# Comparative Analysis of National Cyber Security Strategies using Topic Modelling

Minkyoung Song, Dong Hee Kim, Sunha Bae, So-Jeong Kim
National Security Research Institute, Daejeon, South Korea

***Abstract*—Comprehensive comparative analyses of national cyber security strategies (NCSSs) have thus far been limited or complicated by the unique nature of cybersecurity, which combines various areas such as technology, industry, economy, and defense in a complex manner. This study aims to characterize the NCSSs of major countries, quantitatively considering the time series, and identify further cybersecurity agendas for the benefit of NCSS revision in South Korea, by applying topic modelling to the analysis of eight NCSSs from the US, UK, Japan, and EU. As a result, fifteen agendas were identified and grouped into four sectors. We determined from the agenda distribution that the approach of each country to cybersecurity was different. In addition, additional agendas worthy of consideration for future NCSS revisions in South Korea were proposed, based on a comparison of the 15 aforementioned agendas with those of South Korea. This study is significant for cybersecurity policy in terms of enabling quantitative analysis in a single framework via latent dirichlet allocation (LDA) topic modelling, and deriving further cybersecurity agendas for future NCSS revisions in South Korea.**

***Keywords—Cybersecurity policy; national cyber security strategy (NCSS); policy analysis; quantitative analysis***

## I. Introduction

Even in the midst of the COVID-19 pandemic, many of us were able to maintain our daily lives and national activities through the use of cyberspace. Cyberspace has become a new existential dimension for individuals and society to access the world via the transcendence of the physical limits of time and space. However, as dependence on cyberspace increased through digitalisation across the world, cyber threats have also become more diverse, complex, and menacing. Furthermore, malicious cyber activities on critical infrastructure such as electrical utilities, banking systems, and telecommunications networks could threaten the national security of almost any country. Therefore, at least 100 countries have established national strategies to secure their cyberspace.

A national cybersecurity strategy (NCSS) is one of the most concise documents for understanding the national approach to securing cyberspace. Analysing NCSSs is essential for determining the response stances at a national level and for understanding international cybersecurity trends. However, NCSSs endogenously include multidimensional agendas such as technology, industry, economy, and defence, which make it difficult to perform consistent and systematic analysis of NCSSs and to discover which agenda should be addressed in the development or revision of an NCSS. Meanwhile, text analysis has emerged as a new method for the analysis of large amounts of descriptive data, such as in NCSSs. Text analysis is useful for enabling empirical and quantitative analysis of descriptive data by identifying the keywords of documents and understanding content from relationships between words. Recently, even though text analysis has begun to be introduced into the analysis of NCSSs, there is still room for improvement, such as through the inclusion of time series in the analysis, which can lead to further agendas for future NCSS development.

This study aims to determine the cybersecurity agendas of leading countries and derive their implications using topic modelling, a text analysis technique, to prepare their NCSSs for development and/or revision. To accomplish this objective, we focused on the eight NCSSs of the US, UK, Japan, and EU, who have attempted to assert their leadership in cyberspace by establishing their NCSSs earlier, and by constantly improving their NCSSs in consideration of the changing threat environment. Furthermore, the aforementioned four countries are suitable for inspiring the design of a domestic cybersecurity agenda for South Korea because these countries have similar cybersecurity approaches and similar or higher technology levels with respect to South Korea.

The remainder of this paper is organised as follows. The first part consists of a literature review on topic modelling and NCSS analysis. The second part presents an analysis of target NCSS documents. The third part provides information on 15 cybersecurity agendas and their trends by nation and period as a result of topic modelling analysis, and the last part reveals the conclusion and future direction of research.

## II. Literature Review

### A. Topic Modelling

Unstructured data such as NCSSs have been analysed mainly using qualitative methods rather than quantitative methods because of the nonlinear relationship between cause and effect, the importance of historical reasons, and path-dependent development. However, as natural language processing (NLP) techniques are applied to existing data mining processes, empirical and quantitative analyses of unstructured text data increasingly gain attention in the field of policy analysis. In its early stages, this type of text analysis was used primarily for library and information science and computer engineering, whereas nowadays, it is used for a greater variety of purposes as part of quantitative content analysis.

Topic modelling is a statistical technique used to discover hidden structures from collections of documents. In policy research, topic modelling has been used to discover policy agendas or issues from news articles, speeches, and petitions, and to monitor research trends through the analysis of research papers in time series. Furthermore, research applying topic modelling to policy evaluation has recently emerged. Table I shows a list of these studies with descriptions of the methodology.

TABLE I. A LIST OF POLICY ANALYSIS STUDIES APPLYING TOPIC MODELLING

| **Research Area** | **Study** | **Year** | **Purpose** | **Dataset** | **Algorithm** |
|---|---|---|---|---|---|
| Policy Agenda Analysis | [1] | 2013 | Monitoring public opinion | all posts by top 2,000 'LiveJournal' (blog platform in Russia) users (2011–2012) | LDA |
| | [2] | 2015 | Understanding citizens' direct policy suggestions | 2,850 petition texts (2011–2014) | LDA |
| | [3] | 2017 | Analysing political agenda of European Parliament | English language legislative speeches in European Parliament plenary (1999–2014) | NMF |
| | [4] | 2019 | Policy requirement at citizens' level | 173 posts in social media | LSA |
| | [5] | 2019 | Identifying relation between mass media and public attention | news articles, Google trends query, Twitter keywords (Jul. 31st to Nov. 5th, 2017) | NMF |
| Research Trend Analysis | [6] | 2017 | Discovering themes and trends in transportation research | 17,163 papers (1990–2015) | LDA |
| | [7] | 2018 | Exploring research trend of smart factory | 2,488 international papers and 404 Korean papers (1995–2016) | LSA |
| | [8] | 2019 | Analysing research topics in cybersecurity and data science | 48 papers (2012–2018) | LDA |
| Impact Analysis | [9] | 2021 | Assessing temporal patterns of newspaper coverage | 6,645 articles on German Renewable Energy Act (2000–2017) | LDA |

As shown in Table I, researchers could determine policy implications by selecting appropriate datasets and algorithms according to their research purposes and interpreting the topic modelling results. Specifically, Table I shows that policy agendas could be discovered from SNS postings, petitions, speeches, articles, etc., research trends from research papers, and policy impact from the contents of articles on specific issues. On the other hand, algorithm selection does not depend on the research purpose or area. Some algorithms for categorising topics from words in documents include latent semantic analysis (LSA), non-negative matrix factorisation (NMF), and latent dirichlet allocation (LDA), among which LDA is the most widely used for topic modelling in social science. This is because LDA assumes that multiple topics exist in a single document, which is in harmony with the social science assumption that a single body of text does not reflect only a single point of view, but that multiple competing points of view can appear within the same document. Therefore, this study attempted topic modelling using LDA, the algorithm that is most widely used for policy analysis.

### *B. National Cybersecurity Strategy*

A national cybersecurity strategy (NCSS) is a document that reflects cybersecurity policy direction and stance on cyber threats at the national level. Because the NCSS sets national strategic objectives and priorities for a specific period, it is essential to consider the evolving cyber threat environment and the national approach to cybersecurity in a timely manner. For example, Japan has a cybersecurity policy structure that is revised every three years, and the EU every seven years. However, because of rapid technological changes and the short technological life cycle of information and communications technology (ICT), NCSS revision cycles need to be shorter in the future. For nations that want to properly establish or revise their NCSSs, analysis of the NCSSs of countries that have leadership in cyberspace or similar approaches to cybersecurity is important. This strategy will help with identifying new policy agendas that have not yet been considered and with uncovering any issues that may require cybersecurity cooperation.

Studies on NCSSs have usually aimed to discover common structures or identify further agendas that need to be considered. However, prior to the application of data analysis such as topic modelling to the cybersecurity policy area, qualitative methodologies, which forced reliance on the opinions of experts, were used in the analysis of NCSSs. Qualitative analysis not only consumes large amounts of time, but also is prone to inconsistencies because of the likelihood of differing opinions among these experts. Therefore, it is necessary to establish an automated quantitative analysis system to work alongside qualitative analysis. NCSS analysis using topic modelling has thus far focused only on analysing more countries and more data, which is unsuitable for studies aiming to discover cybersecurity agendas for the establishment or revision of NCSSs. Of course, it is important to examine global cybersecurity trends practically and academically, but in any research for the purpose of establishing or revising an NCSS, it is necessary to limit the scope of analysis to NCSSs in like-minded countries or in advanced countries. Table II outlines prior studies on NCSS analysis.

TABLE II. A LIST OF NCSSS ANALYSIS STUDIES USING TOPIC MODELLING METHOD

| Study | Year | NCSSs | Methodology | Description |
|---|---|---|---|---|
| [10] | 2013 | 19 NCSSs | (Qualitative) comparison based on 11 categories | Identifying formal structures for NCSS development |
| [11] | 2015 | 3 NCSSs | (Qualitative) comparison based on 7 categories | Finding NCSSs, in general, changed from voluntary self-regulation to enforced self-regulation |
| [12] | 2016 | 10 NCSSs | (Qualitative) content analysis | Finding 8 main components of NCSSs |
| [13] | 2019 | 6 NCSSs | (Qualitative) cross-section analysis using 8 comparison elements | Evaluating robustness of existing cyber security strategy of Bangladesh |
| [14] | 2017 | 60 NCSSs | (Quantitative) clustering and topic modelling | (Initial attempt to compare NCSSs using topic modelling method) Identifying 10 topics in NCSSs |
| [15] | 2020 | 101 NCSSs | (Quantitative) topic modelling | Identifying 4 critical agendas in NCSSs |

Topic modelling has contributed to the understanding of international trends in cybersecurity by enabling massive data analysis and extending NCSS analysis to quantitative and empirical areas. However, the limitations of not considering the time series and the scope of analysis remain, rendering these past analyses insufficient for deriving policy implications for future NCSSs. Therefore, this study focuses on characterising the NCSSs of the US, UK, Japan, and EU, tracking changes in their topic distributions over time, and then identifying critical national cybersecurity agendas through comprehensive comparative analysis of the results of topic modelling.

## III. DATASET

South Korea launched its first national cybersecurity strategy in 2019. Although this strategy is not the first official document to reveal the response stance of South Korea to cyber threats, it is the first cybersecurity strategy document established in accordance with the national security strategy. This strategy contains six strategic tasks, the titles of which are listed in detail in Table III.

To implement the NCSS, South Korea has announced an action plan at the agency level to support these six strategic tasks until 2022. This suggests that the policy demand for NCSS revision would increase, such as in identifying additional policy agendas worthy of consideration but not covered by existing NCSSs. Therefore, this study selected the NCSSs of the US, UK, Japan, and EU for comparative analysis to derive additional considerations for revising the NCSS of South Korea. Two criteria were considered in the selection of the target of analysis. For the first criterion, the target must have similar approaches to cyberspace in terms of international relationships, while also having similar ICT research and development level, to that of South Korea. For the second criterion, the target should have published an NCSS more than once, such that its NCSS transition in time series can be tracked. This target selection enables a direct comparative analysis of cybersecurity agendas derived from topic modelling results and the strategic tasks of the South Korean NCSS; it is also suitable for examining NCSS trends by country and period, which have not been provided by prior studies that used topic modelling. The dataset for this study is presented in Table IV. Prior to analysis, the aforementioned eight NCSSs were subjected to pre-processing: synonyms were extracted into single words, and unnecessary words with general meaning were eliminated. As a result, 1,287 words remained for the actual LDA topic modelling analysis.

TABLE III. STRATEGIC TASKS PRESENTED IN NCSS OF SOUTH KOREA

| | |
|---|---|
| **1. Increase Safety of National Core Infrastructure** | |
| 1-1 | Strengthen security of national information and communications networks |
| 1-2 | Improve cybersecurity environment for critical infrastructure |
| 1-3 | Develop next-generation cybersecurity infrastructure |
| **2. Enhance Cyber Attack Response Capabilities** | |
| 2-1 | Ensure cyber attack deterrence |
| 2-2 | Strengthen readiness against massive cyber attacks |
| 2-3 | Devise comprehensive and active countermeasures for cyber attacks |
| 2-4 | Enhance cybercrime response capabilities |
| **3. Establish Governance Based on Trust and Cooperation** | |
| 3-1 | Facilitate public–private–military cooperation system |
| 3-2 | Build and facilitate nation-wide information sharing system |
| 3-3 | Strengthen legal basis for cybersecurity |
| **4. Build Foundations for Cybersecurity Industry Growth** | |
| 4-1 | Expand cybersecurity investment |
| 4-2 | Strengthen competitiveness of cybersecurity workforce and technology |
| 4-3 | Foster growth environment for cybersecurity companies |
| 4-4 | Establish principle of fair competition in cybersecurity market |
| **5. Foster Cybersecurity Culture** | |
| 5-1 | Raise cybersecurity awareness and strengthen cybersecurity practice |
| 5-2 | Balance fundamental rights with cybersecurity |
| **6. Lead International Cooperation in Cybersecurity** | |
| 6-1 | Enrich bilateral and multilateral cooperation systems |
| 6-2 | Secure leadership in international cooperation |

TABLE IV. ANALYSIS TARGET DOCUMENTS

| Nation | Year | Document (NCSS) | Version |
|---|---|---|---|
| U.S. | 2003 | National Strategy to Secure Cyberspace | Previous |
| | 2018 | National Cyber Strategy | Current |
| U.K. | 2011 | The UK Cyber Security Strategy | Previous |
| | 2016 | National Cyber Security Strategy 2016–2021 | Current |
| Japan | 2015 | Cybersecurity Strategy | Previous |
| | 2018 | Cybersecurity Strategy | Current |
| EU | 2013 | EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace | Previous |
| | 2020 | EU Cybersecurity Strategy for the Digital Decade | Current |

## IV. Data Analysis and Result

### A. *Result of Topic Modelling*

A total of 15 agendas were identified, as shown in Table V. Although there are a few tools available for determining topic sets, such as the minimum perplexity approach, the suitable approach is not yet clear. Therefore, we designated an optimal number of topics by reviewing the keywords constituting each agenda in a way that minimised duplication, and maximising the explanatory power of the agendas from a holistic point of view.

Table V consists of the columns Sector, Agenda, Keywords, and Proportion. The naming of each agenda is based on its constituent keywords. Furthermore, the agendas are grouped into four sectors: Infra Stability (I), Protection and Response Capability (II), Industry and Technology (III), and International Cooperation (IV), in accordance to their strategic or operational objectives. Lastly, the rightmost column of Table V presents the proportion of each agenda.

TABLE V. Fifteen Cybersecurity Agendas of US, UK, Japan and EU and their Proportion

| **Sector** | **Agenda** | **Keyword (Top 15)** | **Prop.** |
|---|---|---|---|
| Infra Stability (I) | ① Network and System Vulnerability | **cyber-attack**, **network**, **system**, **vulnerability**, **software**, computer, internet, actor, **damage**, attacker, critical infrastructure, **malware**, **hardware**, attention, **disruption** | 7.93 |
| | ② Cyber Security Role and Responsibility | **security**, **agency**, **system**, **responsibility**, cyber space, **role**, **risk**, state, investment, **control**, IT, procurement, **administration**, **asset**, effectiveness | 5.86 |
| | ③ Risk Assessment and Management | **risk**, **cyber threat**, **vulnerability**, cyber-attack, **critical infrastructure**, **assessment**, **priority**, operation, challenge, company, nation, damage, **risk management**, **resource**, opportunity | 7.13 |
| | ④ Information Communication Network Access Control | **system**, **information**, **network**, **security**, infrastructure, **communication**, **access**, **control**, **information system**, computer, AI, internet, trustworthiness, knowledge, integrity | 6.29 |
| Protection and Response Capability (II) | ① Privacy and Intellectual Property Security | **internet**, information, **right**, **freedom**, **citizen**, **privacy**, **protection**, **security**, business environment, **society**, **DNS**, **online**, **intellectual property**, **breach**, **human right** | 7.04 |
| | ② Cyber Defence Capability | **capability**, **cyber-attack**, **defence**, **cyber threat**, **national security**, nation, **critical infrastructure**, **state**, actor, **cyber terrorism**, **adversary**, network, infrastructure, **ability**, **operation** | 7.85 |
| | ③ Incident Response and Information Sharing | **cyber-attack**, **incident**, **response**, information, **cyber threat**, **capability**, **coordination**, **information sharing**, damage, sharing, **detection**, **recovery**, knowledge, **situational awareness**, **monitoring** | 8.40 |
| | ④ Cyber Crime Law Enforcement and Investigation | **cyber-crime**, **law**, **enforcement**, **capability**, agency, cyber threat, **intelligence**, **response**, **investigation**, **authority**, tool, force, child **protection**, resource, **capacity** | 8.61 |
| Industry and Technology (III) | ① Standard, Certification and Supply Chain Security | **system**, **security**, **operation**, **IoT**, **business environment**, **critical infrastructure**, **standard**, information, **industry**, **assurance**, safety, **certification**, **supply chain**, connection, collaboration | 6.75 |
| | ② ICT Innovation | **information**, **internet**, **society**, **security**, **economy**, infrastructure, **progress**, **innovation**, **multi-stakeholder**, governance, **ICT**, **market place**, communication, country, culture | 4.22 |
| | ③ Public Private Partnership (PPP) | **industry**, cyber awareness, **research**, **R&D**, security, **coordination**, **standard**, public, role, **partnership**, collaboration, company, information, state, **innovation** | 4.61 |
| | ④ Security Awareness and Knowledge | **business environment**, **market place**, **company**, **investment**, **personnel**, **cyber awareness**, risk, cost, judiciary, solution, opportunity, **knowledge**, role, **human resource**, demand | 7.90 |
| International Cooperation (IV) | ① International Norm and State Behaviour | **state**, **rule**, **behaviour**, **principle**, **national security**, **peace**, **law**, **norm**, **stability**, **international community**, **international law**, society, safety, actor, **alliance** | 8.18 |
| | ② EU Member State Cooperation | **member**, **state**, **cooperation**, **defence**, authority, progress, agency, **NIS directive**, **ENISA**, **coordination**, **incident**, **resilience**, role, framework, capability | 3.99 |
| | ③ International Partnership | **country**, **partner**, **cooperation**, cyber threat, **partnership**, **industry**, challenge, capability, information, **ally**, border, network, communication, **participant**, NATO | 5.26 |

### B. *NCSS Agenda Transition*

*1) Topic distribution by nation:* The results of topic distribution for the four nations are presented in Table V. This section aims to identify the differences in cybersecurity approaches by nation. In Fig. 1, which was derived from the current NCSS of each country that was analysed, the blue bar represents the percentage of each agenda, whereas the orange line represents the percentage of each sector, which is the sum of the percentages of agendas constituting that sector (I–IV). According to the results, the NCSSs of the US and UK focused on improving cybersecurity response capability, whereas those of Japan and the EU vitalised the cybersecurity industry and international cooperation, respectively.

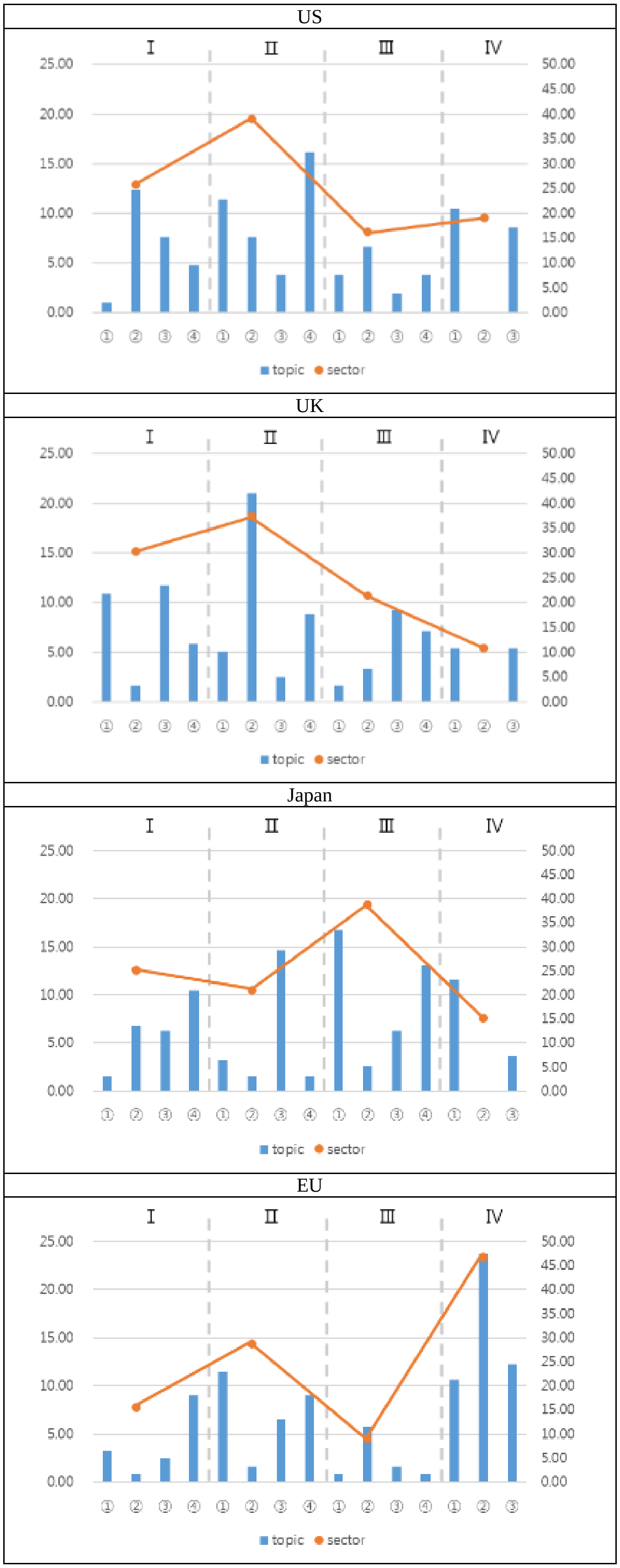

Fig. 1. Topic and Sector Distribution Derived from the Current NCSS of each Country.

The NCSS of the US (2018) emphasised improving incident response capabilities (II), especially cybercrime law enforcement and investigation capabilities (II-④), and establishing cybersecurity governance (I-②). In addition, intellectual property security (II-①) had a relatively higher proportion compared with in other NCSSs, which means that the US, with its world-class technology levels in a wide range of emerging technology areas such as IT, aerospace, and defence industries, likely regard the technological and economic aspects of its cyberspace from a national security perspective.

Similar to the US, the UK (2016) prioritised protection and response capability (II). However, unlike the US, the UK highly concentrated on cyber defence capability (II-②). This may reflect the concept of traditional defence power in cyberspace, and is consistent with the creation of a National Cyber Force, which is known to provide offensive and defensive capabilities in pursuit of national security objectives, and operation of an Active Cyber Defence (ACD) programme, which is meant to reduce harm from commodity cyber-attacks by providing necessary tools and services. Moreover, the UK was also shown to be discussing both vulnerability mitigation (I -①) and risk assessment and management (I -③) to improve infrastructure stability. A risk-centric approach to cybersecurity could be the basis for establishing concretised security measures according to asset or information-specific importance and the level of risk exposed; therefore; the NCSSs of the US, Japan, and UK covered this type of approach at high proportions.

On the other hand, the NCSS of Japan (2018) was characterised by a relatively high proportion (39%) for the cybersecurity industry and technology sector (III). This observation is consistent with the objective of its strategy; the first objective of Japan, unlike in the other analysed countries, was to enable socio-economic vitality and sustainable development. Their suggested policy approach to achieving this objective was to advance cybersecurity, establish a secure supply chain, and build a secure IoT system. This approach to cybersecurity was clearly different from those of the other analysed countries, which prioritised the protection of critical infrastructure and enhancement of deterrence in cyberspace. In addition, their National Information Security Center (NISC), which is responsible for information security policy, announced the necessity to protect the supply chain against dependence on excessive foreign technologies, to drive data accumulation and utilisation using emerging technologies such as AI, and to accomplish international standardisation of related technologies. Based on a comprehensive view of these considerations, the focal point of the cybersecurity policy of Japan seemed to be the revitalisation of future technological industry and economy.

Finally, the topic modelling results characterised the NCSS of the EU as emphasising international cooperation. In particular, the EU sought to improve levels of cyber resiliency and consistency across Europe through cooperative responses in cyberspace based on the NIS Directive, as shown by the word composition of the topic regarding EU member state cooperation. In particular, according to the contents of the EU cybersecurity strategy, the EU would strengthen the interoperability of information systems, establish a security operations centre (SOC) network, and expand the use of the EU Cyber Diplomacy Toolbox to achieve their objectives of improving the level of resiliency and consistency in cyberspace. Therefore, the strategy of the EU would have been devised based on a very high proportion of international cooperation.

*2) Topic distribution by period:* The topic distributions of the analysed NCSSs are shown in Table VI.

As presented in Table VI, there were no significant increases or decreases in the NCSS agenda transitions in time series. This observation indicates that in setting their cybersecurity agendas, each country considers its own threat environment and its geopolitical characteristics rather than the agenda trends at that time. In other words, in the establishment or revision of an NCSS, an understanding of the threat environment facing the country should be obtained, and a clear analysis of their own approach to solving it should be conducted.

The agenda that exhibited the biggest distribution gap in the US strategies was network and system vulnerability. Although the previous strategy of the US prioritised this agenda (which had the highest proportion, at almost 20%), that proportion was significantly reduced to less than 1% in the current strategy. This observation could reflect a change in response posture against cyber-attacks, crimes, or even threats, from passive protection that mitigates critical vulnerabilities in their own network or system, to an active response posture that includes law enforcement in anti-cybercrime efforts and cooperative responses with like-minded countries.

These trends could also be observed in the UK, which addressed strengthening defence and response capabilities in both their 2011 and 2016 strategies. In particular, in their current strategy, the weight of the agenda on cyber defence capability has increased (+12.68%), suggesting that defensive and even offensive operations could be conducted based on an understanding of cyberspace as a military domain.

Meanwhile, the NCSSs of Japan had the smallest change in topic distribution over time, because the three-year NCSS establishment cycle of Japan is not only short compared to those of other countries but also established with the basic act on cybersecurity as a legal basis. On the other hand, because Japan is constantly emphasising the revitalisation of the cybersecurity industry, it is necessary for them to continuously grasp related standards and supply chain security trends in the future.

The EU also had a small change in their distribution of cybersecurity agendas by period. However, a noticeable difference was that the proportion of EU member state cooperation slightly decreased, whereas the proportion of agenda on international partnership somewhat increased. For context, Europe has recently continued to discuss European capability building from the security and defence standpoint and the ‘strategic autonomy’ based on it. As the need to work together with international partners to achieve these goals is emphasised, it is necessary to observe how Europe will strengthen its international partnerships to secure strategic autonomy in the future.

TABLE VI. TOPIC DISTRIBUTION IN EACH NCSS DOCUMENT

| **Topic (Agenda)** | **Topic distribution (%)** | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | **US 2003** | **UK 2011** | **EU 2013** | **JP 2015** | **UK 2016** | **JP 2018** | **US 2018** | **EU 2020** |
| Network and System Vulnerability | 19.42 | 5.30 | 1.15 | 4.04 | 10.92 | 1.57 | 0.95 | 3.28 |
| Cyber Security Role and Responsibility | 13.04 | 0.00 | 1.15 | 4.04 | 1.68 | 6.81 | 12.38 | 0.82 |
| Risk Assessment and Management | 12.17 | 3.03 | 1.15 | 1.79 | 11.76 | 6.28 | 7.62 | 2.46 |
| Information Communication Network Access Control | 8.70 | 0.76 | 2.30 | 2.69 | 5.88 | 10.47 | 4.76 | 9.02 |
| Privacy and Intellectual Property Security | 7.54 | 12.12 | 10.34 | 3.14 | 5.04 | 3.14 | 11.43 | 11.48 |
| Cyber Defence Capability | 8.99 | 8.33 | 1.15 | 2.24 | 21.01 | 1.57 | 7.62 | 1.64 |
| Incident Response and Information Sharing | 6.96 | 2.27 | 11.49 | 17.94 | 2.52 | 14.66 | 3.81 | 6.56 |
| Cyber Crime Law Enforcement and Investigation | 5.22 | 29.55 | 13.79 | 1.79 | 8.82 | 1.57 | 16.19 | 9.02 |
| Standard, Certification and Supply Chain Security | 2.90 | 2.27 | 2.30 | 18.83 | 1.68 | 16.75 | 3.81 | 0.82 |
| ICT Innovation | 2.61 | 5.30 | 4.60 | 6.28 | 3.36 | 2.62 | 6.67 | 5.74 |
| Public Private Partnership(PPP) | 3.48 | 3.03 | 1.15 | 4.48 | 9.24 | 6.28 | 1.90 | 1.64 |
| Security Awareness and Knowledge | 6.38 | 14.39 | 5.75 | 9.87 | 7.14 | 13.09 | 3.81 | 0.82 |
| International Norm and State Behaviour | 0.87 | 10.61 | 9.20 | 14.80 | 5.46 | 11.52 | 10.48 | 10.66 |
| EU Member State Cooperation | 0.00 | 0.76 | 31.03 | 0.00 | 0.00 | 0.00 | 0.00 | 23.77 |
| International Partnership | 1.74 | 2.27 | 3.45 | 8.07 | 5.46 | 3.66 | 8.57 | 12.30 |

### C. Comparative Analysis of NCSS Agendas with Coverage in South Korea

As discussed earlier, NCSS agendas had different distributions depending on the threat environment and approach to cybersecurity of each country. However, the US, UK, Japan, and EU have close cooperation in cybersecurity and in related technologies and research areas, and thus identifying the cybersecurity agendas of these countries is essential for future cooperation or diplomacy. Furthermore, analysing the agendas of like-minded countries is valuable as a method for determining suitable NCSS agendas for a given country because it provides an understanding of global cybersecurity trends in the context of cooperative response. Therefore, this section identifies agendas worthy of consideration for future NCSS revisions in South Korea by comparing the strategic task of the current NCSS with the 15 agendas previously derived.

Table VII is the result of comparing the 15 agendas derived from this analysis with the contents of the NCSS of South Korea. This analysis reveals two agendas that were not covered (marked with ×) and one agenda partially covered (marked with △) in the NCSS of South Korea.

First, one agenda on risk assessment and management in sector I was not covered in the NCSS of South Korea. Because cyber threats tend to be increasingly diverse and sophisticated, a single way of managing security vulnerabilities in systems or networks may not be sufficient for preventing cyberattacks that use social engineering techniques. However, the current NCSS of South Korea has been focused on vulnerability management in the infra stability sector, and not on risk assessment and management. Here, cyber risk is a concept that considers not only vulnerabilities in the system itself but also the possibility of manipulation, disruption, or destruction of specific assets [16].

Moreover, cyber risk management refers to a series of actions that identify the value and importance of individual assets, evaluate the impact of vulnerabilities or risks of exploiting them, and prepare and implement appropriate countermeasures for the assessed risk. Therefore, efforts should be made to ensure the stability of critical infrastructure in a dynamic cyber threat environment through the establishment of a framework for assessing and managing risk to critical assets in addition to vulnerability management [17].

Furthermore, the NCSS of South Korea has no discussion on the protection of intellectual property rights. Competitiveness in science and technology is becoming more important in both cybersecurity and economic aspects compared to in the traditional security perspective. Whereas many countries are making great efforts to secure technological competitiveness, the number of malicious cyber activities targeting the intellectual property (IP) of research institutes or universities has been increasing. Accordingly, countries with high levels of technology, such as the US and UK, are implementing strict measures against such technology theft to maintain their technological and economic superiority [18]. In particular, the US government is using name-and-shame processes, such as public indictments on IP theft, to inform countries about these malicious activities and continue efforts to strengthen relevant law enforcement capabilities. For future NCSS revisions in South Korea, there is a necessity for multilateral discussions to protect future cybersecurity R&D achievements through close cooperation between science, technology, and industry, to secure the technological advantage of the country.

Finally, a discussion on supply chain security is necessary. The supply chain refers to the overall system of organisations, resources, human resources, and information in the process of providing products or services to customers. The supply chain is particularly complex for ICT products and services, and includes processes of S/W and H/W design, deployment, acquisition, operation, and maintenance. Supply chain security issues, which began to be discussed in earnest after the US sanctions against Huawei, are currently being embodied in policies for developing supply chain risk assessment tools or systems, and diversifying or internalising 5G suppliers [19]. However, in the case of the NCSS of South Korea, discussions on overall supply chain risk management, including all ICT products and services such as 5G, IoT devices, and cloud services, are limited, and are covered only through standards and certification systems and the security-by-design concept. Therefore, it is necessary to establish and realise a supply chain security system across the country to analyse supply chain risk and prepare for global supply chain reorganisation under US–China trade tension.

TABLE VII. THE RESULT OF COMPARING THE 15 AGENDAS WITH THE CONTENTS OF NCSS OF SOUTH KOREA

| Sector | Agendas | Comparison Result | |
|---|---|---|---|
| | | (○/△/×) | Related tasks # of Table III |
| Infra Stability | Network and System Vulnerability | ○ | 1-1,2 |
| | Cyber Security Role and Responsibility | ○ | 3-1 |
| | Risk Assessment and Management | × | - |
| | Information Communication Network Access Control | ○ | 2-2 |
| Protection and Response Capability | Privacy and Intellectual Property Security | × | - |
| | Cyber Defence Capability | ○ | 2-1,3 |
| | Incident Response and Information Sharing | ○ | 2-2, 3-2 |
| | Cyber Crime Law Enforcement and Investigation | ○ | 2-4 |
| Industry and Technology | Standard, Certification and Supply Chain Security | △ | 1-3 |
| | ICT Innovation | ○ | 4-3 |
| | Public Private Partnership (PPP) | ○ | 3-1, 4-1,3 |
| | Security Awareness and Knowledge | ○ | 4-1,2 |
| International Cooperation | International Norm and State Behaviour | ○ | 6-2 |
| | EU Member State Cooperation | ○ | 6-1 |
| | International Partnership | ○ | 6-1 |

## V. Conclusion

Cybersecurity has more complex and multidimensional characteristics compared to those of traditional security, and involves a combination of hyper-connected cyberspace, rapid development of ICT, and double-use issues of cyber technology. In addition, differences in the approaches to cyber space and cyber threat environments in different countries contribute to further increasing this complexity, which in turn complicate the macroscopic perspective analysis of national cybersecurity policies. Therefore, this study aimed to derive the national cybersecurity policy agendas of major countries from a macro perspective by using the topic modelling method.

The study was divided into two parts. The first part was to use a topic modelling method to identify national cybersecurity policy agendas in major countries, and the second part was to determine policy agendas that could be further considered for future NCSS revisions in South Korea. Thus far, policy research in the field of cybersecurity with the use of topic modelling has focused on expanding the scope of analysis to observe the global cybersecurity landscape. Therefore, this study is meaningful in that it used topic modelling to explore critical agendas and quantitatively compare the focal points of various NCSSs for the benefit of future NCSS revisions in South Korea.

As a result of this study, 15 agendas were derived from words that compose the NCSSs of the US, UK, Japan, and EU. These agendas were grouped into infrastructure stability, response capability, industrial revitalisation, and international cooperation, in accordance to their attributes. Based on the agenda distribution, we observed that the approach to cybersecurity differed by country: the US and UK focused on response capability, whereas Japan and the EU focused on the cybersecurity industry and international cooperation, respectively. Furthermore, the distribution of NCSS agendas depended only on the perceived cyber threat environment and approach to cybersecurity by country, and no agenda exhibited a significant increase or decrease in proportion over time, regardless of country. On the other hand, we highlight the necessity for discussions on risk assessment and management systems, intellectual property theft, and supply chain security systems, to diversify cyber security management systems at a national level, based on a comparison of the 15 agendas with the NCSS strategic task of South Korea.

This study provides a comprehensive understanding of the cybersecurity policy agenda from the perspective of South Korea. However, because the scope of the analysis was limited to NCSSs and to deriving implications for future NCSS revisions, we propose discovering policy agendas from a wider variety of sources and comparing them in future research. As presented in the previous literature review, policy agendas could be derived from a variety of sources, including publicly published reports, news articles, research papers, petitions, and even SNS postings. In particular, because of the multidimensional nature of cybersecurity policy, multilateral cooperation efforts across society, government, science, technology, industry, and academia are essential for building global cybersecurity resiliency beyond national security. Therefore, it would be meaningful to comprehensively compare cybersecurity policy demands from various perspectives.

## References

[1] O. Koltsova and S. Koltcov, “Mapping the public agenda with topic modeling: the case of the Russian Livejournal”, *Policy & Internet vol. 5, no. 2,* pp. 207-227, 2013.

[2] L. Hagen, O. Uzuner, C. Kotfila, T. M. Harrison and D. Lamanna, “Understanding citizens’ direct policy suggestions to the federal government: a natural language processing and topic modeling approach”, *2015 48th Hawaii International Conference on System Sciences,* 2015.

[3] D. Greene and J. P. Cross, “Exploring the political agenda of the European parliament using a dynamic topic modeling approach”, *Political Analysis vol. 25, no. 1,* pp. 77-94, 2017.

[4] O. B. Driss, S. Mellouli and Z. Trabelsi., “From citizens to government policy-makers: Social media data analysis”, *Government Information Quarterly vol. 36, no. 3*, pp. 560-570, 2019.

[5] S. Pinto and F. Albanese, “Quantifying time-dependent Media Agenda and public opinion by topic modeling”, *Physica A: Statistical Mechanics and its Applications vol. 524*, pp. 614-624, 2019.

[6] L. Sun and Y. Yin, “Discovering themes and trends in transportation research using topic modeling”, *Transportation Research Part C: Emerging Technologies vol. 77*, pp. 49-66, 2017.

[7] H. L. Yang, T. W. Chang and Y. Choi, “ Exploring the Research Trend of Smart Factory with Topic Modeling”, *Sustainability vol. 10, no. 8,* pp. 2779-2793, 2018.

[8] T. Bechor and B. Jung, “ Current State and Modeling of Research Topics in Cybersecurity and Data Science”, *systemics, cybernetics and informatics vol. 17, no. 1,* pp. 129-156, 2019.

[9] J. Dehler-Holland, K. Schumacher and W. Fichtner, “Topic Modeling Uncovers Shifts in Media Framing of the German Renewable Energy Act”, *Patterns vol. 2, no. 1,* 2021.

[10] E. Luiijf, B. Kim and P De Graaf, “Nineteen national cyber security strategies”, *International Journal of Critical Infrastructures vol. 9, no. 1-),* pp. 3-31, 2013.

[11] K. S. Min, S. W. Chai and M. Han, “An International Comparative Study on Cyber Security Strategy”, *International Journal of Security and Its Applications vol. 9, no. 2*, pp. 13-20, 2015.

[12] R. Sabillon, V. Cavaller and J. Cano, “National Cyber Security Strategies: Global Trends in Cyberspace”, *International Journal of Computer Science and Software Engineering vol. 5, no. 5,* pp. 67-81, 2016.

[13] K. Sarker, H. Rahman, K. F. Rahman, M. S. Arman, S. Biswas and T. Bhuiyan, “A Comparative Analysis of the Cyber Security Strategy of Bangladesh”, *International Journal on Cybernetics & Informatics vol. 8,* pp. 1-21, 2019.

[14] F. Kolini and L. Janczewski “Clustering and Topic Modelling: A New Approach for Analysis of National Cybersecurity Strategies”, Pacific Asia Conference on Information Systems, 2019.

[15] J. An, S. Kang and H. Im, “An Analysis of National Cybersecurity Strategies using Topic Model”, *Korean Journal of International Relations vol. 60, no. 4,* pp. 119-169, 2020.

[16] R. R. Perols and U. S. Murthy “The Impact of Cybersecurity Risk Management Examinations and Cybersecurity Incidents on Investor Perceptions and Decisions” , *A Journal of Practice & Theory vol. 40, no. 1,* pp. 73-89, 2021.

[17] A. Buzdugan, “Review on use of decision support systems in cyber risk management for critical infrastructures”, *Journal of Engineering Science, vol. 27, no. 3,* pp. 134-145, 2020.

[18] V. K. Aggarwal and A. W. Reddie, “New economic statecraft: Industrial policy in an era of strategic competition”, *Issues & Studies vol. 56, no. 2,* 204006, 2020.

[19] O. Osunji, “Know your suppliersL A review of ICT supply chain risk management efforts by the US government and its agencies”, *Cyber Security: A Peer-Reviewed Journal, vo. 4, no. 3,* pp. 232-242, 2021.