

Conceptualizing the cyber incident & event statistics reporting standards

Sang-Oun LEE*, H.J. SEO**

*The University of Chicago Harris School of Public Policy, Chicago, IL, USA

**The Attached Institute of ETRI, Daejeon, Korea, a corresponding author

sangounlee@uchicago.edu, hjseo@nsr.re.kr

Abstract— The development of technology led the cyberspace to be directly connected to the daily life. For a nation, it is essential to collect and analyze the statistics produced from cyber-attack incidents to formulate a policy. Specifically, in the Republic of Korea, the second most cyber-attacked country in the world, the synchronization between the cybersecurity technology and policy is essential. However, in current status, the statistics collected by the government ministries in Korea is varied. For instance, the Ministry of Defense and the Ministry of Science & Technology has a different standard in defining the event and incident and its numbers. Thus, the study aims to propose a standardized concept of cyber incident and event statistics which can provide singularized criteria which can be adopted across the ministerial disciplines. In order to provide aforementioned concept, the authors have posed following research questions. First, how to conceptualize the different types of cyber-attacks into a single standard of reporting cyber incidents? Second, what is the proper definition for cyber incident in both national and international levels of policy dialogue? Third, will the established concept can be proposed as an international standard? The authors first breakdown the scattered conceptual knowledge of cybersecurity by the methodology proposed by Gerring (1999) to provide a better concept which can deliver the better knowledge in cybersecurity policy. After, the authors propose the qualitative method in order to develop the single standard in collecting cyber incident statistics. Finally, the authors leave the possible extensions for future related research area based on the proposed method.

Keywords— Cybersecurity, incident, event, statistics, mixed methods

I. INTRODUCTION

The development of technology led the cyberspace to be directly connected to the daily life [1]. For a nation, it is essential to collect and analyze the statistics produced from cyber-attack incidents (henceforth cyber incident) to formulate a policy. Specifically, in Republic of Korea, the second most cyber-attacked country in the world with the explicit state enemy under a war, the synchronization between the cybersecurity technology and policy is essential. However, the rapid development has led the related definitions of cyber-attack categories to be different by the corresponding organizations. For instance, if 100 incidents occurred for hacking e-mails, counting method of the incident is differed by the organizational types. Based on the damage, if the 2

groups have been damaged by the incident, the incidents are counted as 2 incidents. However, if the damage was occurred by the same methodology of malicious code, the incident will be counted as 1. At the same time, if the malicious code infected 100 computer systems, the count for this incident can be also counted as 100.

In Republic of Korea, the network is divided into three which are private, public and national, and defense [3]. Each network has a different corresponding governmental ministry to be responsible for cyber-attacks. As the given example above, the National Assembly asks cyber statistics. However, three corresponding Ministries in Republic of Korea are using different standards of counting and producing the statistics of cyber incidents. A ministry counts incidents both the successful attacks and the attempts which are detected. In case of malicious code attack, the incidents are counted regardless of how close the previous and current incidents are occurred. The private sector network is also adopting the similar standards of counting cyber incidents, which is detected instead of compromise. The type of detection includes Distributed Denial of Service (DDoS) attack, smishing, phishing and pharming [4]. Unlike the other two networks aforementioned, the private network is unavailable to examine by the governmental authority, the data announced from the quality of the statistics are highly dependent on the reports from those who are compromised or those who detected the incidents.

Aforesaid differences in standards for collecting cyber incident data by the types of networks may cause confusion on the reliability of the statistics. Furthermore, the user of the statistics is burdened to understand the sectoral differences which bring additional confusion. Therefore, this research intends to propose a concept of standard in collecting incident statistics in order to provide generic standard over the sectoral networks. The potential contribution of this research is followed. First, the single standard for collecting cyber incident statistics will solve the prevailing confusion from different criteria by the types of networks. Second, decreased confusion will be also introducing more efficiency in the policy making process based on the statistics collected.

In order to tackle the problems stated above, the author poses following research question to build up a reporting

standard of cyber incident across the different types of networks.

1. How to conceptualize the different types of cyber-attacks into a single standard of reporting cyber incidents?
2. What is the proper definition for cyber incident in both national and international levels of policy dialogue?
3. Will the established concept can be proposed as the international standard?

The following section of the paper is composed of the following sections. First, the paper will analyze the concepts of cyber incidents in Korea and internationally. Second, the author employs a methodology of conceptualization proposed by Gerring (1999) [5] to apply in building concepts of cyber incidents. Third, extending from the application in the previous section, the authors conduct qualitative analysis by conducting in-depth interview to conceptualize a single standard in collecting cyber incident statistics. Fourth, the author proposes conceptualizes the standard for statistical data collection of cyber incidents with possible extensions for future research.

II. REVIEW OF CYBER INCIDENT CONCEPTS

Current laws in Korea does not differentiate between the event and the incident of cyber-attack. According to the 2nd clause at the “Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.” (henceforth Network Law), cyber incident is defined as an action of attacking an information system through hacking, computer virus, logical bomb, mail bomb, service denial or high-frequency electronic pulse [6]. Whether the attack successfully compromised the target information system or just detection of the attack is not clearly defined in the Network Law. Therefore, ambiguous expression of the Network Law leads to the confusion of whether the compromise or detection should be counted into a cyber-incident. Furthermore, the Network Law illustrates the concept of cyber incident by a technical methodology that are used in cyber-attack, the status quo statistical data collected mainly collects the data by similar categories but varied criteria. Even though other laws such as “Personal Information Protection Act” also mentions about the cyber incidents, the elaborations on cyber incident is not defined clearly [7].

In contrast, the physical realm of incidents is conceptualizing the notion of an “incident” by the accumulation of experience throughout the history. In aviation incidents, according to the 2nd clause of “Aviation Safety and Security Act”, the aviation incident is defined as any incident occurred from the moment when the person is boarding on an airplane to the moment when everybody on the plane getting off. In addition, the types of incidents are defined as: 1) the death, heavily wound or loss of a passenger, 2) structural or explicit damage to the aircraft, 3) unidentifiable position of the aircraft or unavailable to approach to the aircraft [8]. Aviation incidents are mentioning about the period of the incident, and the Ministry of Land, Infrastructure and Transport is explicitly taking care the crisis control.

In the case of the United States, unlike Korea, the event and the incident is explicitly breaking down into details. According to the Department of Defense [7], cyber incident response, process, reporting method, analysis and tools to handle cyber incident is defined clearly which divides the notion of event and incident. According to the CJCSM 6510.01B, all the cyber incident should be reported, and the reportable event is also further defined in the document (Ibid.). In addition, the Department of Homeland Security [9] is also dividing the concept of the event and incident. The difference between the Department of Defense and the Department of Homeland Security is about whether to define the difference of root-level attack and the user-level attack by a single case or separate cases.

III. APPLICATION OF CONCEPTUALIZATION METHODOLOGY BY GERRING

Gerring (1999) argues that goodness in concept formation cannot be reduced to ‘clarity’, to empirical or theoretical relevance, to a set of rules, or the methodology particular given study [5]. Rather, Gerring (1999) argues to form a concept by eight (familiarity, resonance, parsimony, coherence, differentiation, depth, theoretical utility, and field utility) criteria. Though the method proposed by Gerring is to conceptualize a concept, this research employs this method and attempted to define the single standard for cyber incident statistics [5]. The following application has covered five criteria out of eight which were originally argued by Gerring.

First, familiarity is about a matter of degrees. The present meaning of the given concept should be harmonized with the new meaning. In order to be the new definition of a concept to be accepted depends on whether it is available to be facilitated in daily lives with differing levels of clashes with the status quo. For familiarity to be secured, a new definition should contain as much standardized sense as possible, while not be clashing with the status quo. For instance, when a concept for cyber incident is proposed, the concept should contain the standardized knowledge and backgrounds on the concept itself, while not being clashed with the status quo.

Second, resonance according to Gerring is about how a given concept can be recognized widely. In other words, even though a concept has a same meaning, some concept may be widely accepted but others may not be widely accepted and perish. A concept should not only include clarity, but also should have the vitality of a concept. Gerring called an example of Marx. According to Gerring, Marx has employed ‘proletariat’ instead of ‘labor class’ in order to strengthen his argument over the public. Specifically, in case of cyber related concepts, because most of the concepts are brand new, the lack of resonance will lead to fail to build a concept. If a concept is selected among the technical jargons which are complicated for the general public, the resonance is hardly secured.

Third, parsimony requires a concept to be simple. If a concept contains multiple notion that are overlapped, it is hardly called as a well-established concept. At the stage of building a concept, the builder should consider how the

concept would be interpreted and accepted to the user. As mentioned above, because the cyber area is full of new concepts. Even though it is difficult to deliver a new concept simply straightforward, but the parsimony should also be considered to deliver the clear meaning of the concept.

Fourth, coherence is not only a matter of specifics that define a concept, but also includes all the characteristics that is naturally contained in the phenomenal situations. Coherence is even more emphasized when the characteristics are under the relationship where it is not clear, not the case where the characteristics are contradicting.

Fifth, differentiation is one of the most important criteria for defining concepts, because the determination of characteristics is based on the recognition of the difference between the status quo reality and the newly introduced concept. If the concept of incident and event employed from other physical realms definitions in the legal system, it is applicable to differentiate the event and the incident because of the following reasons. First, as the familiarity criterion argues, the concept should not be clashed with the status quo. Thus, in the cyber realm, the event and the incident should be independently defined concepts. In addition, the differentiation criterion also supports the division of incident and event because it identifies the detection of a cyber-attack and actual damage from a cyber-attack.

In addition, even though the damage was happened on the information system, it is reasonable to exclude such damages caused by the extinction of the resources or internal errors because of the following. According to the 2nd clause of the Network Law, the event occurred by the action of attacking an information system excludes the intra-organizational issues such as system errors. In addition, it also violates the Gerring's coherence criterion which was introduced above. Therefore, the intra-organizational incidents not caused by external cyber-attacks are excluded in defining a cyber-incident or event.

This section has recognized the concept building level of a cyber-incident and an event to develop the further study to define and establish a standard measure of criteria in cyber incident and event statistics collection. Gerring's methodology provided a clearer sense on how the national cyber incident and event should be defined. Further, the analysis and application of Gerring's method suggest to exclude the incident occurred by intra-organizational causes.

IV. RESEARCH METHODOLOGY

Exploring the posed questions cannot be solely done by quantitative analysis because of the following reasons. First, because the cybersecurity policy is relatively new field of analysis academically, the notions or concepts used in the field also shares similar issues of different standards or interpretations [9]. Thus, it is difficult to rely on the previous studies or given data. Second, the purpose of this research is not a development of methodology to analyze the cyber incident statics. Instead, the purpose of this study is to develop the standard concept of counting cyber incidents to build

statistics. Therefore, sole quantitative analysis is not applicable to provide the answers to the research questions.

The research intends to engage the mixed-method study to conceptualize the undefined standards of cyber incidents and cyber event concepts. The quantitative data will collect the cyber incident report data from corresponding ministries of the Republic of Korea for both the event data and the incident data to configure whether the status quo collection of statistics and its definition by each networks is applicable. In this stage, the collected data will be regressed with the National Cyber Threat Alert Index, which is operated by the National Cyber Security Center to determine which networks' data collection standard is well representing the status quo complementary index on cybersecurity in the republic of Korea.

Secondly, the collected data will also be divided and sorted by the status quo criteria differed by the characteristics of the networks (Public & Government, Defense, and Private Sector) to verify the appropriateness of building single standard. The quantitative analysis will lead to the application of Gerring's five criteria of building a concept as aforesated. Based on the given criteria, each definition which are overlapped and not standardized will be employed in developing the questionnaire for qualitative data collection.

The qualitative data collection will include an extensive interview of 40 professional panels who have served in this field for more than 7 years with holding a postgraduate degree in related field such as cybersecurity, computer science, mathematics and policy. The extensive interview will present the collected quantitative piece and present to the interviewees to inquire what can be the medium standard that could cover both of the networks. The interviewers will include the author and two more professionals in cybersecurity policy who served the field as a researcher for more than 7 years with holding a postgraduate degree.

Extensive interview sessions will be video recorded unless the interviewee requests anonymity. Several interviewers who are currently affiliated with the government sector requested anonymity. However, if the video record is not conducted to those who requested in advance, the facial or gestural expressions during the research will be coded by the assistant interviewer during the interview. The coding process of the qualitative data will contain the following. First, the orally recorded data will be scripted by the word processor form and map with the questionnaire that are previously developed by employing the Gerring's concept building criteria. Secondly, the scripted data will add the facial and gestural expression within the scripts to determine whether the further information can be appended over the script. A conclusion may review the main points of the paper. Please do not replicate the abstract as the conclusion. A conclusion might elaborate on the importance of the work or suggest applications and extensions.

V. EXPECTED CONTRIBUTIONS AND LIMITATIONS

This research proposes a mixed method analysis to develop a standard concept for cyber incident statistics criteria. Since the area of study is relatively new field, the statistical data collection criteria differ by the types of networks in the

Republic of Korea. Therefore, the proposed methodology will contribute on conceptualizing the cyber incident statistics by following.

First, the statistical analysis of status quo statistical data from the public & government networks, defense networks, and the private sector networks with the National Cyber Threat Index in Korea will provide which networks' criteria represent the cyber landscape of the Republic of Korea. However, the statistical analysis also may suggest that present criteria are not applicable to represent the underlying cyber environment. Second, because the Gerring's method was initially employed to validate the appropriateness of the concept of dividing the incident and event in the cyber realm, the employed criteria will suggest carefully designed questionnaire for the proposed interview on conceptualizing cyber incident statistics in Korea to the professionals. Third, the proposed interview and analysis are conducted to the focus group in order to build a concept where the field knowledge is well synchronized with the reality.

The research will contribute in developing complementary cyber statistics with standardized concepts. The standardized concepts proposed in this research are expected to contribute in solving status quo inefficiency in policymaking processes of cybersecurity across the sectoral networks. The efficient policy design will not only facilitate the inter-sectoral corporations in cybersecurity, but also facilitate further discussions in the cybersecurity policy academia. Further, the consumers of this research will initially be the policymakers in cybersecurity, however, will be extended to the general public because of the advancement of cyber technologies as well as cyber threats.

However, the proposed research owns following limitations. First, because the quantitative data and qualitative data originate in Republic of Korea, the research results may require further interactions with global standards. Second, the qualitative analysis may provide a grasp in concept building in cybersecurity policy, but it also may fail to fully explain the technicalities within the current jargons that are widely used in the technical field of cybersecurity. Even though one of the objectives of this research is to bridge the detached knowledge between the policy and the technology, the qualitative analysis may not be able to represent the technicalities fully.

REFERENCES

- [1] Lee, S. O., Hong, A., & Hwang, J. (2017). ICT diffusion as a determinant of human progress. *Information Technology for Development*, 23(4), 687-705..
- [2] Lee, S. O. (2018). A New Warfront: North Korea's Cyber Threats. *Chicago Policy Review* (Online).
- [3] Korea government, National Information Security Whitepaper 2018
- [4] KISA, Retrieved June 4, 2018, from <http://www.kisa.or.kr/>.
- [5] Gerring, J. (1999). What makes a concept good? A criterial framework for understanding concept formation in the social sciences. *Polity*, 31(3), 357-393.
- [6] Act No. 14080, "Act on Promotion of Information and Communications Network Utilization and Information Protection, etc.", Republic of Korea.
- [7] Act No. 14107, "Personal Information Protection Act", Republic of Korea.
- [8] Act No. 14116, "Aviation Safety and Security Act", Republic of Korea
- [9] CJCSM 6510.01B: Cyber Incident Handling Program., Retrieved from <http://www.jcs.mil/Portals/36/Documents/Library/Manuals/>.
- [10] H.R. 5074: DHS Cyber Incident Response Teams Act of 2018. (n.d.). Retrieved from <https://www.govtrack.us/congress/bills/115/hr5074/text>.
- [11] Anderson, R. (2001, December). Why information security is hard-an economic perspective. In *Computer security applications conference, 2001. aacsac 2001. proceedings 17th annual* (pp. 358-365). IEEE.

Sang-Oun Lee is a graduate student at the University of Chicago Harris School of Public Policy and the Chief Information & Financial Officer at the EPIKAR Inc. Mr. Lee holds bachelor's degree in International Liberal Arts from Waseda University, Tokyo, Japan, and Masters of Science degree in Technology Management, Economics and Policy from Seoul National University, Seoul, Korea. Prior to start his graduate studies at the University of Chicago, Mr. Lee served Assistant Manager at the Korea Internet & Security Agency and The Attached Institute of ETRI for three years specializing in cybersecurity policy research and practice.

H.J. SEO received his PhD degree in computer engineering from the Yonsei University, Seoul, Korea. Currently, H.J. Seo is a project manager of future technology research center at the attached institute of ETRI-Electronic and Telecommunication Research Institute- where he is conducting research activities in the area of code analysis, false positive rate reduction, national level data analysis, and so on. H.J. Seo researched and developed virtual reality systems and decision making support systems for Korean governments and industries in Imaging Media Center of Korea Institute of Science and Technology. H.J. Seo worked for national technology strategy and policy in Korean Institute for Defense Analysis as a senior researcher and The Attached Institute of ETRI as a principal researcher since 1999.