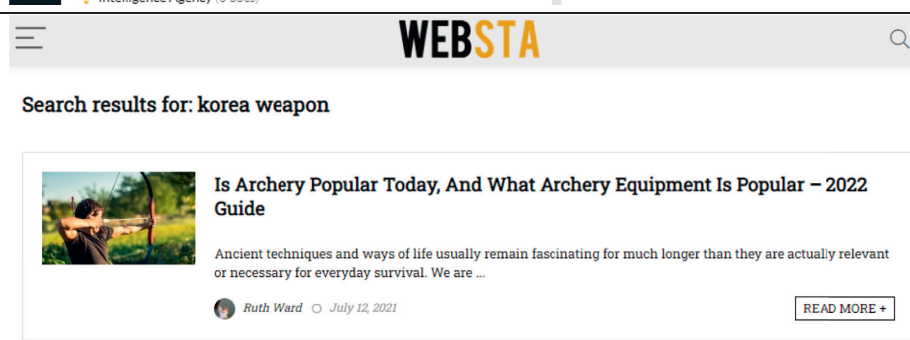
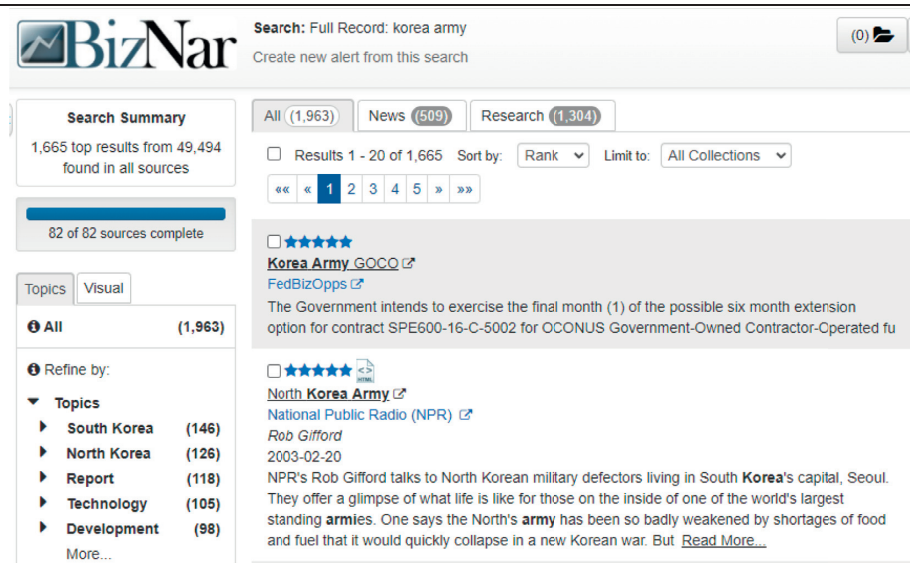
OSINT Search engine	Search	Characteristics
Carrot2 [24]		(i) Clustering engine for main search engine results
WebSTAR [25]		(i) Systematic and multilateral analysis of Instagram search results (ii) Provides keyword hashtag results together
Biznar [26]		(i) Google search results for Deep Web by theme and source (ii) Automatic notification function provided when keyword search results are checked

Table 2: Continued.

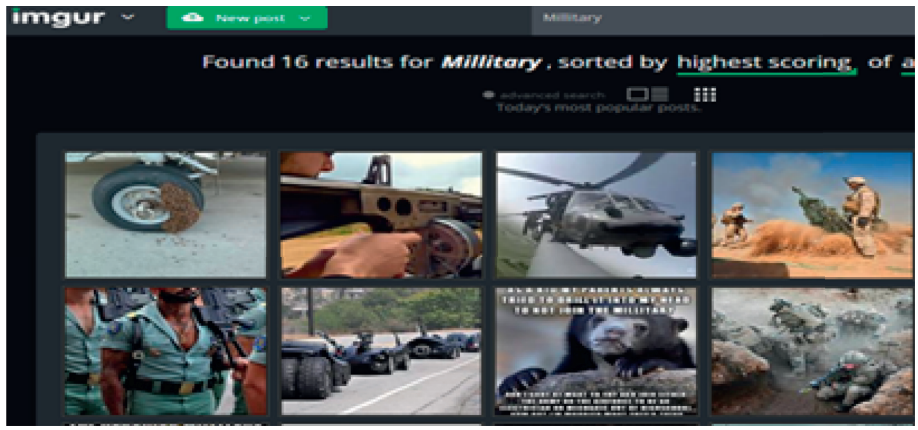
OSINT Search engine	Search	Characteristics
Imgur [27]		(i) Image-specialized hosting service (ii) Integrated image retrieval of major search engines

Table 3: Military information keyword search results for SNS objects.

	Analysis of military intelligence keywords									
OSINT search engine	Military secret	Preferential treatment for radiation	Defense industry company	Reserve army	Defense capability improvement project	Officer	Weapon system	National defense operation	Radiation agency project	Subtotal
Carrot2	52	45	48	47	30	66	66	70	41	465
WebSTAR	13	1,046	162	7,542	2	61,625	15	24,511	11	94,927
Biznar	519	657	515	559	380	523	548	615	500	4,816
Imgur	0	0	0	0	0	0	0	1	0	1
Sum total	584	1,748	725	8,148	412	62,214	629	25,197	552	100,209

accuracy of the information was low because of the large amount of information contained in the defect information. information was high because of the small amount of defect information.

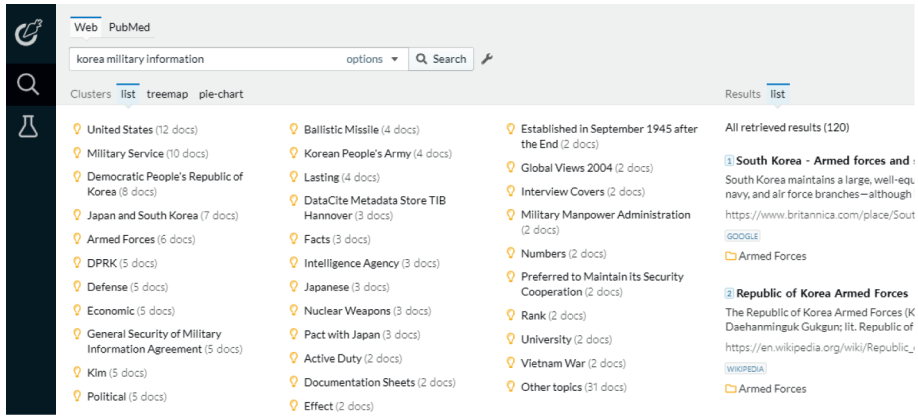
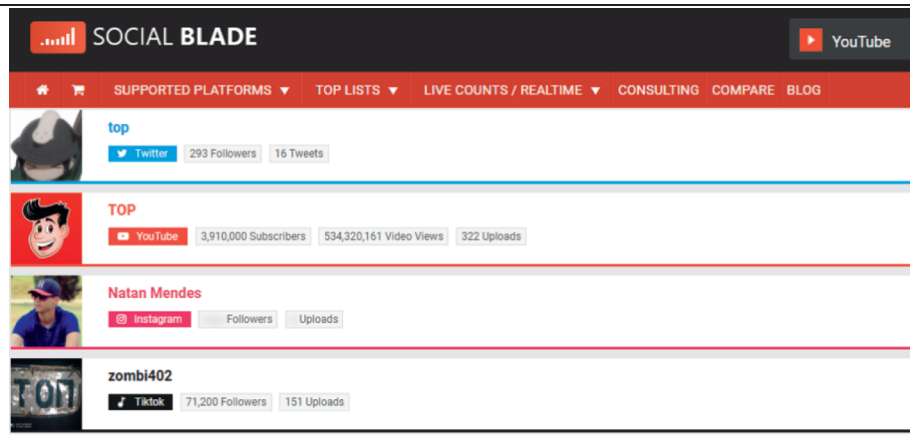
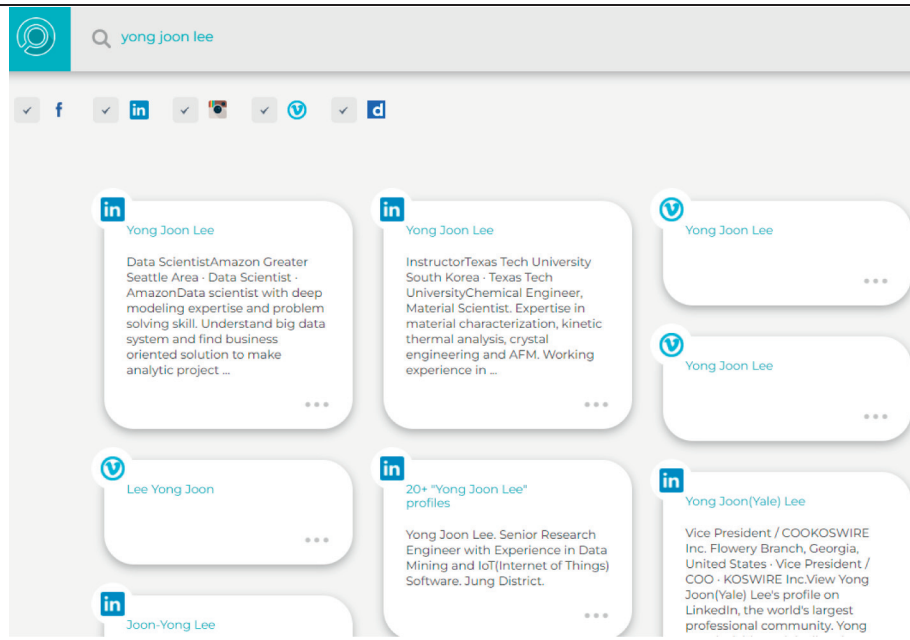
3.3. SNS Target Person Name Keyword Search Experiment. In this experiment, OSINT information was collected through statements about five people related to military information on SNSes, and the amount and accuracy of the information collected are discussed. The target SNSes were Facebook and Instagram, and the portal used three different OSINT search engines—Carrot2, Social Blade, and Social Searcher—to search Google and Naver. Table 4 shows the characteristics of the OSINT search engines.

In this experiment, three OSINT search engines were used to collect information on five people involved with military information on SNSes. In this study, any information about related people is presented in a non-identifying manner. In Table 5 Carrot2 (440), Social Blade (31), and Social Searcher (2), respectively were information collection for OSINT information collection. The Social Searcher OSINT search engine mainly searched for images, so the amount of information analyzed was small. The total collection volume was 471, followed by Person C (303), Person A (58), Person B (47), Person E (33), and Person D (30). The level of information collected was high, and the speed of information collection was high. Compared with the amount of information collected, the accuracy of the

3.4. Personal Identification Number Search Experiment for SNS Target Person. In this experiment, OSINT information was collected from the personal identification numbers of five people related to military information on SNSes, and the amount and accuracy of the information collected were discussed. The target SNSes were Facebook and Instagram, and the portals were Google and Naver using two OSINT search engines, Carrot2 and Pipl. Table 6 shows the characteristics of the OSINT search engines.

In this experiment, two OSINT search engines were used to collect information using the personal identification numbers of five people involved in military information on SNSes. In this study, information about related people is presented in a non-identifying manner. In Table 7 Carrot2 (4) and Pipl (3), respectively, were information collection for OSINT information collection. This is because the total collection volume is small, and the recent Personal Information Protection Law requires the government to delete personal identification numbers posted on SNSes. It was confirmed on the SNSes that, even if an individual agrees, his or her personal identification number would not be disclosed. The level of automation for collecting information was low, and the speed of collection was slow.

Table 4: Characteristics of SNS target person name keyword OSINT search engine.

OSINT search engine	Search	Characteristics
Carrot2		(i) Clustering engine for main search engine results
Social Blade [28]		(i) Clusters and provides key SNS public information (ii) Provides fast search for video materials through streaming-based search
Social Searcher [29]		(i) Provides clustering information for main search engine results

3.5. Expected Effect. As shown in Table 8, OSINT information is collected through SNSes, and the utilization of military information leakage is shown below. Regarding military information keywords, the amount of information was high, the accuracy of information was low, the level of automation was high, and the speed of collection was low.

Table 5: SNS target person name keyword OSINT search results.

OSINT search engine	Analysis of military intelligence keywords					
	Person (A) name	Person (B) name	Person (C) name	Person (D) name	Person (E) name	Subtotal
Carrot2	42	32	302	30	32	440
Social Blade	15	15	0	0	1	31
Social Searcher	1	0	1	0	0	2
Sum total	58	47	303	30	33	471

Table 6: Characteristics of OSINT search engines for personal identification numbers of SNS target characters.

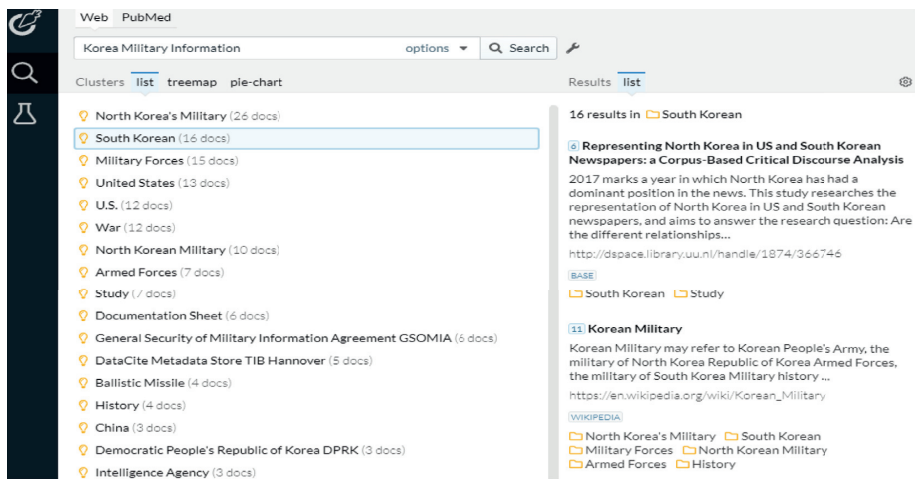
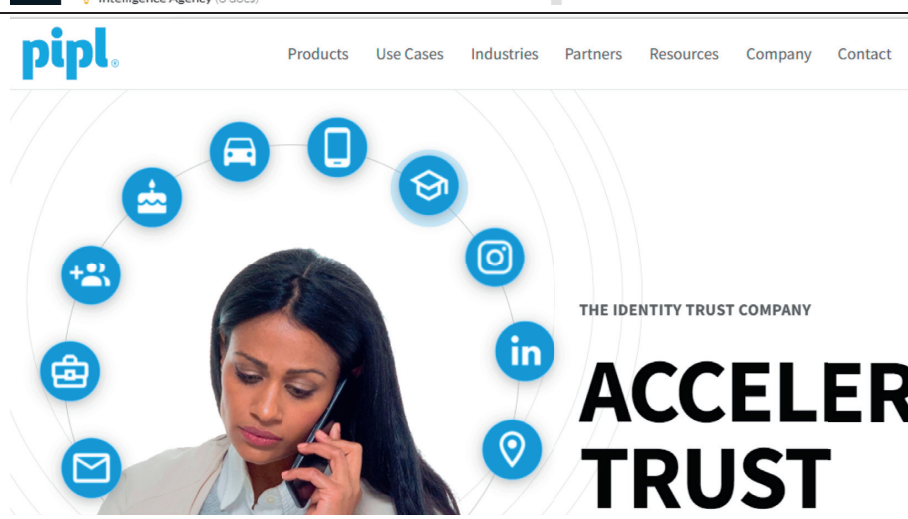
OSINT search engine	Search	Characteristics
Carrot2		(i) Clustering engine for main search engine results
Pipl [30]		(i) Provides personal information through paid services (ii) Provides SNS-saved archive information retrieval function for people

Table 7: SNS target person personal identification number keyword OSINT search experimental results.

OSINT search engine	Analysis of military intelligence keywords					
	Person (A) personal identification number	Person (B) personal identification number	Person (C) personal identification number	Person (D) personal identification number	Person (E) personal identification number	Subtotal
Carrot2	1	0	1	0	2	4
Pipl	1	0	2	0	0	3
Sum total	2	0	3	0	2	7

Table 8: OSINT information analysis experimental results by SNS to respond to military information leakage.

Search content	OSINT collection and utilization						
	Search engine	Number of searches	Amount of information	Accuracy of information	Automation level	Collection rate	Utilizability
Military intelligence keyword	(i) Carrot2 (ii) WebSTAR (iii) Biznar (iv) Imgur	100,209	Upper	Lower	Upper	Lower	Upper
Person's name	(i) Carrot2 (ii) Social Blade (iii) Social searcher	471	Middle	Middle	Upper	Upper	Upper
Personal identification number	(i) Carrot2 (ii) Pipl	0	Lower	N/A	Lower	Lower	Lower

The overall utilization rate was excellent. Regarding the statements of military intelligence officials, the accuracy of the information and the accuracy of the information were intermediate, and the speed of automation and collection was high. Owing to the strengthening of the Personal Information Protection Law, the personal identification numbers of military intelligence personnel were considered to be ineffective.

4. Conclusion

OSINT, an information gathering and analysis system that utilizes public information on SNSes, is a necessary information activity to counter terrorism and cyberterrorism. It is impossible to respond without recognizing the collection of information about terrorism in real space. Therefore, terrorist awareness is the most important stage, and in real space, victims, witnesses, and law enforcement agencies recognize terrorism. Terrorism and cyberterrorism in cyberspace are difficult to recognize from the reports of victims and witnesses. Many terrorist attacks in cyberspace are difficult to identify. Although it is not possible to patrol directly in cyberspace, as in real space, cyberspace can be patrolled by collecting information using OSINT technology. In this study, OSINT information analysis activities for military information leakage were presented to SNSes. In this study, two or more OSINT collection tools were used to search for military information keywords, characters' names, and the personal identification information of characters. Regarding the utilization of OSINT information through SNSes to cope with military information leakage, the amount of information, accuracy of the information, automation level, and collection speed were low. The overall utilization rate was excellent. Regarding statements by military intelligence officials, the accuracy of the information and the accuracy of the information were intermediate, and the speed of automation and collection was high. Owing to the strengthening of the Personal Information Protection Law, the personal identification numbers of military intelligence personnel were considered to be ineffective. Further research will be conducted on the combination of location information on terrorism and cyber threat information and the correlation with relevant secondary information.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] L. Caviglione, S. Wendzel, A. Mileva, and V. Simon, "Multidisciplinary solutions to modern cybersecurity challenges," *JoWUA*, vol. 12, no. 4, pp. 1–3, 2021.

[2] G. Lacava, A. Marotta, F. Martinelli et al., "Cybsersecurity issues in robotics," *JoWUA*, vol. 12, no. 3, pp. 1–28, 2021.

[3] N. Polatidis, E. Pimenidis, M. Pavlidis, S. Papastergiou, and H. Mouratidis, "From product recommendation to cyber-attack prediction: generating attack graphs and predicting future attacks," *Evolving Systems*, vol. 11, no. 3, pp. 479–490, 2018.

[4] K. Huang, C. Zhou, Y.-C. Tian, S. Yang, and Y. Qin, "Assessing the Physical Impact of Cyberattacks on Industrial Cyber-Physical Systems," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 10, pp. 8153–8162, 2018.

[5] C. Heinz, M. Zuppelli, and L. Caviglione, "Covert channels in transport layer security: performance and security assessment," *JoWUA*, vol. 12, no. 4, pp. 22–36, 2021.

[6] J. Martínez Torres, C. Iglesias Comesaña, and P. J. García-Nieto, "Review: machine learning techniques applied to cybersecurity," *International Journal of Machine Learning and Cybernetics*, vol. 10, no. 10, pp. 2823–2836, 2019.

[7] M. Husak and J. Kaspar, "Towards predicting cyber attacks using information exchange and data mining," in *Proceedings of the 2018 14th International Wireless Communications Mobile Computing Conference(IWCMC)*, Limassol, Cyprus, June 2018.

[8] A. A. AhmedandN and A. K. Zaman, "Attackintention Recognition: Areview," *IJ Network Security*, vol. 19, no. 2, pp. 244–250, 2017.

[9] E. Cho, "A system for national intelligence ActivityBasedonAll kindsof OSINT(OpenSource INTelligence)

ontheInternet," *Journal of Information Security*, vol. 3, no. 2, pp. 41–55, June2003.
[10] Honormonument, "Honor the Victims of Terrorism," 2022, https://honormonument.org/2020/06/22/the-institute-for-the-study-of-violent-groups-isvg.
[11] Y.-B. Leau and S. Manickam, *Network Security Situation Prediction: A Review and Discussion"*, Springer, Berlin Heidelberg, 2015.
[12] B. Aziz, "A note on the problem of semantic interpretation agreement in steganographic communications," *Journal of Internet Services and Information Security*, vol. 11, no. 2, pp. 47–57, 2021.
[13] Start, "Global Terrorism Database," 2022, https://www.start.umd.edu/gtd.
[14] N. Badie and H. Lashkari, "Anewevaluation criteria for effective security awareness in computer riskmanagement based on AHP," *Journal of Basic and Applied Scientific Research*, vol. 2, no. 9, pp. 9931–9947, 2012.
[15] E. Bashier and T. Ben Jabeur, "An efficient secure image encryption algorithm based on total shuffling, integer chaotic maps and median filter," *Journal of Internet Services and Information Security*, vol. 11, no. 3, pp. 46–77, 2021.
[16] L. D. Bodin, L. A. Gordon, and M. P. Loeb, "Information security and risk management," *Communications of the ACM*, vol. 51, no. 4, pp. 64–68, 2008.
[17] Krcert, "Cyber threat information analysis and sharing (C-TAS) system," 2021, https://www.krcert.or.kr/webprotect/ctas.do.
[18] Symantec, "ISTR Internet Security Threat Report," 2019, https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf.
[19] Fireeye, "Bericht M-Trends," 2021, https://www.fireeye.com/current-threats/annual-threat-report.html.
[20] S. Rahmadika, M. Firdaus, S. Jang, and K.-H. Rhee, "Blockchain-enabled 5G edge networks and beyond: an intelligent cross-silo federated learning approach," *Security and Communication Networks*, vol. 2021, no. 4, pp. 1–14, 2021.
[21] Sans, "The Evolution of Cyber Threat Intelligence(CTI): 2019 SANS CTI Survey, Sans," 2019, http://org/reading-room/whitepapers/threats/paper/38790.
[22] J. M. Acuff and M. J. Nowlin, "Competitive intelligence and national intelligence estimates," *National Intelligence Studies*, vol. 34, no. 5, pp. 654–672, 2019.
[23] M. Yun, "Construction of database for terrorism and Crime through OSINT," *The Korean Association of Criminal Psychology*, vol. 13, no. No.2, pp. 113–136, 2017.
[24] Search, "Carrot2," 2021, https://search.carrot2.org/#/search/web.
[25] Webstagram, "Instagram Search Account Instagram Web Viewer," 2022, https://webstagram.org.
[26] Biznar, "Deep Web Technologies," 2022, https://biznar.com/biznar/desktop/en/search.html.
[27] Imgur, "Be the memes you want to see in the world," 2022, https://imgur.com.
[28] Social Blade, "Analytics Made Easy," 2022, https://socialblade.com.
[29] Social-searcher, "Free Social Media Search Engine," 2022, https://www.social-searcher.com.
[30] PIPL, "Theidentity trust company," 2022, https://pipl.com.