Evaluating Cybersecurity Capacity Building of ASEAN Plus Three through Social Network Analysis

Yu-Kyung Kim[1], Myong-Hyun Go[2], Sonyong Kim[3], Jaeyeon Lee[3], Kyungho Lee[1]*

[1] School of Cybersecurity, Korea University, Republic of Korea
[2] The Asan Institute for Policy Studies, Republic of Korea
[3] Hanwha Systems, Republic of Korea
rladb1125@korea.ac.kr, mhgo@korea.ac.kr, sonyong.kim@hanwha.com, jaeyeon46.lee@hanwha.com, kevinlee@korea.ac.kr

Abstract

The strategic rivalry between the United States and China is out in full swing in Southeast Asia. As the result, ASEAN is emerging both as a key player as well as a playground for pivotal global and regional actors. South Korea, Japan, and China known as ASEAN Plus Three, have strong economic, political, and technological ties with the region, and have leveraged their cyber capabilities to compete for influence in the region. This study evaluates the relative performances of the Plus Three' cyber outreach efforts to the region by visualizing the complex web of actors and cyber cooperation and assistance activities with network analysis tools and open-source databases. We quantitatively analyze national cyber security cooperation of ASEAN including South Korea, Japan, and China through capacity building indicators and social network methodology. This study (1) analyzes cybersecurity cooperation in ASEAN Plus Three, (2) explores factors that influence cooperation, and (3) lays out a quantitative basis for establishing national information policy and cybersecurity strategy. We find that the Plus Three, despite the outward similarity in their respective regional strategies, are a study of contrasts, with one of them emerging as an influential yet silent power in the regional cyber diplomacy domain.

Keywords: ASEAN Plus Three, Cybersecurity, National information policy, Social network analysis

1 Introduction

The Association of Southeast Asian States (ASEAN) is emerging as a critical strategic bloc that stands at the confluence of China's expansive Digital Silk Road [1], its territorial ambitions in the South China Sea [2], and the United States' Indo-Pacific strategy that is set to counter both. The ASEAN and its wide-ranging Asia-Pacific community, recognized as a neutral organization, plays an important role in international cybersecurity cooperation in the context of United States-China strategic competition [3]. In other words, ASEAN and India are developing cooperative relationships with partner countries to meet internal demands for economic growth, security enhancement, and social development, while simultaneously responding to external factors such as confrontation and competition between the camps triggered by the US and China [4]. ASEAN member states are also becoming significant contributors to the global information and communication technology (ICT) supply chain and the rapidly growing export of ICT services [5]. Apart from its strategic importance, ASEAN stands on its own merits. The combined ASEAN population is approximately 659 million and its Gross Domestic Product (GDP) is expected to exceed US$ 4 trillion by 2022, thus making it the world's seventh-largest market. ASEAN's digital economy has the potential to add US$ 1 trillion more to the GDP over the next decade [6].

Cybersecurity has been an emerging and critical area for cooperation and assistance in the field of ASEAN member states but lags significantly behind other countries in terms of cyber capacity and readiness. ASEAN member states rank low in the cybersecurity rankings of the International Telecommunication Union (ITU)'s Global Cybersecurity Index and Estonia's National Cyber Security Index and there is uneven cyber development within the regional bloc. According to the Global Cyber Security Index 2020 [7], Singapore and South Korea ranked 4th out of the total countries with 98.52. Malaysia (98.06, 5th place), Japan (97.92, 7th place), Indonesia (94.88, 24th), Vietnam (94.59, 25th), and China (92.53, 33rd) followed. The remaining ASEAN member states did not score above 90, and Myanmar ranked 99th with a score of 36.41. The National Cyber Security Index shows similar intra-group inequality, with Singapore and Malaysia scoring more than 70, while the average for the rest of the states is estimated at around 28 [8]. In the backdrop of the rapidly rising demand for ICT technologies driven by economic development, population growth, and cross-border ICT connectivity susceptible to cyber threats [3], this capacity divide increases the vulnerabilities of ASEAN member states in cybersecurity.

Not only are superpowers such as the United States and China paying attention to ASEAN. The centrality of ASEAN in the foreign policy of relevant global actors has generated a plethora of cooperation and support initiatives as many countries compete for influence in the region. Among these initiatives, cybersecurity which involves cooperation, assistance, and cyber capacity building has become a critical dimension for improving ASEAN's cyber capacity. These initiatives also create opportunities for cooperation between ASEAN and

*Corresponding Author: Kyungho Lee; E-mail: kevinlee@korea.ac.kr

DOI: 10.53106/160792642023032402031

major global and regional actors. These connections help the ASEAN member states and allow major global and regional actors to promote trade opportunities and expand their influence in the region. There is a certain competitive element among the major actors jockeying for regional influence in Southeast Asia, which, in turn, can lead to the rapid expansion of assistance and cooperation.

This study focuses on three major actors: South Korea, Japan, and China. Unlike other major global actors, these three East Asian countries are formally connected to ASEAN through a regional expansion mechanism called the ASEAN Plus Three [9-10]. South Korea, Japan, and China's association and cooperation strategies with ASEAN include cyber diplomacy and security cooperation. The Plus Three also parlay their competitive advantages in ICT industries to advance foreign policy goals. In cyberspace, the geopolitical characteristics based on technological power best manifest themselves in complex security and foreign policy strategies. Here, the performance of the regional strategies of respective powers can be evaluated through the intertwined links of cooperation and assistance. Northeast Asia's Indo-Pacific strategy is a diplomatic strategy that uses networks to maximize the national interests of ASEAN members [4]. In the network, there are actors with centrality, and those who increase the value by filling the structural void in the network. Therefore, by analyzing the cybersecurity cooperation network of ASEAN members and ASEAN Plus Three, it is possible to establish a diplomatic strategy that can demonstrate value beyond national power. This study uses network analysis techniques to visualize and quantify the relative influences of the three Northeast Asian actors among the ASEAN member countries.

2 Literature Review

ASEAN was founded in 1967 as a regional community to respond jointly to communist militants in the Vietnam War and the Indochina Peninsula; it grew in response to rapid changes in international affairs [11]. This community aims to provide an environment for peaceful conflict management by encouraging constant interactions among members and building mutual trust to pursue common purposes [12]. The current member states of the ASEAN are Brunei, Cambodia, Indonesia, Laos, Malaysia, Myanmar, Philippines, Singapore, Thailand, and Vietnam. Although most of these ASEAN member states lack cybersecurity, this community actively promotes it through various policy discussions and strategic announcements.

The wide-ranging Asia-Pacific community is recognized as a neutral organization, with ASEAN playing an important role in international cybersecurity cooperation in the context of United States-China relations [3]. Furthermore, ASEAN members are the global hub for ICT hardware production and rapidly developing as exporters of ICT services [5]. Additionally, most ICT users are located in Asia, which is likely to increase the demand for ICT and its support services in these regions. Contrarily, improved cross-border connectivity of ICT and its services has increased the probability of cyber threats [3]. Consequently, ASEAN member states have become the main targets of cyberattacks [13]. Securing cyberspace, therefore, is becoming a fundamental prerequisite for ASEAN security and digital economies, which can be addressed by reviewing members' cybersecurity strategies and laws [13]. Nevertheless, the willingness to address cyber policy issues depends largely on the cyber maturity of Southeast Asian countries [14], within which cybersecurity strategies are planned and implemented. Because complex foreign policy relations and diplomatic cooperation among ASEAN member states echo the current competition for supremacy in cyberspace.

To understand how ASEAN member states cooperate in cyberspace, there is a need to analyze cyberspace cooperation in ASEAN. However, the literature has several shortcomings. Research in this field is limited due to the paucity of publicly available information on ASEAN's cyber policies. Additionally, it is difficult to analyze the cyber policy direction of independent ASEAN member states because these nations do not openly discuss their policies. Nonetheless, a few studies have compared and analyzed cyber policy strategies within regional organizations such as ASEAN and various cyber-agreement consultative bodies.

China diverges from its Northeast Asian neighbors in that it aims to replace existing cyber norms with a new China-centric order. The "Digital Silk Road", part of the grander infrastructure building program, the Belt and Road Initiative, is China's main conduit to Southeast Asia. China is also making active use of international forums and organizations dedicated to forming international standards for cybersecurity such as the Shanghai Cooperation Organization, ASEAN Regional Forum, and traditional international organizations like the United Nations Group of Governmental Experts, and ITU. In accordance with each country's national strategy, ASEAN emphasizes cooperation with practical benefits while maintaining ASEAN centrality.

2.1 Cybersecurity Strategies of ASEAN Plus Three

In recent years, the three Northeast Asian powerhouses, South Korea, Japan, and China years have been deepening their cooperation with ASEAN, particularly in the field of cyber diplomacy and security cooperation. Each of these three nations has formulated dedicated national strategies with strong ASEAN salience. They are South Korea's "New Southern Policy" and "Indo-Pacific Strategy of South Korea", Japan's "Free and Open Indo-Pacific strategy", and China's "Digital Silk Road strategy".

South Korea has been pushing to strengthen its cooperation with ASEAN through the New Southern Policy, which was officially announced in Indonesia in November 2017. Since the promulgation of the NSP in 2017 by President Moon, the policy has been used to strengthen relations with ASEAN in various fields such as people-to-people exchanges, economic exchanges, and diplomatic cooperation [15]. The NSP can be considered as South Korea's effort to strengthen its influence with Southeast Asia at a time when the strategic competition between the US and China is intensifying in the wider Indo-Pacific region. The trigger for this policy was China's economic retaliation toward South Korea's deployment of Terminal High Altitude Area Defense. To respond to this move, South Korea selected

10 ASEAN member states and India as economic partners for market diversification [4]. Additionally, President Yoon emphasized the role of cyber security by selecting cyber security as a national task in 2022.

Japan's ASEAN strategy lies within the framework of the Quadrilateral Security Dialogue the "Quad", composed of Australia, India, and the United States. To strengthen relations with ASEAN, the former Prime Minister Shinzo Abe initiated bilateral policy dialogues with ASEAN in February 2009. Japan is perhaps the most consistent player in cybersecurity among the Plus Three nations. It enacted the Basic Cybersecurity Act in 2014 and has been consistently pursuing international cooperation policies with ASEAN, the European Union, and the United States since then. In 2021, Japan specified the realization of Free and Open Indo-Pacific and comprehensively presented the possibility of multilateral cooperation with the United States, Australia, India, and ASEAN member states among others [16].

2.2 Assessing National Cybersecurity Capabilities

Evaluation of national cybersecurity capabilities is a precondition for cooperation in cyberspace. Unfortunately, the indices that measure cybersecurity capabilities are diverse and not integrated. Common evaluation metrics have never been formally discussed to assess the capabilities of cybersecurity. Pawlak et al. [17] proposed policy recommendations for cybersecurity capacity building by presenting conceptual underpinnings of cybersecurity capacity building. However, it is necessary to objectively grasp the current situation by analyzing the national cybersecurity capacity building construction relationship using quantitative cooperative activity data. Koulas et al. [18] analyzed the cybersecurity cooperation between "Cyber Emergency Response Team (CERT) and Cyber Security Incident Response Team (CSIRT)" through Webometric Network Analysis. However, it is difficult to evaluate national information policy, cybersecurity policy, and diplomatic partnerships based on the activities of CERT and CSIRT alone. Therefore, we aim to analyze quantitative cybersecurity cooperation to establish national cybersecurity policies and strategies.

Indicators for cybersecurity assessment are developed by international organizations or think tanks and evaluated through policies, organizations, national strategies, and cooperation. Some indicators are compared through measurements between countries, while others provide exponential scores based on the indicators. We present three indicators that evaluate global cybersecurity capabilities that are considered in this study.

The Global Cybersecurity Index (GCI) compiles information on the cybersecurity efforts of 193 ITU member states [7, 19]. Traditionally, GCI is evaluated through five elements: law, technology, organization, competency development, and cooperation. The GCI assessment method consists of 82 surveys including questions on each of the five weighted factors determined by an expert group [19]. The GCI, however, does not have data for all countries, as some have refused to participate in its online questionnaire survey. In other words, due to the limitation of data collection through the questionnaire, it could be interpreted as an additional online survey, which may have positively affected on the country's participation in the survey. However, the ASEAN Plus Three, the subjects of this study, actively participated in this survey.

Accordingly, it is necessary to refrain from obsessing over the rankings of GCI but to analyze the areas where a nation is doing well and where efforts need to be strengthened. In the 2020 GCI survey, the UK ranks second among the total countries with a score of 99.54. (1st place with a score of 0.931 in 2018 GCI) South Korea and Singapore ranked fourth with scores of 98.52. The global ranking of ASEAN Plus Three member states were: Malaysia (5th), Japan (7th), Indonesia (24th), Vietnam (25th), China (33rd), Thailand (44th), Philippines (61st), Brunei (85th), Myanmar (99th), Laos (131st), and Cambodia (132nd). Singapore's high ranking was possibly due to its strong cybersecurity capabilities as ASEAN's cybersecurity hub and Malaysia scored high due to its focus on strategic publications and legal frameworks. We compared the scores for each of the five elements of the GCI as illustrated on Figure 1. As this study focuses on cybersecurity cooperation, the cooperation areas among the five elements were also carefully considered. The areas of cooperation in the GCI were collected from countries that have signed bilateral and multilateral agreements, and those with inter-ministerial and public-private partnerships. In the field of cooperation, South Korea, Japan, Singapore, Malaysia, Indonesia, and Vietnam scored 20 out of 20, followed by the Philippines (19.41), China (18.91), and Thailand (17.34). The scores of the remaining countries did not exceed 10.

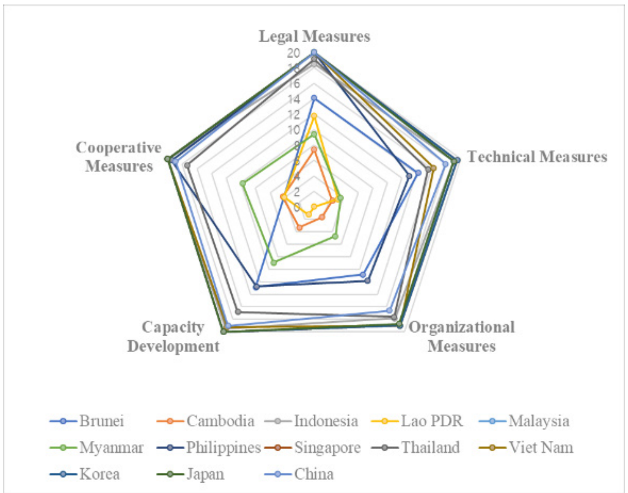


Figure 1. Comparison of GCI results for ASEAN Plus Three

This study also used data from the Global Forum on Cyber Expertise (GFCE) [20] and the United Nations Institute for Disarmament Research (UNIDIR) [21] cyber policy portal. Consisting of 102 members, 70 partners and 65 events, GFCE aims to strengthen the cyber capacity building ecosystem and international cooperation [20]. It combines various organizations to help coordinate their efforts to build the prerequisites to norms adoption, implementation, and accountability. The outcome of the 2015 GFCE meeting in the Hague initiated a platform for policymakers, practitioners, and experts [22]. The Cyber Knowledge Portal (Cybil), powered by GFCE, is a platform that provides knowledge on international cyber capacity building, first shared at the 2018 GFCE Annual Meeting in Singapore. Cybil's data consists of 823 projects, 797 actors, on a total regarding national cybersecurity cooperation, and comprises three types of content; projects; resources; and events. Moreover, Cybil is divided into five themes: cybersecurity policy and strategy; cyber incident management and protection of sensitive information; cybersecurity culture and technology; cybercrime; and cybersecurity standards. Figure 2 presents the thematic distribution of ASEAN members and the cyber capabilities of South Korea, Japan, and China through GFCE's Cybil data. Out of the 10 topics, most events are categorized in the "National Computer Security Incident Response" category out of the 10 topics, which suggests that the cybersecurity field is the most important in the national cyber domain.

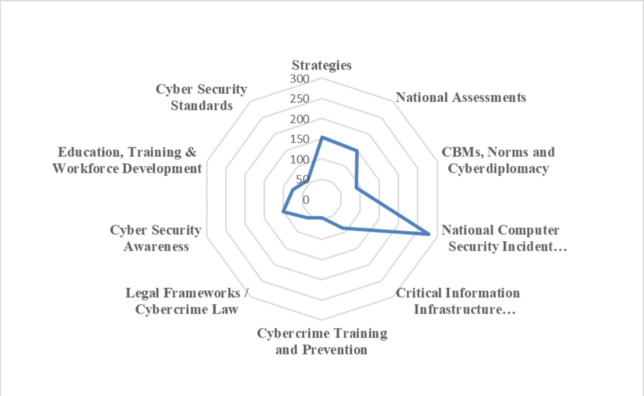


Figure 2. Distribution of topics of GFCE cybersecurity

The UNIDIR Cyber Policy Portal is an interactive map of the global cyber policy environment and is published by the United Nations Institute for Disarmament Research [21]. In addition to various intergovernmental, organizational, and multilateral frameworks, UNIDIR provides the cyber policy profiles of 193 UN member states. Data from the UNIDIR Cyber Policy Portal is collected and linked to publicly available online sources. The advantage of this portal is the high reliability of its information, as it consists of official documents distributed by national or intergovernmental organizations. Therefore, salient studies on cyber governance usually use the UNIDIR Cyber Policy Portal data. For example, Solar [23], examined military agencies dedicated to cybersecurity in emerging democracies such as Argentina, Brazil, Indonesia, Philippines, and Mexico using the UNIDIR data. Similarly, Gramaglia et al. [24] examined the organization and structure responsible for cyber defense in NATO member states based on the UNDIR data. They analyzed cyber commands, military Computer Emergency Response Team (CERT), and special cyber units through the national profile of UNIDIR in 28 NATO member states.

3 Cyber Capacity Building Activities Analysis

ASEAN Plus Three has long emphasized cooperative relations in cybersecurity. Nevertheless, given the loose, non-binding nature of ASEAN agreements and policies, there is much leeway with which ASEAN member states enter into bilateral and multilateral cyber agreement and assistance programs. For instance, the Philippines accepted US assistance to combat cyber terrorism in ASEAN [25], but Malaysia did not, on the grounds that it infringed upon its national sovereignty. Indonesia also refused US. assistance because other ASEAN member states pressured them to do so. Thus, ASEAN's cybersecurity efforts show a high degree of heterogeneity in terms of cooperation, agreement, and reaction to external influence. In contrast to the United States, China takes an approach that is more sensitive to the issue of sovereignty; it works with ASEAN on non-traditional security cooperation with a focus on national sovereignty that flexibly leads to various formal agreements [26]. This perspective embodies an approach to security that reflects the norms of authoritarian developmentalism.

ASEAN is also characterized by a wide range of levels of economic development that reflect the region's heterogeneity in terms of the development of the ICT sector [14]. In other words, ASEAN members' efforts regarding cyber policy issues are hampered by differing levels of cyber maturity. Countries with high cyber development, such as Singapore, tend to push for developments in norms adoption, capacity-building measures, and other cyber-policy aspects. In contrast, nations such as Myanmar are more focused on establishing protective measures for their national infrastructure [14]. Consequently, the direction of each member state's cybersecurity policy is associated with the maturity and complexity of its ICT sector, and the national strategies of each ASEAN member state. In turn, the level of maturity is associated with the degree of cybersecurity cooperation of each member state. This study used the visualization of cyber assistance and agreements through the social network analysis, to better infer the maturity and effectiveness of the Plus Three' ASEAN strategies in the cyber domain. It also identified the relationship among cybersecurity assistance, cooperation, and agreements to find the characteristics of the relationships of ASEAN member states with the Plus Three.

3.1 Method

This study is descriptive and provides an intuitive understanding of the state of affairs in the ASEAN cyberspace through the use of network analysis visualization assistance. To this end, it employed data from GFCE [20] and UNIDIR [21]. Our data source comprised various aspects of cyber cooperation, including policies, strategies, cybercrime, and infrastructure protection. However, we excluded cooperation on ICT development and development from the analysis on cybersecurity cooperation. We extracted 178 entries from the GFCE dataset with 824 (Receivers is one of ASEAN Plus Three) for the period from 1999 to 2022. We added 98 entries, information on international cybersecurity cooperation, from the latest UNIDIR data, providing a cyber policy profile of the Receiver. Additionally, this study framed its analysis on the latest cyber security strategy documents of ASEAN Plus Three member states and compared and analyzed their domestic and foreign cyber activities.

The network consists of two actors (Funder-Receiver country or two countries) and the connections they make. The Funder means the donor country and the Receiver means the recipient country in this study. The cybersecurity cooperation network in this study comprises 48 countries or institutions that are actors in the network and are referred to as "nodes," and the number of exchanged cybersecurity cooperative events between these nodes is referred to as "links". The information about this connection network is constituted in the form of a matrix, where each row or column represents each actor, and information on the connection from row to column is stored. The arrow representing the link indicates a cybersecurity cooperation event between the Funder and the Receiver countries, and the thickness of the link denotes the number of cybersecurity cooperation events that have occurred between the Funder and Receiver countries. In the Assistance relationship, the distinction between Funder and Receiver countries is clear, but Cooperation and Agreement do not distinguish between Funder and Receiver countries.

The collected data sets were divided into bilateral and multilateral assistance, cooperation, and agreements. Bilateralism and multilateralism are concepts derived from a liberal perspective that presupposes cooperation between state actors [27]. In Europe, the formation of a collective security identity is the main security strategy, but the Northeast Asian countries and ASEAN Plus Three must also consider the aspects of bilateralism according to their regional characteristics. Bilateralism was used as the core logic of the Northeast Asian security structure based on its high effectiveness in terms of traditional security. However, as cyberspace is a virtual space and not a physical one, cooperation should be analyzed in terms of bilateral and multilateralism.

Based on the data compiled from information in GFCE and UNIDIR, we could visualize cybersecurity assistance, cooperation, and agreement relationships using social network analysis techniques. Social network analysis is a powerful technique used to model social structure [28]. In particular, the concept of structure as a relational construct presented by social network analysis helped us understand the structure of international relations in cyberspace. The analyses and graphs in this study were made using Polinode [29] and UCINET [30], social network analysis software.

We used representative social network metrics such as "Total Degree" ("In Degree" and "Out Degree") and "Density" to quantify support, collaboration, and contractual relationships, and focused on the concept of centrality. The results of the data analysis reveal the relationship between the principal and Receiver countries' assistance or cooperation initiatives by each country (a "node" in network terminology). Therefore, given the reciprocal nature of each country's cybersecurity cooperation, the relationship was measured in statistics. A node is a national actor or, in some cases, an international organization, whose size indicates importance as a particular node in the network, replaced by the size of the Total Degree. The Total Degree for a node is the total number of edges that that node has; for directed networks, it is the sum of In Degree and Out Degree [2]. The width of a link between nodes is the width of a link between two given countries. This link means the frequency of cybersecurity-related agreements or outreach activities that occur.

The most salient indicator in this study was the centrality of states in the complex web of cyber policy relations. Centrality in a network is an indicator that can be used to analyze which country plays a central role in the entire network. Therefore, centrality refers to the occupied central position of a network [31]. A node occupying a central position in the network would have a stronger influence on relations with other neighboring nodes. We examined the centrality of Funder and Receiver countries in the field of cybersecurity cooperation by calculating degree centrality, betweenness centrality, and closeness centrality. Further, this allowed us to examine the level of influence of Funder and Receiver countries as the level of influence directly corresponds to how central a country is in its relationship network of assistance, cooperation, and agreement. The most direct of these network centralities was degree centrality, which was calculated as the sum of connections owned by a node. The centrality analysis in this study only considered the direction of assistance in which cooperation between countries was unilateral and did not incorporate the direction of cooperation and agreement in which the cooperation between countries was mutually performed.

$$D = \frac{L}{g(g-1)/2}. \tag{1}$$

D: *Density*, *L*: *The number of existing ties*, *g*: *The number of existing nodes*.

Density represents the overall level of connectivity between nodes in a network. The more connections between nodes within the network, the higher the density. The density of a network can thus be measured by the number of links in the network; the greater the number of links, the higher the density of the network.

$$C_D(N_i) = \sum_{j=1}^{g} x_{ij},\ i \neq j. \tag{2}$$

$C_D(N_i)$: *Node i's degree centrality*, g: *The number of existing nodes*,

$\sum_{j=1}^{g} x_{ij}$: *Number of connections that node i has with other nodes of* $(g–1)$,

$x_{ij} = 0$ *or* 1.

Degree centrality determines that the node is at the center of the network as the number of connections between the node and other nodes increases. Accordingly, it was used as an index to evaluate the activity of the node [32]. The closer to 1 of Degree centrality, the higher the activity and the higher of times other nodes in the network pass through the node.

$$C_C(N_i) = \frac{1}{\sum_{j=1}^{g} d(N_i, N_j)},\ i \neq j. \tag{3}$$

$C_C(N_i)$: Node i's closeness centrality, g: The number of existing nodes,

$\sum_{j=1}^{g} d(N_i, N_j)$: The sum of the shortest path distances between node i and node j.

Closeness centrality is a concept that denotes how close a node is to others. Accordingly, it was measured using the sum of all the shortest paths with other nodes. As degree centrality considers only the connection relationship of adjacent nodes, it does not include the indirect connection relationship [33]. Judging only by degree centrality, the actual center may be in the periphery instead of the center of the entire network. Accordingly, it is necessary to identify the node located at the center of the entire network through proximity centrality. While degree centrality emphasizes the actor's activity, proximity centrality accentuates the actor's independence [31].

$$C_B(N_i) \sum_{j<k} \frac{g_{jk}(N_i)}{g_{jk}},\ i \neq j \neq k. \tag{4}$$

$C_B(N_i)$: Node i's betweenness centrality, g_{jk}: The number of shortest paths between two nodes i and k.
$g_{jk}(N_i)$: The number of paths containing node i among the shortest paths between two nodes i and k.

Between centrality is not a numerical value based on a simple distance such as connection centrality but a concept in which a node existing between two nodes based on the shortest distance plays the role of a communicator, and a node with a strong communicator role is judged as the center of the network [34]. A node with high mediation centrality can be interpreted as having a high linking degree between organizations in cybersecurity cooperation, and it has a mediating role between organizations.

4 Results

4.1 Assistance Relationship of Cybersecurity

Figure 3 illustrates the assistance relationship of cybersecurity between Funders (Blue square nodes) and Receivers (Red circular nodes) among ASEAN Plus Three, including South Korea, Japan, and China. The largest Funder of assistance is the UK, and the largest Receivers are Singapore, Malaysia, and Brunei. Singapore, as a Funder, has the largest influence in the assistance relationship of cybersecurity, followed by Japan and South Korea. In other words, among ASEAN members, Singapore has a significant influence as a funder country. The remaining ASEAN members have a similar level of influence as Receiver countries of cybersecurity assistance. Among Northeast Asian countries, Japan is the largest Funder, followed by South Korea and China. Japan is a Funder node not only in the Japanese state, but also in the Japan-ASEAN Integration Fund (JAIF) institution, which suggests that the influence of Japan's cybersecurity assistance to South Korea, China, and Japan is very large.

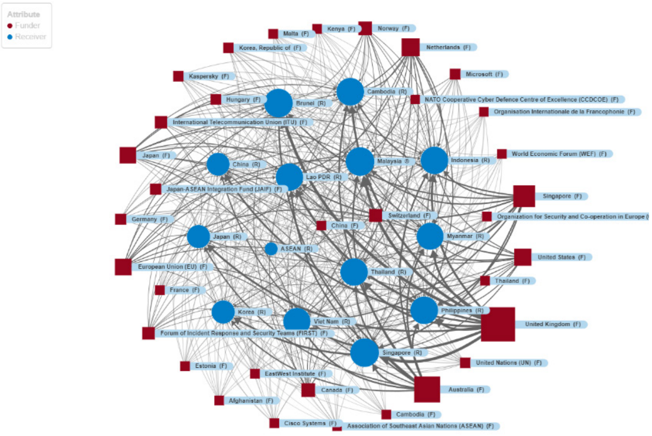


Figure 3. Assistance relationship of cybersecurity

Organizations with high proximity centrality within the entire network are located at the center of assistance relationships among cybersecurity cooperation networks and are in a position where they can easily form cooperation with other organizations in the network. Comparing the centrality of Funder countries, as can be seen in Appendix A, the ASEAN Plus Three countries that show the highest connected centrality are Japan, South Korea, and Singapore, with a connected centrality value of 0.929. When looking at the number of mediation centrality, Japan, South Korea, and Singapore reveal the highest values, similar to the connected centrality. Thus, it can be concluded that Japan, South Korea, and Singapore, with the highest mediation centrality, play a mediating role between organizations that are actors in cybersecurity cooperation. Similarly, Japan, South Korea, and Singapore show the highest figures for proximity centrality. Japan, South Korea, and Singapore are central to assistance relations among cybersecurity cooperation networks and indicate high activity and influence.

Thus, when analyzing the degree of connectivity and centrality, Japan exerts the highest influence in terms of cybersecurity cooperation in ASEAN Plus Three. Although South Korea is not a strong cooperative Funder like Japan, it has the second strongest influence after Japan among ASEAN Plus Three. Among ASEAN member states, Singapore is also considered to be actively engaged in cybersecurity cooperation in both the Funder and Receiver aspects. However, the conclusion that Japan is the most central player in providing assistance and, thus, gaining influence over ASEAN member states should be qualified by the fact that China also has umbrella bilateral discussions with ASEAN member states that are not limited to non-monetary cooperation. Often, China's assistance agreements are operationalized through military agreements, where cybersecurity may be a sub-section. When it comes to norm building, China prefers multilateral cybersecurity discussions with regional cooperation organizations such as the Shanghai Cooperation Organization (SCO) and ASEAN Regional Forum (ARF), in addition to working within the framework of international organizations such as the United Nations GGE and ITU [35]. China's influence in the region is prominent but difficult to quantify. Thus, the result of the assistance analysis should be considered in light of the limitation inherent in the dataset used in the study.

4.2 Cybersecurity Cooperation Relationships

This section analyzes the cyber security cooperation between ASEAN Plus Three. Figure 4 and Figure 5 present cybersecurity cooperation between ASEAN Plus Three but with different network layout algorithms. Figure 4 simulates the physical force of the network through the "Force Directed" algorithm, and Figure 5 is based on the layer in an optimal way through the "Hierarchical" algorithm. By identifying the location of each country based on the hierarchy, it is possible to identify the cybersecurity cooperation of similar roles and levels. Figure 4 and Figure 5 suggest that South Korea, Japan, and China actively engage in cybersecurity exchanges and cooperation on bilateral or multilateral relations almost indiscriminately. Similarly, Table 1 presents ASEAN members with a similar degree of connection, and Northeast Asian countries reveal a similar indiscriminate degree of connection. However, when the density is checked, a result different from the degree of connection is derived. Density values are high for Northeast Asian countries. This means that Northeast Asia has more links in cybersecurity cooperation with ASEAN member states than ASEAN members do and that the influence of these links is strong.

When analyzing the cooperative relationship in terms of centrality, the values of mediation centrality and proximity centrality are the same, except for ASEAN cooperatives. However, in the centrality of connection, Malaysia has the highest number, followed by the Philippines, Indonesia, Singapore, Thailand, Brunei, Laos, Cambodia, Vietnam, and Myanmar. Malaysia is thus the most active in terms of assistance in cybersecurity cooperation. A noticeable cluster composed of Vietnam, Myanmar, Cambodia, and Laos is also emerging from the cornucopia of cooperation relations. It is probably a reflection of the more active cooperation formalized through the informal country grouping of Cambodia-Laos-Myanmar-Vietnam (CLMV) group [36].

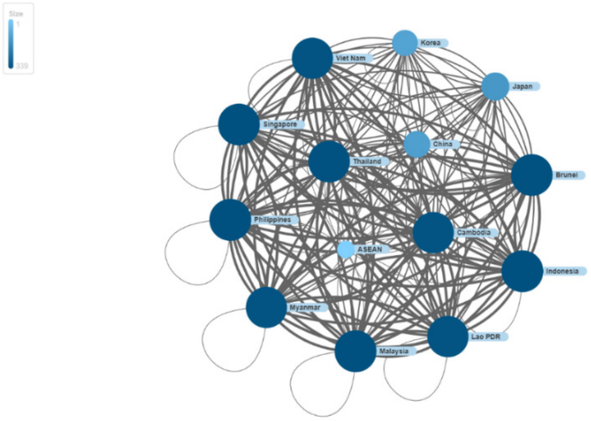


Figure 4. Cooperation relationships of cybersecurity (Force-Directed analysis)

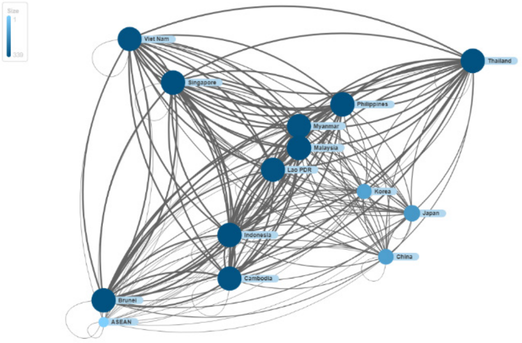


Figure 5. Cooperation relationships of cybersecurity (Hierarchical analysis)

Table 1. Centrality index of nodes in the cooperation and the agreement relationships of cybersecurity

	Cooperation			Agreement		
	Degree centrality	Closeness centrality	Betweenness centrality	Degree centrality	Closeness centrality	Betweenness centrality
Brunei	0.738	0.500	0.000	0.000	0.071	0.000
Cambodia	0.725	0.500	0.000	0.077	0.143	0.000
Indonesia	0.743	0.500	0.000	0.000	0.071	0.000
Lao PDR	0.725	0.500	0.000	0.231	0.169	19.231
Malaysia	0.745	0.500	0.000	0.154	0.153	10.256
Myanmar	0.723	0.500	0.000	0.000	0.071	0.000
Philippines	0.743	0.500	0.000	0.154	0.165	17.949
Singapore	0.741	0.500	0.000	0.154	0.167	5.128
Thailand	0.738	0.500	0.000	0.154	0.165	3.846
Viet Nam	0.723	0.500	0.000	0.154	0.171	15.385
ASEAN	0.000	0.071	0.000	0.000	0.171	0.000
Korea	0.262	0.500	0.000	0.077	0.140	0.000
Japan	0.327	0.500	0.000	0.231	0.173	24.359
China	0.286	0.500	0.000	0.154	0.157	10.256

4.3 Agreement Relationship of Cybersecurity

Cybersecurity agreement strongly reflects the reality of cyberspace instead of assistance or cooperation. Many national governments have cooperated informally by sharing cyber threat intelligence, investigating attacks or crimes, preventing or stopping harmful conduct, providing evidence, and arranging for the rendition of individuals to a requesting state [37]. However, cybersecurity agreements are indicative of long-term cooperation and partnership and provide a useful foundation for continued cooperation in the future. We examined the cybersecurity agreements of ASEAN member states. The cybersecurity agreements describe specific commitments that apply to the signatory state. They have a stated goal to improve cybersecurity capability and can be multilateral.

Figure 6 and Figure 7 present the relationship between ASEAN Plus Three represented by cybersecurity agreements. According to Table 1, Japan shows a strong centrality of the network. Unlike previous studies [38], South Korea reveals low centrality among countries in Northeast Asia. This could be because previous studies had considered the relationship between ICT development and cooperation. In this study, more accurate results are derived by analyzing only agreements related to cybersecurity. Contrary to expectations among ASEAN members, Laos has the highest level of connection and centrality of connection.

Laos has signed cybersecurity agreements with China, Vietnam, and Thailand, and thus, shows the thickest link. Accordingly, Laos can be regarded as the most active country among ASEAN member states in the treaty relationship.

Assistance relations have the highest density (0.885) among assistance, cooperation, and agreement relations of cybersecurity, as illustrated in Table 2. Although there is a slight difference, cooperation relations also indicate a high density (0.857), and the mutuals (0.857) show the highest value. However, in an agreement relationship, the density (0.110) is very low, and the mutuals (0.110) are also low. Therefore, the national relationship in cybersecurity favors a form of assistance or cooperation.

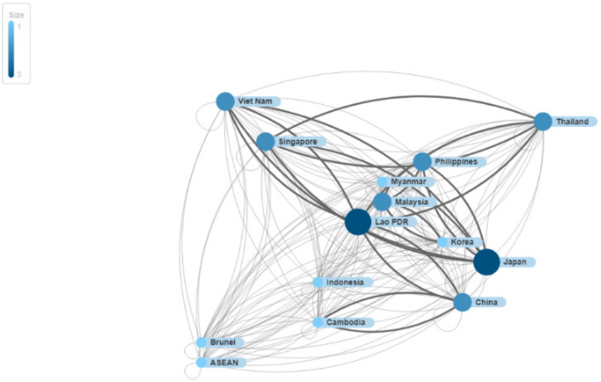


Figure 6. Agreement relationship of cybersecurity (Force-Directed analysis)

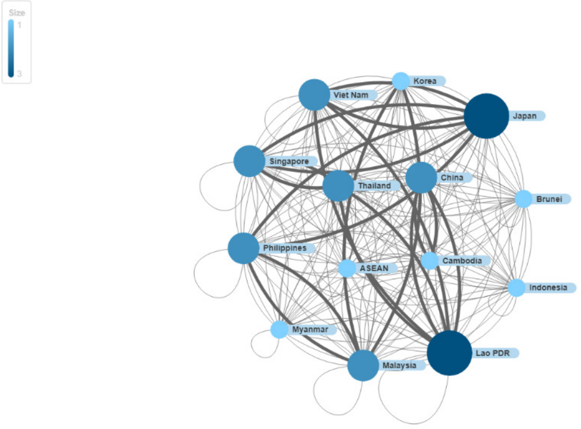


Figure 7. Agreement relationship of cybersecurity (Hierarchical analysis)

Table 2. Metrics comparison for assistance, cooperation, and agreement relations of cybersecurity

Relationship	Number of ties	Average degree	Degree centralization	Out-dree centralization	In-dree centralization	Density	Average distance	Mutuals
Assistance	161	11.500	0.000	0.124	0.124	0.885	1.047	0.769
Cooperaton	156	11.143	0.077	0.071	0.071	0.857	1.000	0.857
Agreement	20	1.429	0.141	0.130	0.130	0.110	2.844	0.110

4.4 Discussion

Qualitative examination shows that Japan is indeed a more consistent actor in this domain, as well as the network statistics show that Japan is more influential than ASEAN Plus Three in terms of cyber cooperation. The ASEAN-Japan Information Security Policy meeting held in 2009 helped promote the awareness of social and economic importance of securing the cyberspace. Our analysis shows that Singapore is the leader in terms of ASEAN's cybersecurity cooperation. In Singapore's cybersecurity assistance relationship, Malaysia's cybersecurity cooperation relationship, and Laos' cybersecurity agreement relationship, Thailand showed a remarkable degree and centrality within the regional group. Singapore, Malaysia, and Brunei have been active in terms of cybersecurity agreements as beneficiaries. However, other ASEAN member states, such as Myanmar, showed a relatively low level of interest in the diplomatic engagement of the plus Three. As a country with high cybersecurity capabilities, as it is ranked 4th in the GCI, Singapore, by definition, promotes many activities such as declarations, conferences, and policy discussions. The preponderance of Singapore in the cooperative and diplomatic activities with ASEAN member states and Plus Three means that unless other members dispute its leading role, the directions of the cybersecurity strategies of ASEAN will be quietly but effectively shaped by Singapore's guiding hand.

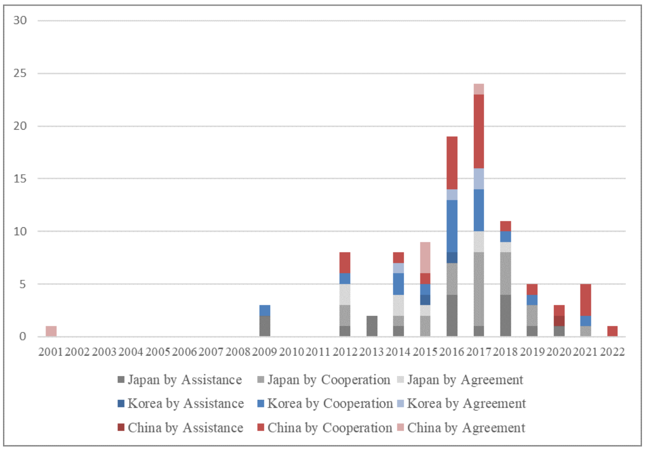


Figure 8. Assistance, cooperation, and agreement relationship of cybersecurity by Northeast Asia

We relied on the ITU's GCI 2020 report to identify potential relationships between cyber cooperation and cybersecurity functions. GCI calculates a cybersecurity competency score based on a survey of cybersecurity projects and policies. Therefore, the numbers in the GCI indicate competence and readiness but not necessarily technical competence. Our study demonstrates that high competence in cybersecurity is correlated with a high level of international cooperation. According to ITU's GCI 2020 [7], South Korea and Singapore ranked 4th with 98.52. Malaysia ranked 5th with 98.1, Japan 7th with 97.9, Indonesia 24th with 94.9, Vietnam 25th with 94.6, China 33rd with 92.5, and Thailand 44th with 86.5. According to our analysis, these are all countries with active cyber cooperation. Furthermore, based on our results, China has a strong network in the field of cybersecurity cooperation when the scope is limited to ASEAN. Given the descriptive scope of the study, we were not able to establish a clear causal relationship between capability and cooperation, that is, whether capability leads to cooperation or vice-versa. This question should be addressed in follow up studies.

Qualitative examination shows that Japan is indeed a more consistent actor in this domain, as well as the network statistics show that Japan is more influential than ASEAN Plus Three in terms of cyber cooperation. The ASEAN-Japan Information Security Policy meeting held in 2009 helped promote the awareness of social and economic importance of securing the cyberspace. In 2013, the 40th year of ASEAN-Japan Friendship and Cooperation for the ASEAN-Japan Ministerial Policy focused on the Cybersecurity Cooperation [39]. In 2006, Japanese Prime Minister Junichiro Koizumi pledged the JAIF [40]. Since then, the ASEAN-Japan Cybersecurity Capacity Building Centre (AJCCBC) was established in Thailand. Japan has utilized existing channels such as the International Criminal Police Organization (ICPO - INTERPOL), G8 24/7 Network, and the electronic ASEANAPOL Database System (e-ADS) to counteract cyber-attacks.

Although South Korea, Japan, and China seem to be equally influential by looking at the relationship graphs, a deeper look reveals that three have had differing degrees of effectiveness with their approaches. In particular, Japan shines for its policy consistency. Figure 8 shows the instances of cyber assistance and agreements signed over the last two decades, revealing that in contrast to South Korea, which mostly focused on signing agreements, Japan consistently extended cybersecurity assistance to ASEAN member states. South Korea ranked 4th among the total countries in the GCI study, making headlines in terms of cybersecurity cooperation. suggest that it was driven by for example, South Korea has established "Korea's Indo-Pacific Strategy" as a way to build a regional cooperative network, and this strategy can be interpreted as not focusing on diplomatic relations with ASEAN, but to broaden contact with the United States. As China becomes more active in cyber cooperation and assistance, it suggests that new priorities related to the Digital Silk Road lie behind the growing number of cooperative activities with ASEAN. Although the rather low level of Chinese activities in the cyber domain could be due to China's preference for umbrella agreements with ASEAN instead of deal directly with the member states. Nevertheless, one cannot discount the possibility that China's low influence level could also be attributed to the polarized views of ASEAN member states on the ongoing spat over maritime borders in the South China Sea.

Starting with the initiation of bilateral policy dialogues with ASEAN in February 2009, bilateral cooperation has been strengthened through continuous information security policy meetings. Japan is building a cybersecurity system led by Japan, and through bilateral cybercrime dialogue, information sharing for the purpose of combating cybercrime, international cooperation, and strengthening response capacity, along with information sharing through the ASEAN-Japan Cooperation Fund (Japan ASEAN Integration Fund) providing financial support for ASEAN. Japan's other cyber assistance commitments to ASEAN are ASEAN Cyber Capacity Development Projects and ASEAN Joint Operations Against Cybercrime.

5 Conclusion

Our study has identified key players in the ASEAN cyber diplomacy domain and evaluated their strategic approaches. The study's findings and implications are more relevant than ever, as Southeast Asia and its maritime environs are deeply affected by the U.S.-China strategic competition. For China, the biggest challenge against extending its influence in the region is probably its polarizing image as a revisionist power. For instance, China maintains comprehensive military and security relations with Thailand, and relations with Malaysia have been upgraded to a comprehensive partnership. But Indonesia regards China as a potential adversary and Singapore openly calls for U.S. intervention to check China's rise. In other words, China's mixed records in its relations with ASEAN also extends to the cyber cooperation and agreements. South Korea and Japan, two key U.S. allies in the region and tied to the ASEAN institution along with China through the Plus Three mechanism, have a pivotal role in shaping regional dynamics through diplomatic outreach in which cyber cooperation and assistance figure prominently.

While seemingly similar in strategic outlooks, our studies find that South Korea and Japan are a study of contrasts. This study finds that Japan is the most successful player that can exert a considerable influence on ASEAN member states through its extensive and consistent cyber assistance and cooperation policies. In combination with its long track record of investments and involvement in the region, it can be assistance Japan is the silent power that is the most influential state actor in ASEAN's cyber domain. But it remains to be seen whether Japan's active stance on cyber assistance and cooperation with ASEAN can bear more tangible fruits for Japan's Free and Open Indo-Pacific strategy, which calls for a more active deterrence posture against China that many ASEAN member states, despite their shared misgivings about the rising hegemon, may not agree with.

Acknowledgement

This study was supported by a grant-in-aid from HANWHA SYSTEMS.

References

[1] L. Zhou, *Let's build a digital silk road: Xi Jinping looks to cement China's ties with Asean*, South China Morning Post 27, November, 2020.

[2] S. Wasserman, K. Faust, *Social Network Analysis: Methods and Applications*, Cambridge, United Kingdom: Cambridge University Press, 1994.

[3] C. H. Heinl, Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime, *Asia policy*, No. 18, pp. 131-160, July, 2014.

[4] Y. Choi, *The task of the Yun Seok-Yeol government's foreign policy: New Southern Policy as 'Korea's Indo-Pacific Strategy'*, Vol. 22, No. 349, April, 2022. https://www.sejong.org/web/boad/1/egofiledn.php?conf_seq=2&bd_seq=6435&file_seq=18005

[5] K. M. Vu, ICT diffusion and production in ASEAN countries: Patterns, performance, and policy directions, *Telecommunications Policy*, Vol. 41, No. 10, pp. 962-977, November, 2017.

[6] INTERPOL, *Interpol Report Highlights Key Cyberthreats in Southeast Asia*, February, 2020. https://www.interpol.int/News-and-Events/News/2020/INTERPOL-report-highlights-key-cyberthreats-in-Southeast-Asia

[7] ITU, *Global Cybersecurity Index 2018*, June, 2019. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

[8] National Cyber Security Agency (NACSA), Federal Government Administrative Centre, Malaysia, *Malaysia Cyber Security Strategy 2020-2024*, October, 2017. https://asset.mkn.gov.my/web/wp-content/uploads/sites/3/2019/08/MalaysiaCyberSecurityStrategy2020-2024Compressed.pdf

[9] R. Stubbs, ASEAN plus three: emerging East Asian regionalism? *Asian Survey*, Vol. 42, No. 3, pp. 440-455, May/June, 2002.

[10] ASEAN+3, *History*, The ASEAN Secretariat, March, 2023. https://aseanplusthree.asean.org/about-apt/history/

[11] S. R. Park, *Cybersecurity international cooperation status in ASEAN*, KISA Report, Vol. 9, November, 2019. https://www.kisa.or.kr/20302/form?postSeq=364&page=1#fnPostAttachDownload

[12] K. Mahbubani, R. Severino, *ASEAN: The Way Forward*, Mckinsey & Comapany, May, 2014. https://www.mckinsey.com/industries/public-and-social-sector/our-insights/asean-the-way-forward

[13] J. Sunkpho, S. Ramjan, C. Ottamakorn, Cybersecurity policy in ASEAN countries, *Information Institute Conferences*, Las Vegas, NV, USA, 2018, pp. 1-7.

[14] C. T. Dai, M. A. Gomez, Challenges and opportunities for cyber norms in ASEAN, *Journal of Cyber Policy*, Vol. 3, No. 2, pp. 217-235, June, 2018.

[15] Y. A. Oh, Korea's New Southern Policy: Progress, Problems, and Prospects, *Asia Pacific Bulletin*, pp. 1-2, July, 2020.

[16] I. Misumi, The background of enactment and amendment of the Basic Act on Cybersecurity, *Japan Society of Security Management*, Vol. 34, No. 1, pp. 28-34, August, 2020.

[17] P. Pawlak, P.-N. Barmpaliou, Politics of cybersecurity capacity building: conundrum and opportunity, *Journal of Cyber Policy*, Vol. 2, No. 1, pp. 123-144, March, 2017.

[18] E. Koulas, S. I. H. Shah, V. Peristeras, Webometric Network Analysis of Cybersecurity Cooperation, in: K. Arai (Eds.), *Intelligent Computing: Proceedings of the 2022 Computing Conference*, Springer, Cham, 2022, pp. 103-122.

[19] ITU, *Global Cybersecurity Index 2020*, D-STR-GCI.01-2021, June, 2022. https://www.itu.int/epublications/publication/D-STR-GCI.01-2021-HTM-E

[20] The Global Forum on Cyber Expertise (GFCE), Delhi Communique on a GFCE Global Agenda for Cyber Capacity Building, *the Global Conference on Cyberspace 2017*, New Delhi, India, 2017, pp. 1-4. https://thegfce.org/wp-content/uploads/2020/04/DelhiCommunique.pdf

[21] UNIDIR, *Cyber Policy Portal*, March, 2023. https://unidir.org/cpp/en

[22] C. Slack, Wired yet disconnected: the governance of international cyber relations, *Global Policy*, Vol. 7, No. 1, pp. 69-78, February, 2016.

[23] C. Solar, Cybersecurity and cyber defence in the emerging democracies, *Journal of Cyber Policy*, Vol. 5, No. 3, pp. 392-412, November, 2020.

[24] M. Gramaglia, E. Tuohy, P. Pernik, *Military Cyber Defense Structures of NATO Members: An Overview*, Background Paper, Tallinn, Estonia: International Centre for Defence and Security (RKK/ICDS), December, 2013.

[25] J. T. Chow, ASEAN counterterrorism cooperation since 9/11, *Asian Survey*, Vol. 45, No. 2, pp. 302-321, March/

April, 2005.

[26] D. Arase, Non-traditional security in China-ASEAN cooperation: The institutionalization of regional security cooperation and the evolution of East Asian regionalism, *Asian Survey*, Vol. 50, No. 4, pp. 808-833, July/August, 2010.

[27] C. Hemmer, P. J. Katzenstein, Why is there no NATO in Asia? Collective identity, regionalism, and the origins of multilateralism, *International organization*, Vol. 56, No. 3, pp. 575-607, Summer, 2002.

[28] J. Scott, What is social network analysis? *Bloomsbury Academic*, 2012.

[29] A. Pitts, Polinode: A web application for the collection and analysis of network data, *2016 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)*, San Francisco, CA, USA, 2016, pp. 1422-1425.

[30] J. D. Johnson, UCINET: a software tool for network analysis, *Communication Education*, Vol. 36, No. 1, pp. 92-94, 1987.

[31] K.-Y. Kwak, *Social Network Analysis*, Seoul, Republic of Korea: Chungram, 2014.

[32] L. C. Freeman, *Centrality in social networks: Conceptual clarification*, Social network: critical concepts in sociology, Londres: Routledge, 2002.

[33] M. A. Beauchamp, An improved index of centrality, *Behavioral science*, Vol. 10, No. 2, pp. 161-163, 1965.

[34] M.-J. Lee, J. Lee, J. Y. Park, R. H. Choi, C.-W. Chung, Qube: a quick algorithm for updating betweenness centrality, *Proceedings of the 21st international conference on World Wide Web*, Lyon, France, 2012, pp. 351-360.

[35] S. Kim, Cybersecurity strategies of major powers in world politics: from the comparative perspective of national strategies, *Journal of International and Area Studies*, Vol. 26, No. 3, pp. 67-108, September, 2017.

[36] ASEAN, *Joint Media Statement of the Tenth CLMV Economic Ministers' Meeting*, August, 2018. https://asean.org/speechandstatement/joint-media-statement-of-the-tenth-clmv-economic-ministers-meeting/

[37] A. Sofaer, D. Clark, W. Diffie, Cyber security and international agreements, in: *proceedings of a workshop on deterring cyberattacks*, Washington, D.C.: National Academies Press, 2010, pp. 179-206.

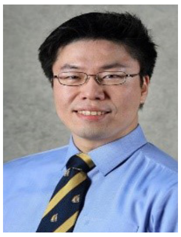
[38] Y.-K. Kim, M.-H. Go, K. Lee, Influence Through Cyber Capacity Building: Network Analysis of Assistance, Cooperation, and Agreements Among ASEAN Plus Three Countries, *WISA 2022: Information Security Applications*, Jeju, Republic of korea, 2022, pp. 330-343.

[39] ASEAN, *Joint Ministerial Statement of the ASEAN-Japan Ministerial Policy Meeting on Cybersecurity Cooperation,* ASEAN, September, 2013. https://asean.org/joint-ministerial-statement-of-the-asean-japan-ministerial-policy-meeting-on-cybersecurity-cooperation/

[40] JAIF, *Overview Purposes of JAIF*, March, 2023. https://jaif.asean.org/overview/

Biographies

Yu-Kyung Kim is a Ph.D. candidate in the Department of Information Security at Korea University. She received a bachelor's degree in law from Sookmyung Women's University in 2017. From 2017 to 2019, she served in the military as a military police officer.



Myong-Hyun Go is a research fellow at the Asan Institute for Policy Studies. Dr. Go received his Ph.D. in policy analysis from the Pardee RAND Graduate School. His research applies quantitative perspectives to traditional and non-traditional security issues.

Sonyong Kim received a B.S. degree in Electrical Engineering from the Korea University, Republic of Korea, in 2019. He has been with Hanwha Systems since 2019, and is currently a Junior Engineer with the Cyber Battlefield Team.

Jaeyeon Lee received a B.S. degree in Information Communication Engineering from the Catholic University of Korea in 2002. She received her M.S. degree in Information Communication Engineering from Gwangju Institute of Science and Tech in 2004. She has been with Hanwha Systems since 2004, in military information and communication.

Kyungho Lee received his Ph.D. degree from Korea University. He is currently a professor in the Graduate School of Cybersecurity at Korea University, and has been leading the risk management laboratory in Korea University since 2012. He was a CIO, CISO, CPO at Korea University.