Global: Jurnal Politik Internasional

Volume 24 | Number 1 Article 5

July 2022

The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices

Azza Bimantara
Department of International Relations, Corvinus University of Budapest, azza.bimantara@gmail.com

Recommended Citation
Bimantara, Azza (2022) "The Normative Enactment of International Cybersecurity Capacity Building Assistance: A Comparative Analysis on Japanese and South Korean Practices," *Global: Jurnal Politik Internasional*: Vol. 24: No. 1, Article 5.
DOI: 10.7454/global.v24i1.684
Available at: https://scholarhub.ui.ac.id/global/vol24/iss1/5

Global: Jurnal Politik Internasional Vol. 24 No. 1. Page 109-142. DOI: 10.7454/global.v24i1.684
 E-ISSN: 2579-8251

THE NORMATIVE ENACTMENT OF INTERNATIONAL CYBERSECURITY CAPACITY BUILDING ASSISTANCE: A COMPARATIVE ANALYSIS ON JAPANESE AND SOUTH KOREAN PRACTICES

Azza Bimantara

Department of International Relations
Corvinus University of Budapest

Email: azza.bimantara@gmail.com
Submitted: 18 November 2021; accepted: 2 June 2022

Abstrak

*Komunitas internasional mendorong negara-negara untuk mendukung dan membantu satu sama lain dalam mengurangi risiko yang berasal dari kesenjangan digital melalui kerja sama internasional. Namun, mereka tidak dapat menyepakati bagaimana norma-norma internasional berlaku untuk dunia siber, apalagi membentuk dan mengatur bantuan pembangunan kapasitas keamanan siber (CCB) internasional. Negara-negara menggunakan bantuan CCB internasional untuk menerapkan norma-norma dunia maya berdasarkan persepsi mereka. Hal ini menghasilkan variasi dalam bentuk bantuan CCB internasional yang diberikan oleh negara donor. Menggunakan teori konstruktivisme sosial dan konsep CCB sebagai bantuan internasional, tulisan ini membandingkan praktik bantuan CCB dari kasus-kasus terpilih di dua negara donor: Jepang dan Korea Selatan. Analisis lebih lanjut menekankan peran struktur normatif negara donor dalam membentuk identitas, peran, kepentingan, dan perilaku mereka dalam bantuan CCB internasional. Struktur normatif kerja sama keamanan siber internasional Jepang membentuk identitas dan peran Jepang yang mengutamakan kepentingan normatif dan material yang dominan keamanan. Sementara itu, struktur normatif "*developmental*" Korea Selatan mengonstruksi identitas dan peran negara yang membentuk normatif pembangunan dan kepentingan material. Bantuan CCB internasional Jepang sangat berorientasi pada keamanan, sementara Korea Selatan kurang berorientasi pada keamanan. Perbedaan ini menegaskan fragmentasi norma siber global akibat proses persepsi yang berbeda oleh negara-negara di seluruh dunia.*

Kata kunci:

Bantuan CCB internasional, kesenjangan digital, keamanan siber, Jepang, Korea Selatan

Abstract

The international community encourages states to embrace the international cooperation to support and assist each other in reducing risks stemming from the digital divide. However, they cannot agree upon how international norms apply to cyberspace, let alone shaping and regulating international cybersecurity capacity building (CCB) assistance. States use international CCB assistance to impose cyber-norms based on their perceptions. It results in different forms of assistance provided by each donor country. Using social constructivism theory and the CCB concept as international assistance, this paper compares the practice of CCB assistance from two donor countries: Japan and South Korea. It emphasises the role of each donor country's normative structure in shaping their identities, roles, interests, and behaviours in international CCB assistance. Japan's international cybersecurity cooperation normative structure shapes Japan's identities and roles that prioritise security-dominant normative and material interests. Meanwhile, South Korea's developmental focus constructs the country's identities and roles that shape developmental normative and material interests. This research finds that Japan's assistance is highly security-oriented while South Korea's is less security-oriented. Their differences highlight the fragmentation of global cyber-norms caused by different perception processes.

Keywords:

International CCB assistance, digital divide, cybersecurity, Japan, South Korea

INTRODUCTION

The UN General Assembly adopted Resolutions A/RES/68/243 and A/RES/70/237—based on several reports from the United Nations Group of Governmental Experts or UN GGE (2010; 2013; 2015) and the United Nations Open-ended Working Group or UN OEWG (2021)—on the importance of the international assistance on cybersecurity capacity building (CCB) for tackling the digital divide and its risks. The importance of such agreements is twofold. First, the international community has successfully securitised the digital divide problem, a state of inequality among countries in cybersecurity capacity and its advancement to benefit from the internet (Smith, 2002). Data from the International Telecommunication Union or ITU (2020) shows internet penetration in developing and least developed countries in 2019 (44.4% and 19.5%) is still below the world average of 51.4%, let alone developed countries' (86.7%). As the global economy is getting digitalised, some countries lacking digital development cannot benefit from advancements in information and communications technologies (ICTs). Such a shortcoming will make countries more vulnerable to any cyber-related threat that can disrupt or destroy critical infrastructures—both physical and virtual (Hohmann, Pirang, & Benner, 2017, pp. 8-9; van Puyvelde & Brantly, 2019). Moreover, insecure networks in one place can be abused to disrupt infrastructure around the globe (Hohmann & Pirang, Why Policymakers Should Care About Weak Digital Infrastructure Abroad, 2017).

Second, such securitisation results in contesting discourses of CCB in addressing the digital divide problem. It is clear that UN GGE preferred international CCB assistance to "reduce risk and enhance security [and to] promote a peaceful, secure, open, and cooperative ICT environment" (UN GGE, 2015, pp. 10-12; 2013, p. 2). However, the discussion moves to the realm of politics of international cooperation. The practice of international CCB assistance—another term is "cybersecurity sharing"—is no different from international assistance. Both resemble the requirement of a voluntary transfer of resources from one government or other agencies to support the general development of others (Williams, 2020). In short, international CCB assistance is being politicised.

Patryk Pawlak's study (2016) that illustrates this notion by arguing that CCB is a politicised foreign policy instead of the technocratic process becomes the cornerstone for

further studies in the field. It derives into two categories of focus: the practical dynamics and the normative dynamics of international CCB assistance. The former focuses on the donor-recipient relationship in shaping international CCB assistance. It includes each donor and recipient's role in driving international CCB assistance and challenges and obstacles in matching their interests (Schia, 2016; Muller, 2015; Pawlak & Barmpaliou, 2017). Further studies illustrate such dynamics in specific countries and international/regional organisations in conducting CCB assistance (Contreras & Barrett, 2020; Calandro & Berglund, 2019; Crespo, Wanner, & Ghernaouti, 2018; Hitchens & Goren, 2017). The latter focuses on norm constructions behind international CCB assistance itself. In general, there have been numerous studies about global cyber norms. There are studies on the theoretical prospect of constructing global cyber norms and its deadlock within the international community (Grigsby, 2017; Henriksen, 2019; Hurwitz, 2014; Finnemore & Hollis, 2016). However, only Zine Homburger's study that narrows its discussion specifically to the dynamics of international CCB assistance. He (2019, p. 2) argued that the lack of global cyber norm causes the politics of international CCB assistance to become a fragmented arena; each donor country will use CCB assistance to impose its cyber norms preferences toward recipient countries. Nevertheless, studies conducted by Homburger, and others within this category, overly focus on the structural level of analysis ("international society-centric") (Hobson, 2000, p. 149), while studies taking a state-centric approach is still rare. There should be a study in the field to reveal how cyber norms motivate the donor countries to advance and implement international CCB assistance towards recipient countries in addressing the digital divide problem.

Based on this literature gap, this paper posits the research questions: what do the digital divide and cybersecurity mean for states? How do states interpret their own identities and roles in international cybersecurity cooperation? What motivates them to implement international CCB assistance? How do they similarly and differently implement international CCB assistance? Using social constructivism theory and the concept of CCB as international assistance, it will comparatively analyse how normative focuses of the two donor countries—Japan and South Korea—are reflected in different forms of CCB programmes or projects with recipient countries. It argues that one's cybersecurity normative structure would define

its identity/role and normative-material interest in conducting international CCB assistance. As a result, the corresponding orientation, dimension, and forms of CCB assistance will follow. However, as Japan's security-oriented normative structure differs from South Korea's non-security-oriented (developmental) one, their identities/roles, normative-material interests, and practices also differ. This difference highlights the fragmentation of global cyber-norms.

This paper is structured as follows. First, it will introduce two analytical frameworks that will be used—CCB as international assistance and "hybrid" social constructivism theory—along with their operationalisation. It will also introduce the methodology—a qualitative, case-based comparative research design based on a "pragmatic-constructivist" research paradigm. Next, it will compare the normative structure of Japan and South Korea regarding their perception of the digital divide, cybersecurity, and international CCB assistance at the domestic and international levels. Then, it examines how Japan and South Korea's differing normative structures shape their identities/roles and normative-material interests regarding international cybersecurity cooperation. Those analyses will assess how the actual practices of Japan's and South Korea's international CCB assistance reflect their respective normative structure, identities/roles, and interests. A brief, additional comment on reproducing fragmented global cyber norms will conclude this study.

ANALYTICAL FRAMEWORK

CCB as International Assistance

UN GGE and UN OEWG reported in 2010, 2013, 2015, and 2021 about the mainstreaming of CCB as a practice of international assistance. Those reports consistently recommend that states provide international assistance that includes cooperation to improve ICT stability and security while preventing harmful pertinent practices, careful consideration on how best to cooperate in addressing cyber-related threats, and responsiveness to appropriate requests from the international community for assistance in addressing cyber-related issues.

Many scholars have attempted to formulate a definition for CCB that fits with the international assistance context. Muller (2015, p. 7), Homburger (2019, p. 4), and Hohmann et al. (2017, p. 12) emphasise the words like "support," "assistance," and "provision" in their

definition of CCB. The definitions imply the relations between donor and recipient states. They also reflect the development and security perspectives inferred from the very definition of cybersecurity. The development perspective is about "how to provide developing nations with increased access to, and the ability fully benefit from the Internet and cyberspace more generally." Meanwhile, the security perspective is about "[…] reducing digital security risks stemming from access and use of ICTs." This duality can be flexible because it can be linked and utilised in approaching security and development issues. Donor countries can impose political interests through international CCB assistance. Such political imposition can take forms in the conditionality for the assistance to be delivered, the contested norms, culture, approach, and institution regarding the CCB governance, or issue linkage.

By combining key points from each definition from the existing studies, this study proposes the following definition of international CCB assistance: *a set of activities, be it knowledge, technical, or institutional, from donor countries in supporting and assisting recipient ones to provide, build, and develop their cybersecurity capacity and capability so they can reap benefit while also reducing risks stemming from access and use of ICTs*.

This research also combines findings from several previous studies related to the definition and typology of international CCB assistance. First, Alexander Klimburg and Hugo Zylberberg (2015) segmented and dichotomised CCB activities into security-related and non-security-related official development assistance (ODA) according to the Development Assistance Committee of the Organization for Economic Cooperation and Development (OECD-DAC). Second, the Global Cyber Security Capacity Centre (GCSCC) at the University of Oxford made numerous guidance in developing cybersecurity capacity—called Cybersecurity Capacity Maturity Model for Nations (CMM). The list is derived from five CCB dimensions as follows: (1) policy and strategy, (2) cyberculture and society, (3) educational training and skills, (4) legal and regulatory frameworks, and (5) standards on organisations and technologies (GCSCC, 2021, pp. 5-6). Third, Theresa Hitchens and Nilsu Goren (2017, pp. 5-6) focused on the typology of CCB activities in a framework called "information sharing agreements," ranging from training, research, policy, information-experience sharing, military, cyberoperations, cyber-exercises, cybercrime, and best practice.

Social Constructivism

Social constructivism argues that social normative structure determines a state's identity and interest, resulting in the state's behaviour in international politics. The normative structure itself is a set of autonomous and constitutive norms which exist independently from the state (Hobson, 2000, p. 148). For constructivists, the state's behaviour follows the "logic of appropriateness" (March & Olsen, 1989).

Hobson (2000, p. 148) identifies three variants of constructivism: (1) international society-centric, (2) state-centric, and (3) radical or postmodern (further exploration will focus only on the first two variants). In international society-centric theory, the international realm becomes the "realm of obligation" consisting of two sub-structures or tiers: the principal socialising norms and international organisations (Hobson, 2000, p. 150). Any dynamics from the international level will affect the state's behaviour to conform to what becomes internationally recognised "appropriate" behaviours. International society and its principal normative structure will reproduce themselves (Hobson, 2000, p. 150). Meanwhile, state-centric theory rarely focuses on the international level. There is a dynamic interaction between domestic normative structure and domestic institutionalisation or state-building (state-society relations and state-transnational linkage). This "domestic realm focus" affects the state's identity, interest, and behaviour (Hobson, 2000, p. 167).

Table 1. Theoretical Framework of Social Constructivism Proposed

Objectives	**Tenets**	**Referent Data**	**Japan**	**South Korea**
What do digital divide and cybersecurity mean for Japan and South Korea?	Normative Structure	International Realm		
		Domestic Realm		
How do Japan and South Korea interpret their own identities and roles in the context of international cybersecurity cooperation?	Identity	Role(s)		

What motivates Japan and South Korea in implementing international CCB assistance?	Interests	Material		
		Normative		
How do Japan and South Korea similarly and differently implement international CCB assistance?	Policy or Behaviour (CCB orientation, dimension, and activity)	Non-security	Cybersecurity education, training, and skills	Training
				Others
			Standards, organizations, and technologies	Research
				Technology Transfer
				Others
			Cyber culture and society	Information sharing & Best practices
				Promotion of development awareness
				Others
		Security	Legal and regulatory frameworks	Cybercrime & Cyber-operation
				Legal & Judicial Development
				Others
			Cybersecurity Policy and Strategy	Military
				Policy and Strategy
				Security System Management and Reform
				Cyber-exercise
				Others

Source: Author

This study aims to combine both variants by integrating the "international realm" variable with the "domestic realm" variable and framing them as a new normative structure. This structure concerning international cybersecurity governance and cooperation affects the state's identity, interest, and behaviour in international CCB assistance. Table 1 illustrates this paper's analytical framework operationalisation.

RESEARCH METHOD

This study follows what David L. Morgan (2007, p. 67), Thi Tuyet Tran (2017), and John W. Creswell (2013, pp. 9-10) termed a "pragmatic-constructivist" research paradigm. It seeks

the "middle ground" of tension between the objectivity of observable phenomenon of CCB as international assistance as part of inter-state behaviours (e.g., the network of actors, institutions, material capabilities) and its inherent tendency to be driven by "non-material/intangible factors" (e.g., norms, identities, and ideas). It manifests in a case-based comparative analysis design, which tries to compare a limited number of cases in return for more exploration of numerous "variables" to thicken the description. The definitive conceptualisation or theorisation within the research is constructed simultaneously with the research progress, and the case selection would be very paradigmatic according to the research purpose (della Porta, 2008, p. 208).

There are several reasons behind the selection of Japan and South Korea in this study. First, this research attempts to make a breakthrough by departing from mainstream studies in the field whose focus is on Western cybersecurity profiles—e.g., US, UK, European Union (EU), Council of Europe (CoE), Russia, and others. Second, according to Global Cybersecurity Index (GCI) in 2018, ITU (2019a, pp. 14, 62) categorised Japan (with GCI 0.880) and South Korea (with GCI 0.873) as countries with a "high-level commitment" toward cybersecurity. The third is that Japan and South Korea, as developed countries, have strong traditions of being donor countries. Their membership status within the OECD-DAC (OECD, 2021) and their respective reputable international cooperation agencies—Japan International Cooperation Agency (JICA) and Korea International Cooperation Agency (KOICA)—support the premise.

This research obtained data that consisted of two referent sets: (1) the general national cybersecurity profile of Japan and South Korea and (2) international CCB assistance activities/programmes/projects conducted by Japan and South Korea. The data are primarily qualitative from primary or secondary sources (see Table 2) found through desk-study activity (Lamont, 2015, pp. 79-91). The method of the data analysis will be qualitative, with a tendency to go to both content and discourse analysis (Johannesson & Perjon, 2014, p. 65). The data will be positioned and analysed based on this paper's analytical framework and writing structure.

Table 2. List of Referent Data Proposed

Referent Data like…	That indicate…	To find…	In the form of … that can be found in…
Cybersecurity Profile	Policy/Strategy Institution Actor/Agency Mapping Public Discourse or Narrative	• Norm • Identity • Interest	• Official documents o National government websites o International organization website (e.g.: UNIDIR) • Archives o Catalogue (e.g.: Cybil.org) • Media report o Journalistic website • Academic sources o Books, journal articles, research reports, etc. • Other web-based information source
International CCB Assistance Activity / Program / Project	Resource transfer—(in)tangible From donor country's government or official agency Toward recipient country as developing one in sense of both economic development and ICT advancement	• Behaviour	

Source: Author

DISCUSSION

Structuring The Meaning Of The Digital Divide And Cyber-Norms

International-level Normative Structure

Japan and South Korea have several similarities in their international normative structure. First, both countries are active participants of UN GGE. Both countries and other participants managed to formulise eleven voluntary, non-binding norms, rules, or principles of responsible behaviour of states to promote an open, secure, stable, accessible, and peaceful ICT environment (UN GGE, 2013; 2015; UN General Assembly, 2021). Out of eleven cyber-norms, three address the importance of international cooperation in tackling the digital divide: (1) cooperation in increasing stability and security in the use of ICTs; (2) consideration of how best to cooperate against cybercrime; (3) responding to appropriate requests for assistance by another State whose critical infrastructure is vulnerable. These cyber norms simultaneously "teach" UN member states, including Japan and South Korea, to participate in international cybersecurity cooperation, particularly international CCB assistance, to narrow the digital divide.

Second, both countries are active members of ITU, an UN-backed ICT agency. Membership in ITU has "encouraged" countries like Japan and South Korea to prioritise conducting CCB cooperation, particularly with developing countries. It is shown by two ITU events regarding spam-combating and computer incident response teams (CIRTs) facilitation

worldwide: World Telecommunication Development Conference (WTDC) and World Telecommunication Standardization Assembly (WTSA) (ITU, 2021). Third, both are the only Asian countries that have become members of OECD-DAC. Such memberships oblige Japan and South Korea, two developed nations, to actively participate in ODA. OECD-DAC members recommend international CCB assistance as one of the development agendas to facilitate cybersecurity cooperation at policy and operational levels across political, economic, and social issues (OECD, 2012, pp. 51, 72).

However, Japan has become a member of the Convention on Cybercrime, also known as the Budapest Convention (Council of Europe, 2021), while South Korea is not a party to the Convention. It is the first international treaty to address cyber-related crime, cyber-terrorism, and cyber discrimination by harmonising national laws, improving investigative techniques, and increasing cooperation among nations (Council of Europe, 2001; Schmitt, 2017). By being a party to the Convention, Japan's cybersecurity governance is becoming security-oriented. The Budapest Convention influences Japan's cybersecurity paradigm to be more oriented towards traditional security. Unlike Japan, traditional security is not the determinant for South Korean norms on cybersecurity governance and international CCB assistance.

Japan's Perceptions of the Digital Divide and Cyber-Norms

The Japanese perspective on the digital divide combines infrastructural and socio-economic (i.e., intergenerational) perspectives. The problem of the digital divide Japan is experiencing is caused by the fact that internet penetration in Japan is centralised in Honshu Island (Nishida, Pick, & Sarkar, 2014, pp. 1000-1003). Moreover, the number of older people using the internet is far fewer than the younger population (Chen & Wellman, 2004, p. 23; Nishida, Pick, & Sarkar, 2014, p. 1009). Despite an initial increase in broadband access by the Japanese Government, the intergenerational digital divide is yet to be solved.

Japan's cybersecurity governance is state-led. There are two factors: strong state guidance and weak-to-moderate societal ventures. Japanese cybersecurity governance is highly centralised under the Prime Minister of Japan and its Cabinet (Secretariat), Ministry of Defence (MOD), Ministry of Internal Affairs and Communication, Ministry of Justice,

Ministry of Economy, Trade, and Industry (METI), Ministry of Foreign Affairs (MOFA), Cyber Attack Analysis Council and National Public Safety Commission. Stefan Soesanto (2020, p. 30) said that these governmental bodies create more innovation in cybersecurity governance than private sectors or civil society. On the other hand, the role of private or civil society is weak and less self-incentivised. Japanese business leaders lack the technical expertise and experience necessary to make good cybersecurity decisions (Matsubara, 2018). They view cybersecurity as corporate social responsibility practice instead of an asset or investment to improve competitiveness (Matsubara, 2018).

Norms regarding cybersecurity governance adopted by the Japanese Government are also highly securitised for two reasons. First, the Japanese governmental bodies previously mentioned are all elites of the Japanese "security community" and "intelligence community." Despite the presence of METI in the policy-making process, its influence is still undermined by the higher government bodies like the Ministry of Defence and the National Public Safety Commission (Soesanto, 2020, pp. 20, 22-24). Consequently, policy areas specialised by Japan's cybersecurity governance are mainly around cybercrime, cyber terror, and cyber defence. Japanese cybersecurity strategy and laws reflect what Lene Hansen and Helen Nissenbaum (2009, pp. 1163-1165) refer to as "hyper-securitisation." The Japanese security community used past cybercrime events, cyber terrorism, and cyber defence incidents and even imagined the worst cyber-threat scenario to justify the sophisticated evolution of national cybersecurity strategy. They evolved from the 2000 Basic Act and Special Action Plan to two National Strategies on Information Security to three Cybersecurity Strategies between 2013 and 2018, introducing the Basic Act on Cybersecurity in 2014. Japanese cybersecurity governance also refers to National Defence Guidelines and Japan-US Defence Guidelines to narrate a "toward-militaristic" approach to cybersecurity (Soesanto, 2020, pp. 12-17, 24-25).

Second, geopolitically speaking, Japan expands its "defence perimeter" in cyberspace to cover neighbouring actors, both states and regional organisations, while avoiding a direct cyber-dialogue with China. Japan-ASEAN CCB cooperation becomes an instrument to foster the Japan-ASEAN security community and environment amidst the growing cyber threat from China (Larasati, 2018, pp. 92-93). The trilateral meeting between US, Japan, and South

Korean vice foreign ministers on cybersecurity policy coordination and cooperation also responds to the growing threat of North Korea in terms of nuclear weapons as well as other security issues. The meeting addressed issues of critical infrastructure, cyber-threats, and cyber-trend (US Embassy and Consulate in the Republic of Korea, 2017). The expansion of Japan's cooperation toward Europe, for example through the Japan-EU Cyber Dialogue in 2014, follows the same logic. Third, there is a growing trend of Japan militarising its response toward cyber threats. Japanese MOD and SDF have developed a cyber doctrine for domestic defence and increasingly international cooperative purposes (Kallender & Hughes, 2017, p. 129). Japanese MOD (2010, pp. 184-185) issued a White Paper announcing the 'Six Pillars of Comprehensive Defence Against Cyber Attacks,' which emphasises digitalising military defence capabilities against any cyber-related threat.

In short, Japan's security-oriented cybersecurity governance at the domestic level and cooperative approach and security orientation on cybersecurity influence Japan's normative structure for international CCB cooperation to be security-oriented.

South Korean Perception of the Digital Divide and Cyber-Norms

The socio-economic perspective has dominated South Korea's experience with the digital divide. Its digital divide seems to be increasing along the lines of income and education (Chen & Wellman, 2004, p. 23). Despite the 97% rate of national internet penetration in January 2021 (Kemp, 2021), the rate for the physically disabled, elderly, people living in rural areas, and low-income earners is far slower (Yonhap News Agency, 2020). Moreover, the deployment of ICTs in the various socio-economic frameworks, such as education, happens because Korea has limited natural resources and depends on a knowledge-based economy to remain economically viable and competent (Sedimo, Bwalya, & Plessis, 2011).

Although societal-cultural acceptance towards the Government's intervention in ICT infrastructure advancement in South Korea is high, South Korea's perception of other forms of Government cyberspace intervention is different. Concerning its state-society relations in cybersecurity governance, South Korea's national institution consists of moderate state intervention with moderate-to-strong societal hesitation. Three factors explain this situation. First, public-private partnership in South Korean cybersecurity governance is minimal (Kim

D. , 2019, pp. 79-80). Second, South Korea's administrative system and legal framework in cybersecurity affairs are scattered without the proper mechanism to integrate them into a more unified governance. There are many governmental bodies including the National Cyber Security Centre (NCSC) under the National Intelligence Agency (NIA), Korean Internet and Security Agency (KISA) under the Ministry of Science and ICT (MSIT), Cyber Command under the Ministry of National Defence (MND), and Cyber Bureau under National Police Agency (KNPA). There are also three sets of complex laws on the internet and information security in Korea: laws on promotion of the internet and the internet industry, laws on cybersecurity, and laws on personal information protection (KISA, 2021). However, South Korea's scattered and inadequate cybersecurity policies/bodies resulted in difficulties in deterring North Korea (Park P. , 2018; Kim D. , 2019, p. 58). Third, South Korean Government's effort to incorporate civil society to support and champion cybersecurity governance advancement is difficult. South Korean civil society, in general, is suspicious of any South Korean policy that aims to regulate the public sphere that, in general, is supposed to be an open, accessible, and democratic domain. Such fear is justified based on the history of South Korean authoritarianism around the 1970s and 1980s regarding civil surveillance and domestic political interference (Park D. , 2016).

Norms regarding cybersecurity governance in South Korea are a mixture of security-oriented and economic development-oriented. South Korea's cyber defence to deter the imminent threat, mainly from North Korea and China, and the presence of a "security community" that holds responsibility for governing cybersecurity, such as NCSC, KISA, NCC, and Cyber Bureau, strengthen the notion of security orientation (Bartlett, 2018, p. 29). However, the degree of securitisation of South Korean cybersecurity is not as high as Japan. The main factor lies in the competing economic development orientation of cybersecurity governance. MSIT, playing a vital role in South Korean cybersecurity governance, represents the national legacy of economic and financial guidance and bureaucratic-political interest in promoting South Korean science and technological advancement. "National legacy" means a political-economic culture during the 1970s-1980s that played a "stronger" interventionist role, relying more on top-down orders (Bartlett, 2018, pp. 30-31). The "bureaucratic-political interests" mean that MSIT's aim to assure South Korea's cybersecurity policy can promote

South Korean science and technological advancement which would also serve the interests of the ICT industries (Kim D. , 2019, p. 68; Bartlett, 2018, pp. 31-32).

In short, South Korea has fostered a "developmental" orientation of cybersecurity governance while embracing a cooperative-with-low-securitisation approach to cybersecurity and CCB. These made the South Korean normative structure for international CCB cooperation "developmental."

Defining Identities And Roles Within The Context Of International Cybersecurity Cooperation

Japan's Identity and Role Conception in International Cybersecurity Cooperation

It is generally agreed that Japan's international identity changed from a pre-war "warmonger" nation to a post-war "pacifist" one. Pre-war Japan held several identities, such as "militarist" and "authoritarian," "imperialist," and "aggressor" or "bullying country" or "a strong country" (Katzenstein, 1996; Hobson, 2000, pp. 167-169; Hagström & Gustafsson, 2015, p. 9). All those identities and role enactment dramatically changed after the defeat of Japan in World War II. The rest of the twentieth century saw a slow yet incremental reverse of those identities and roles to become a "post-war pacifist" Japan: "anti-militarist," "economic power," "developmental state," a "cooperative" member of the international community, and "weak" at some point (Tonami, 2018, pp. 1211-1212; Kono, 1999; Yasushi & McConnell, 2008; Hagström & Gustafsson, 2015, pp. 12-14). The contemporary period of Japan's international relations, particularly during the second term of Prime Minister Shinzo Abe (2012-2020), witness another change in Japan's identity within international politics. This study proposes the term "revisionist" identity, inspired by Abe's effort to reinterpret Article 9 of the Japanese Constitution to benefit the Japanese SDF's remilitarisation. He embraced this kind of identity to seek a balance between two previous contrasting identities. He tried to present Japan as a nation that is (1) "cooperative" yet "assertive," (2) "strong" yet "not a bully," and (3) becoming a "military and economic power" yet "democratic and human rights champion."

By linking the pertinent evolution of Japan's identity with the context of international cybersecurity cooperation, the security-oriented normative structure has shaped Japan's

identity/role into a "responsible global cybersecurity stakeholder" in promoting peaceful and secure global cyberspace. Through bilateral and multilateral cyber diplomacy, Japan has become one of the responsible countries in shaping international collective action to ensure a free, fair, and secure cyber-space (Matsubara & Mochinaga, 2021, p. 25). To be "responsible" globally, Japan needs to be "digitally strong" as a regional and global cyber power. As the cyber threat is growing and even militarised, strengthening cyber defence capabilities is a viable option for Japan. It mainly deters advanced persistent threats (APTs) to Japanese cyberspace from China, North Korea, and Russia (NIDS, 2014, pp. 52-53). Moreover, due to its "cooperative/assertive" identity/role that cannot be achieved alone, Japan needs to embrace international cybersecurity cooperation. Such an urgency has been supported by Japan's reputation for being a country with high capabilities of being a partner and even donor in much international cooperation and assistance and a thrust to become a globally responsible cybersecurity stakeholder (Menocal, 2011).

In short, Japan's security-oriented international cybersecurity cooperation normative structure combined with previously discussed "revisionist" identity and role in foreign policy results in Japan's strive for the following identity and role within international cybersecurity cooperation: a "cyber-power" with urgency and responsibility to contribute towards peaceful and secure global/regional cybersecurity on behalf of Japan's security interests.

South Korean Identity and Role Conception in International Cybersecurity Cooperation

South Korea was initially a minor power. The most popular proverb to describe South Korea's position within international politics is "a shrimp among whales," describing its role in the past as the geopolitical pivot for great power politics throughout history (Park S. J., 2015, p. 3). South Korea was also a "developing nation" due to its identity as an "international development beneficiary nation" of ODA by OECD. After the 1990s democratisation and post-1997-crisis national economic development consolidation, South Korea has become more stable internally.

Scholars like Heike Hermanns (2013), Jongryn Mo (2016), Leif-Eric Easley & Kyuri Park (2017), Moch Faisal Karim (2018), Patrick Flamm (2019), Sook-Jong Lee (2012), and Jeffrey Robertson (2007) agreed that South Korea has transformed into a middle power.

Flamm (2019, pp. 136-141) identified three identities/roles of South Korea as a middle power: "Rising Korea," "Leading Korea," and "Righteous Korea." "Rising Korea" indicates South Korea's rising role in international relations. The roles derived from such identity range from being a "bridge between worlds," "responsible middle power," and "economic power." Starting from President Roh Tae-woo's pursuit of South Korean status as a "mediator" between developing and developed countries or Western and Non-Western countries (Karim, 2018, p. 356), South Korea aims to become a "responsible middle power." In doing so, President Lee-Myung-bak's terminology of "Global Korea" in harmonising its interests with other global actors (Lee M.-b. , 2009) and South Korea's recent economic prowess become the foundation for "Rising Korea." "Leading Korea" means South Korea wants to be a global role model (Flamm, 2019, pp. 138-140). Combined with the "Global Korea" identity, it refers to South Korea's national image and brand-building and exportation of South Korean culture to a global audience. People-oriented soft power diplomacy is vital for South Korea's global popularity—e.g., Hallyu and the innovation model (Hermanns, 2013, pp. 75-76; Jamrisko & Wei, 2020). "Righteous Korea" refers to South Korean international identity/role as a "peaceful and cooperative" nation contributing towards world peace, security, and order (Flamm, 2019, pp. 140-141). Its role enactment involves South Korea's activism in international cooperation—whether it is security issues or economic development and cooperation issues—and becoming an agenda-setter (Mo, 2016, p. 594). For example, South Korea successfully changed its "beneficiary" status to a "benefactor" and "developed country" identity by joining OECD-DAC High-Level Forum on Aid Effectiveness in 2011. The forum founded the Busan Partnership Agreement for Effective Development Co-operation (OECD, 2011).

If we link South Korea's identity evolution with its normative structure of international cybersecurity cooperation that is "developmental," we can see that the identity of "Rising Korea" has shaped South Korea's identity into one of the "world ICT leaders." It was testified by ITU (2018) while describing how government interventions and investments in modern technology since the 1950s have been responsible for South Korean recent digital economic boom. The international community expects South Korea, now leading the world's ICT advancement, to play a contributive role in the cybersecurity sector (Kim S. , 2014, p.

324). From the "Leading/Rising Korea" identities, there are three recognisable roles: "strong internet nation," "pioneer of the digital "new deal," and a "leader in cyber-diplomacy." South Korea is home to several giant ICT corporations, such as Samsung, LG, SK, and KT, the fastest internet connection in the world (Pulse, 2020), a global pioneer for a "digital new deal," according to President Moon Jae-in (2020), and a reputable country for its e-Government. South Korean cyber diplomacy is directed into two segments of the "Righteous Korea" identity/role. The first one is to incorporate South Korean cultural assets with their diplomatic goals to promote the national brand/image to the global audience. In this context, South Korea is better than Japan in incorporating its cultural assets with its diplomatic goals in the international community (Park, Chung, & Park, 2019, p. 1481). The second one is cyber diplomacy to set the agenda of international cybersecurity cooperation, such as promoting peaceful and secure global cyberspace, mediating cyber conflicts, and other forms of cybersecurity cooperation, namely international CCB assistance.

In short, South Korea's "developmental" international cybersecurity cooperation normative structure combined with its "middle-power" status results in the following identity and role within international cybersecurity cooperation: a "cyber middle power" for the mutual development of the international community's cyber capabilities.

Explaining Interests In Motivating International CCB Assistance

Japan's Motives

Japan's normative structure, identities, and roles in international cybersecurity governance discussed in the previous section contribute to Japan's normative and material interests in conducting international CCB assistance. There are three normative interests (Vosse, 2019, p. 3). First, Japan wants to ensure that the international community approaches international cybersecurity governance through multilateral and bilateral partnerships. Second, Japan aims to proliferate the norms of cooperative approach in building cyber capacity towards recipient countries. Third, being the party to the Budapest Convention, Japan is obliged to govern its cyberspace with respect for democracy, human rights, and the rule of law. Japan explicitly combats any cyber related crime within its cyberspace and within its capacity. Consequently,

Japan aspires to ensure that other countries follow a similar path as active players in international cybersecurity governance.

There are several material drivers for Japan's international CCB assistance. The first is related to "prestige." Conducting international CCB assistance will help Japan build such an image in which recipient countries will perceive Japan as a role model in CCB that should be followed and preferred for future CCB projects. Second, in terms of "politico-diplomatic" concerns, international CCB assistance is a good option for Japan's confidence-building measures (CBMs) (Maiese, 2003). It means that if Japan cooperates and even assists developing countries in building cyber capacity, Japan's own cyber capabilities will not be feared even if Japan's cybersecurity is getting militarised. Third, regarding "security" consideration, Japan considered international CCB assistance as an instrument to promote a better way to build cybersecurity capacities following what donors idealise as "peaceful and secured cyberspace." Because Japan's national cybersecurity depends on international dynamics, helping other countries build their cyber-capacity will also strengthen Japan's national security. Lastly, in terms of "commerce," if Japan helps CCB in developing countries, it can simultaneously promote it socio-economic development and create a market for foreign economies. Moreover, international CCB assistance allows Japan to export its defence mechanisms to other countries.

South Korean Motives

Like Japan, South Korea's international CCB assistance has its normative and material components that constitute its interests worldwide. In terms of normative components, South Korea's international CCB assistance aims to promote international partnerships and cooperation in cybersecurity by enriching prevalent bilateral and multilateral cooperation systems (National Security Office of the Republic of Korea, 2017, p. 23). The international community, including the UN GGE and UN OEWG, has "taught" South Korea to conduct CCB cooperation with other countries to develop cyber capacities together and reproduce the cyber-norms toward other countries (Ebert & Groenendaal, 2020, p. 25). South Korea's international CCB assistance also promotes developmental norms. South Korea is committed to conducting CCB assistance toward other countries to narrow the digital gap that results in

cyber risks, poverty, and economic stagnation (Ebert & Groenendaal, 2020, p. 23; Hohmann & Pirang, 2017).

There are also South Korea's material interests in international CCB assistance: "security," "prestige," and "politico-diplomacy." Like Japan, South Korea's cybersecurity profile is enmeshed in Asia-Pacific dynamics, involving considerable risk of cyberconflict with technically advanced countries like China, North Korea, and Russia and the prevalence of regional disputes. By conducting CCB assistance towards recipient countries nearby, South Korea can geopolitically assure its cybersecurity within the region from any cyber-related risk from the external realm. Nevertheless, "security measures" do not necessarily affect or shape its normative interest like Japan. Because it is not a party to the Budapest Convention, South Korea does not internalise security-oriented cybersecurity governance, let alone CCB. Instead, it creates a more "developmental" orientation. In terms of "prestige," South Korea's National Security Office (2017, p. 24) aims to expand foreign assistance projects for cybersecurity capacity building to developing countries in a reciprocal manner and share cybersecurity technologies and systems. By conducting CCB assistance with other countries, South Korea aims to enact its "Global Korea" role in CCB governance and build a reputation as an international role model for CCB governance. In terms of "politico-diplomatic" interests, international CCB assistance can be used to make issue linkage. South Korea's ODA combines non-traditional security concerns, such as development, with cybersecurity (Kim S. , 2014, p. 7). In collaboration with the World Bank, one obvious result of South Korea's cyber diplomacy is to establish two CCB assistance projects: "Combatting Cybercrime: Tools and Capacity Building for Emerging Economies" and "Global Cyber Security Capacity Program."

The Practice Of International CCB Assistance

An Explanation for Japan's Performance

Around 24 projects of Japan's international CCB in the region take all forms, except technology transfer, legal and judicial development, and military. Although Japan's material interests in providing international CCB assistance include "security" considerations, securitising and militarising cyber-related issues are sensitive, especially for its Southeast

Asian (SEA) counterparts. Henceforth, Japan's approach in conducting security-oriented CCB programmes focuses more on legal and regulatory frameworks and comprehensive policy and strategy. Nevertheless, Japan's security-oriented CCB programmes for its recipients ranges from cybercrime eradication and cyber-operations policy and strategy development (MOFA Japan, 2019; 2019; GFCE, 2016; INTERPOL, 2018; NISC, 2015; 2018), to security system management and reform (ASEAN, 2016, p. 4; ICT4Peace, 2018; JICA, 2013; 2019a), and even cyber exercise (ID-SIRTII/CC, 2017; AJCCBC, 2018; JAIF, 2018; METI Japan, 2020; Tajima, 2020). Meanwhile, Japan's non-security-oriented CCB projects focus on cybersecurity education, training, skills, standards, organisations, technologies, and cyberculture and society. They include training (NISC, 2015; JICA, 2018; 2019b; 2020; METI Japan, 2021), research (Laskar & Sarkar, 2020), information and best practices-sharing (NISC, 2015), and promotion of ICT development awareness (NISC, 2015).

The ratio between security-oriented and non-security-oriented projects is fifteen to nine. Most of the projects are conducted through engagement between Japan's cyber security bodies and their counterparts, proving the linearity of security-oriented approach with its material and normative interests, identity/role, and normative structure.

An Explanation for South Korean Performance

South Korea has around sixteen international CCB projects without forms of technology transfer, legal and judicial development, security system management and reform, cyber-exercise, and military. The recipient countries are diverse, ranging from the Balkans to African countries. The projects are mostly integrated and institutionalised under collaboration with international organisations. Take cybercrime eradication & cyber operations as an example. Through its National Police Agency (KNPA), the South Korean Government will fund INTERPOL projects around EUR 4.4 million to combat cybercrime, including child sexual abuse and cyber-enabled financial crime (INTERPOL, 2020). However, South Korea does not fully participate in the programme's technical and operational affairs.

Another example is the "Global Cybersecurity Capacity Program" (GCCP). It is an initiative taken by the World Bank and financed by the South Korean Government through a scheme called the Korea World Bank Partnership Facility (KWPF) to bridge existing gaps in the cybersecurity capacities of its client countries. GCCP took limited forms of CCB assistance, such as training (World Bank, 2019, pp. 21-57), information sharing and best practices (World Bank, 2019, p. 50), promotion of development awareness (World Bank, 2020), and policy and strategy (World Bank, 2019, p. 43) They were conducted in two phases: "Phase I" and "Phase II." In its "Phase I," the programme has assisted six countries—Albania, Bosnia and Herzegovina, the Republic of North Macedonia, Ghana, Kyrgyzstan, and Myanmar—in strengthening cybersecurity capacities between 2016 and 2019 (World Bank, 2019, p. 4). Its "Phase II" will engage other countries like Kosovo, Serbia, and more in 2020-2021 (World Bank, 2020).

Outside the GCCP framework is the Korea-Indonesia ICT Training Centre for technology transfer (Embassy of the Republic of Korea for the Republic of Indonesia, 2011). South Korea established a cybersecurity centre at the Bandung Institute of Technology to research and promote development awareness (Kusumastuti, 2015). It is similar to ASEAN Cyber University which is also South Korean programme (ACU Project, 2012). South Korea also cooperate with China and India on information and best practices-sharing, particularly in CIRTs (Hitchens & Goren, 2017, pp. 70, 99).

The ratio between security-oriented and non-security-oriented projects is fourteen to two. It proves that the South Korean approach to CCB projects is less security-oriented. Instead of cyber security bodies, they engaged more with economic and development institutions in conducting the projects. Henceforth, South Korea's performance in international CCB assistance established the "developmental notion" and consistent with its normative structure, identity/role, and material-normative interests.

Additional Discussion

Table 3 summarises the previously discussed comparison between Japan's and South Korea's international CCB assistance over the last decade based on their project quantity, orientations, dimensions, and forms. It collects any international CCB project that shows two

attributes: (1) any resource transfer related to CCB assistance activities, tangible or intangible, from Japanese and South Korean Governments or official agencies and (2) the status of recipient countries, which can be considered developing if measured by their economic development and ICT advancement. They reflect policy orientation or behaviour related to international CCB assistance. Therefore, both countries' engagement with, for example, China and India, despite the latter's economic prowess, still counts in this manner.

Table 3. Comparative List of Japan and South Korea's International CCB Projects

Orientation	Dimensions	Forms	Japan	South Korea
Non-security	Cybersecurity education, training, and skills	Training	• The 1st ASEAN-Japan Information Security Training (Tokyo, 23 - 27 August 2010) • Project on Capacity Building for Cyber Security in Vietnam (26 June 2019 – 25 November 2021) • Project for Human Resources Development for Cyber Security Professionals (22 May 2019 – 21 May 2024) • Japan - US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region in FY2020—in cooperation with US DHS (8-12 March 2021, Online) • Capacity Building in Policy Formation for Enhancement of Measures to Ensure Cybersecurity in ASEAN Region (January-February 2020)	• Korea-Indonesia ICT Training Centre (since 2011) • GCCP (Technical Assistance & Workshop) in Kyrgyzstan (Bishkek on 25-26 April 2018) • GCCP (Workshop) in North Macedonia (Skopje, 2-3 April 2018) • GCCP (Workshop) in Bosnia and Herzegovina (Sarajevo, 3-4 December 2018)
	Standards, organisations, and technologies	Research	• India-Japan Finalisation of 5G and AI cooperation (October 2020)	• Cybersecurity Centre in Indonesian University (since 2015)
	Cyber culture and society	Information sharing & best practice	• The 1st ASEAN-Japan Information Security Policy Meeting (Tokyo 24 - 26 February 2009)	• GCCP (Seminar) in Albania (Tirana, 6-7 December 2018) • MoU between South Korea's Ministry of Science,

				ICT & Future Planning, and China's Ministry of Industry and Information Technology (January 2014) • MoU between Korean and Indian CERT (16 January 2014)
		Promotion of development awareness	• The 2nd ASEAN-Japan Government Network Security Workshop (Hanoi, 16 - 17 December 2010) • ASEAN-Japan Joint Information Security Awareness Raising Initiatives (November 2011)	• ASEAN Cyber University (since January 2009) • GCCP (Seminar) in Ghana (since 2019) • GCCP (Seminar) in Myanmar (since 2019) • GCCP (Seminar) in Kosovo (since 2019) • GCCP (Seminar) in Serbia (since 2019) • GCCP (Seminar) in Montenegro (since 2019)
Security	Legal and regulatory frameworks	Cybercrime eradication & cyber-operation	• The 3rd ASEAN-Japan Cybercrime Dialogue (Bandar Seri Begawan, 23-24 January 2019) • Countermeasures Against Cybercrime by JICA 2015 • Preventing and Combating Cybercrime in Southeast Asia—in cooperation with GFCE and UNODC (since 2016) • ASEAN Cybercrime Operations Desk—in cooperation with INTERPOL (July 2018) • Agreement between CERT India and Japan Computer Emergency Response Team Coordination Centre (JPCERT/CC) (January 2015)	• Korean Fund for INTERPOL's Fight Against Child (Sexual) Exploitation (FACE) project & cyber-enabled financial crime (2020)
	Cybersecurity policy and strategy	Policy and strategy	• The 1st ASEAN-Japan Government Network Security Workshop (Tokyo, 21 - 22 October 2009) • The 2nd & 3rd ASEAN-Japan Information Security Policy Meeting (Bangkok 29 - 31 March	• GCCP (Technical Assistance) in North Macedonia (Skopje, 2-3 April 2018)

		2010; Tokyo, 7 - 8 March 2011) • Annual CIIP Workshops in ASEAN (20 October 2016) • International Cyber Security Policy and Capacity Workshop for ASEAN Countries—in cooperation with UK and ICT4Peace Foundation (April 2017 - March 2018)	
	Security system management and reform	• ASEAN – Japan Cybersecurity Working Group/Policy Meeting (Tokyo, 16-17 October 2018) • Improvement of Information Security Response Capacity in Indonesian Government (23 July 2014 - 22 January 2017) • ANC-JICA-Id-SIRTII Cyber Security Seminar—in partnership with Indonesia (Dili, 8 February 2019) • [The Establishment of the] ASEAN-Japan Cybersecurity Capacity Building Centre [and its "Step 2] (Bangkok, 2018)	_
	Cyber-exercise	• Annual Cyber Exercises in ASEAN (March 2013- December 2021) • Japan-ASEAN0US-EU Cyber-defence drill (planned in 2020-2021)	_

Source: Author

Two caveats are important in this comparison. First, it excludes three forms of CCB projects—technology transfer, legal and judicial development, and military—because neither Japan nor South Korea conduct them. Second, it must be admitted that there are slight differences in comparing data from Japanese and South Korean practices. While data from the former mainly focused on cooperation with SEA counterparts, data from the latter show more diversity in terms of regional partners.

Such "unfair comparison" can be justified. Empirically speaking, Japan has more region-focused international CCB assistance than South Korea's, which is more diverse. Most of Japan's international CCB recipients come from the SEA region, namely ASEAN member states. It happens because Japan realises the importance of the region's cybersecurity capacity and its impact toward regional cybersecurity governance more than South Korea does. SEA have several issues regarding the digital divide, in terms of internet penetration (Ingram, 2020, p. 8; World Bank, 2021), digital gender gaps (ITU, 2019b, pp. 4, 6), unequal distribution of ICT skills (ITU, 2019b, p. 10), exploitable unsecured infrastructures (Raska & Ang, 2018, p. 2), insufficient strategic mindset, policy preparedness, and institutional oversight (Ingram, 2020, p. 18), business community's reluctancy to deal with cyber-risks, lack of human resources and infrastructures, and infancy of cyber-culture within society and state. In this case, Japan takes geopolitical measures into account more than South Korea does. Such findings are consistent with the initial analysis this study has explicated in previous sections, concerning the linearity between the normative structure, identities/roles, normative-material interests, and state policy (i.e., international CCB assistance). Therefore, the data difference precisely confirms the initial premises and analyses this study proposes.

CONCLUSION

Based on the conceptualisation of CCB as a practice of international assistance and social constructivism theory, this study concluded the role of normative structure, identity/role enactment, and interest configuration in shaping states' orientation in international CCB assistance. When specific normative structure—a combination of the international "realm of cybersecurity obligation" and domestic "realm of national cybersecurity institution"—interacts with the country's preceding identities and roles in general foreign policy, the process configures pertinent country's normative and material interests that genuinely drives a country to conduct international CCB assistance. Thus, the orientations, dimensions, and forms of activities/programmes/projects will manifest and reproduce the given normative structure and perceived identities/roles.

The two study cases from Japan and South Korea justify the argument. Japan's security-oriented normative structure in international cybersecurity has shaped Japan's

identity and role in international cybersecurity governance to be a country with security-dominant normative and material interests. Therefore, Japan's international CCB assistance has been highly security-oriented. Meanwhile, South Korea's "developmental" international cybersecurity normative structure embraces South Korea's well-known reputation in the international development realm so that the country puts more emphasis on the mixture of international CCB assistance with "developmental" normative and material interest. Henceforth, many programmes/projects of South Korea's international CCB assistance take a non-security orientation. Eventually, both countries reproduce different normative structures of international CCB assistance imposed on them in the first place. This comparison perfectly asserts the notion of fragmentation of global cyber-norms caused by a different process of perceiving them by countries worldwide.

ACKNOWLEDGEMENT

This study is a summarised version of the author's master's final thesis with a similar title for Corvinus University of Budapest. This achievement cannot be accomplished without the academic guidance by author's supervisor, Beáta Paragi, PhD, and financial support from the Stipendium Hungaricum Scholarship by Tempus Public Foundation.

BIBLIOGRAPHY

ACU Project. (2012). *History*. Retrieved April 19, 2021, from ACU Project: https://web.archive.org/web/20130409112925/http://aseancu.org/about/history.jsp

AJCCBC. (2018). *ASEAN-Japan Cybersecurity Capacity Building Centre*. Retrieved April 18, 2021, from https://www.ajccbc.org/

ASEAN. (2016, October 20). *CIIP Guidelines Ver. 3.0.* Retrieved April 18, 2021, from https://asean.org/wp-content/uploads/2012/05/01-CIIP-Guidelines-Ver3.0.pdf

Bartlett, B. G. (2018). *Institutional Determinants of Cyber Security Promotion Policies: Lessons from Japan, the U.S., and South Korea.* Berkeley: Graduate Division of the University of California, Berkeley.

Calandro, E., & Berglund, N. (2019). *Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance: the SADC case.* Retrieved January 26, 2021, from https://researchictafrica.net/wp/wp-content/uploads/2019/11/33_Calandro_Berglund_Unpacking-Cyber-Capacity-Building-1.pdf

Chen, W., & Wellman, B. (2004). The Global Digital Divide - Within and Between Countries. *IT & Society, 1*(7), 18-25.

Contreras, B., & Barrett, K.-A. (2020). Challenges in building regional capacities in cybersecurity: a regional organizational reflection. In E. Tikk, & M. Kerttunen (Eds.), *Routledge Handbook of International Cybersecurity* (pp. 211-214). London: Routledge.

Council of Europe. (2001, November 23). *Convention on Cybercrime*. Retrieved April 10, 2021, from Council of Europe: https://www.coe.int/en/web/conventions/full-list/-/conventions/rms/0900001680081561

Council of Europe. (2021). *Parties/Observers to the Budapest Convention and Observer Organisations to the T-CY*. Retrieved February 19, 2021, from https://www.coe.int/en/web/cybercrime/parties-observers

Crespo, L., Wanner, B., & Ghernaouti, S. (2018). Cybersecurity Capacity Building: A Swiss Approach. In M. Bartsch, & S. Frey (Eds.), *Cybersecurity Best Practices: Lösungen zur Erhöhung der Cyberresilienz für Unternehmen und Behörden* (pp. 525-538). Cham: Springer.

Creswell, J. D. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches.* Thousand Oaks: SAGE Publication.

della Porta, D. (2008). Comparative Analysis: Case-Oriented versus Variable-Oriented Research. In D. Della Porta, & M. Keating, *Approaches and Methodologies in the Social Science: A Pluralist Perspective* (pp. 198-222). Cambridge: Cambridge University Press.

Easley, L.-E., & Park, K. (2017). South Korea's mismatched diplomacy in Asia: middle power identity, interests, and foreign policy. *International Politics, 55*(2), 242-263.

Ebert, H., & Groenendaal, L. (2020). *Cyber Resilience and Diplomacy in the Republic of Korea: Prospects for EU Cooperation.* Paris: EU Cyber Diplomacy and Resilience Clusters.

Embassy of the Republic of Korea for the Republic of Indonesia. (2011, June 1). *Peresmian Balai Pelatihan dan Pengembangan Teknologi Informasi dan Komunikasi(Korea-Indonesia ICT Training Center)*. Retrieved April 19, 2021, from Kedutaan Besar Republik Korea untuk Republik Indonesia: https://overseas.mofa.go.kr/id-id/brd/m_2707/view.do?seq=659019&srchFr=&amp%3BsrchTo=&amp%3BsrchWord=&amp%3BsrchTp=&amp%3Bmulti_itm_seq=0&amp%3Bitm_seq_1=0&amp%3Bitm_seq_2=0&amp%3Bcompany_cd=&amp%3Bcompany_nm=&page=34

Finnemore, M., & Hollis, D. B. (2016). Constructing Norms for Global Cybersecurity. *The American Journal of International Law, 110*(3), 425-479.

Flamm, P. (2019). *South Korean Identity and Global Foreign Policy: Dream of Autonomy.* New York: Routledge.

GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM).* Oxford: Global Cyber Security Capacity Centre.

GFCE. (2016). *Preventing and Combating Cybercrime in Southeast Asia*. Retrieved April 18, 2021, from GFCE: https://thegfce.org/initiatives/preventing-and-combating-cybercrime-in-southeast-asia/

Grigsby, A. (2017). The End of Cyber Norms. *Survival, 59*(6), 109-122.

Hagström, L., & Gustafsson, K. (2015). Japan and identity change: why it matters in International Relations. *The Pacific Review, 28*(1), 2.

Hansen, L., & Nissenbaum, H. (2009). Digital Disaster, Cyber Security, and the Copenhagen School. *International Studies Quarterly, 53*(4), 1155-1175.

Henriksen, A. (2019). The End of the Road for The UN GGE Process: The Future Regulation of Cyberspace. *Journal of Cybersecurity, 5*(1), 1-9.

Hermanns, H. (2013). National Role Conceptions in the 'Global Korea' Foreign Policy Strategy. *The Korean Journal of International Studies, 11*(1), 55-82.

Hitchens, T., & Goren, N. (2017). *International Cybersecurity Information Sharing Agreements.* College Park: Center for International & Security Studies, University of Maryland.

Hobson, J. M. (2000). *The State and International Relations.* Cambridge: Cambridge University Press.

Hohmann, M., & Pirang, A. (2017, April 12). *Why Policymakers Should Care About Weak Digital Infrastructure Abroad*. Retrieved from Council on Foreign Relations: https://www.cfr.org/blog/why-policymakers-should-care-about-weak-digital-infrastructure-abroad

Hohmann, M., Pirang, A., & Benner, T. (2017). *Advancing Cybersecurity Capacity: Implementing a Principle-Based Approach.* Berlin: Global Public Policy Institute.

Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*, 224-242.

Hurwitz, R. (2014). The Play of States: Norms and Security in Cyberspace. *American Foreign Policy Interests: The Journal of the National Committee on American Foreign Policy, 36*(5), 322-331.

ICT4Peace. (2018, November 15). *International Cyber Security Capacity Building Program: Promoting Openness, Prosperity, Trust and Security in Cyberspace.* Retrieved April 18, 2021, from https://ict4peace.org/wp-content/uploads/2019/04/Cybersecurity-Policy-and-Diplomacy-Capacity-Building-15-Nov-2018.pdf

ID-SIRTII/CC. (2017, December 9). *Regional Security Awareness JICA*. Retrieved April 18, 2021, from ID-SIRTII/CC: https://idsirtii.or.id/kegiatan/detail_nama/multilateral_cooperation/53/regional-security-awareness-jica.html

Ingram, G. (2020, December 15). *Development in Southeast Asia: Opportunities for donor collaboration.* Retrieved April 24, 2021, from Brookings: https://www.brookings.edu/wp-content/uploads/2020/12/Development-Southeast-Asia-Ch2-Digital.pdf

INTERPOL. (2018, July). *ASEAN Cybercrime Operations Desk*. Retrieved April 18, 2021, from INTERPOL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations/ASEAN-Cybercrime-Operations-Desk

INTERPOL. (2020, February 11). *Korea to fund INTERPOL projects combating cyber-enabled crime*. Retrieved April 19, 2021, from INTERPOL: https://www.interpol.int/en/News-and-Events/News/2020/Korea-to-fund-INTERPOL-projects-combating-cyber-enabled-crime

ITU. (2018, February 12). *How the Republic of Korea became a world ICT leader*. Retrieved April 14, 2021, from ITU: https://news.itu.int/republic-korea-leader-information-communication-technologies/

ITU. (2019a). *Global Cybersecurity Index (GCI) 2018.* Geneva: ITU Publications.

ITU. (2019b). *Measuring digital development: Facts and figures 2019.* Geneva: ITU Publications.

ITU. (2020, November). *Key ICT indicators for developed and developing countries, the world and special regions (totals and penetration rates).* Retrieved Feburary 11, 2021, from https://www.itu.int/en/ITU-D/Statistics/Documents/facts/ITU_regional_global_Key_ICT_indicator_aggregates_Nov_2020.xlsx

ITU. (2021). *Mandate*. Retrieved April 10, 2021, from ITU: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/about-cybersecurity.aspx

JAIF. (2018, July 2). *ASEAN-Japan Cybersecurity Capacity Building Centre (Step 2)*. Retrieved April 18, 2021, from Japan-ASEAN Integration Fund: https://jaif.asean.org/project-brief/asean-japan-cybersecurity-capacity-building-centre-step-2/

Jamrisko, M., & Wei, L. (2020, January 18). *Germany Breaks Korea's Six-Year Streak as Most Innovative Nation*. Retrieved April 13, 2021, from Bloomberg: https://www.bloomberg.com/news/articles/2020-01-18/germany-breaks-korea-s-six-year-streak-as-most-innovative-nation

JICA. (2013, December 4). *Project on capacity building for information security*. Retrieved April 18, 2021, from JICA: https://www.jica.go.jp/project/english/indonesia/014/outline/index.html

JICA. (2018, December 11). *Project for Human Resources Development for Cyber Security Professionals*. Retrieved April 18, 2021, from JICA: https://www.jica.go.jp/project/english/indonesia/023/outline/index.html

JICA. (2019a, February 8). *ANC-JICA-Id-SIRTII conducted Cyber Security Seminar*. Retrieved April 18, 2021, from JICA: https://www.jica.go.jp/easttimor/english/office/topics/press190208_en.html

JICA. (2019b). *Project on Capacity Building for Cyber Security in Vietnam*. Retrieved February 19, 2021, from JICA: https://www.jica.go.jp/project/english/vietnam/052/index.html

JICA. (2020, February 7). *The first technical cooperation project implemented under the Japan-ASEAN Technical Cooperation Agreement -Making contribution to building up capacity to formulate policy to ensure cybersecurity in the ASEAN region*. Retrieved April 18, 2021, from JICA: https://www.jica.go.jp/english/news/press/2019/20200207_10_en.html

Johannesson, P., & Perjon, E. (2014). *An Introduction to Design Science.* Cham: Springer.

Kallender, P., & Hughes, C. W. (2017). Japan's Emerging Trajectory as a 'Cyber Power': From Securitization to Militarization of Cyberspace. *Journal of Strategic Studies, 40*(1-2), 118-145.

Karim, M. F. (2018). Middle power, status-seeking and role conceptions: the cases of Indonesia and South Korea. *Australian Journal of International Affairs, 72*(4), 343-363.

Katzenstein, P. J. (1996). *Cultural Norms and National Security.* Ithaca: Cornell University Press.

Kemp, S. (2021, February 11). *Digital 2021: South Korea*. Retrieved April 9, 2021, from DataReportal: https://datareportal.com/reports/digital-2021-south-korea

Kim, D. (2019). *Restructuring the National Cybersecurity Governance System in South Korea: Critical Information Infrastructure.* Seoul National University, Graduate School of International Studies. Seoul: Graduate School of International Studies, Seoul National University.

Kim, S. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studies, 12*(2), 323-352.

KISA. (2021). *Laws on the Internet and Information Security of Korea.* Seoul: KISA.

Klimburg, A., & Zylberberg, H. (2015). *Cyber Security Capacity Building: Developing Access.* Oslo: NUPI.

Kono, Y. (1999). *Myth and Reality: Why Japan Strives For Multilateralism*. Retrieved April 10, 2021, from Ministry of Foreign Affairs of Japan: https://www.mofa.go.jp/announce/fm/kono/speech0101.html

Kusumastuti, L. W. (2015). *ITB-Korea Stregthen Cooperation in Cyber Security*. Retrieved February 19, 2021, from Institut Teknologi Bandung: https://www.itb.ac.id/news/read/4728/home/itb-korea-stregthen-cooperation-in-cyber-security

Lamont, C. K. (2015). *Research Methods in International Relations.* London: Sage.

Larasati, A. I. (2018). ASEAN-Japan Contribution to Regional Security: Cybersecurity Capacity Building (2014-2017). Bekasi: President University.

Laskar, R. H., & Sarkar, S. (2020, October 7). *India, Japan finalise key cyber-security deal to boost cooperation on 5G, AI*. Retrieved April 18, 2021, from Hindustan Times: https://www.hindustantimes.com/india-news/india-japan-finalise-key-cyber-security-deal-to-boost-cooperation-on-5g-ai/story-WCMa9En3NFPkQMWClGNFJI.html

Lee, M.-b. (2009, September 23). *Address by H.E. Mr. Lee Myung-bak President of the Republic of Korea, 64th Session of the.* Retrieved April 13, 2021, from http://www.un.org/ga/64/generaldebate/pdf/KR_en.pdf

Lee, S.-j. (2012). *South Korea as New Middle Power: Seeking Complex Diplomacy.* Seoul: East Asia Institute.

Maiese, M. (2003, September). *Objectives of Confidence-Building Measures*. Retrieved April 16, 2021, from Beyond Intractability: https://web.archive.org/web/20130908031946/https://www.beyondintractability.org/essay/confidence-building-measures

March, J., & Olsen, J. (1989). *Rediscovering Institution.* New York: Free Press.

Matsubara, M. (2018, June 4). *How Japan's New Cybersecurity Strategy Will Bring the Country Up to Par With the Rest of the World*. Retrieved April 10, 2021, from Council on Foreign Relations: https://www.cfr.org/blog/how-japans-new-cybersecurity-strategy-will-bring-country-par-rest-world

Matsubara, M., & Mochinaga, D. (2021, February). Japan's Cybersecurity Strategy: From the Olympics to the Indo-Pacific. *Asie Visions*(119), pp. 1-25.

Menocal, A. R. (2011, July 14). *The future of Japan's ODA: defining donor identity in a crowded marketplace*. Retrieved April 12, 2021, from ODI: https://odi.org/en/events/the-future-of-japans-oda-defining-donor-identity-in-a-crowded-marketplace/#:~:text=to%20international%20development.-,1.,player%20in%20the%20development%20community.&text=Consistency%20%E2%80%93%20Japan%20is%20viewed%20by,the%20%

METI Japan. (2020, November 6). *Outcomes of the 13th ASEAN-Japan Cybersecurity*. Retrieved April 18, 2021, from METI Japan: https://www.meti.go.jp/english/press/2020/1106_003.html

METI Japan. (2021, March 15). *Japan - US Industrial Control Systems Cybersecurity Week for the Indo-Pacific Region in FY2020*. Retrieved April 18, 2021, from METI: https://www.meti.go.jp/english/press/2021/0315_001.html

Mo, J. (2016). South Korea's middle power diplomacy: A case of growing compatibility between regional and global roles. *International Journal, 71*(4), 587-607.

MOD Japan. (2010). *Defense of Japan 2010.* Tokyo: Urban Connections.

MOFA Japan. (2019, January-February). *Countermeasures Against Cybercrime.* Retrieved April 18, 2021, from https://www.jica.go.jp/english/our_work/types_of_assistance/tech/acceptance/training/about/2018/sector/c8h0vm0000eqy9ys-att/1884518_e.pdf

MOFA Japan. (2019, January 18). *The 3rd ASEAN-Japan Cybercrime Dialogue*. Retrieved April 18, 2021, from MOFA Japan: https://www.mofa.go.jp/fp/is_sc/page25e_000294.html

Moon, J.-i. (2020, June 1). *Opening Remarks by President Moon Jae-in at 6th Emergency Economic Council Meeting*. Retrieved April 12, 2021, from Office of the President of the Republic of Korea: https://english1.president.go.kr/Briefingspeeches/Speeches/833

Morgan, D. L. (2007). Paradigms Lost and Pragmatism Regained Methodological Implications of Combining Qualitative and Quantitative Methods. *Journal of Mixed Methods Research, 1*(1), 48-76.

Muller, L. P. (2015). *Cyber Security Capacity Building in Developing Countries: Challenges and Opportunities.* Oslo: NUPI.

National Security Office of the Republic of Korea. (2017). *National Cybersecurity Strategy.* Seoul: National Security Office of the Republic of Korea.

NIDS. (2014). *NIDS China Security Report 2014: Diversification of Roles in the People's Liberation Army and People's Armed Police.* Tokyo: 9National Institute for Defense Studies.

NISC. (2015). *ASEAN-Japan Collaboration on Information Security*. Retrieved April 18, 2021, from National Center of Incident Readiness and Strategy for Cybersecurity: https://www.nisc.go.jp/eng/fw_top.html

NISC. (2018, October 16-17). *ASEAN – Japan Cybersecurity Working Group/Policy Meeting.* Retrieved April 18, 2021, from https://www.nisc.go.jp/press/pdf/aseanj_meeting20181026.pdf

Nishida, T., Pick, J. B., & Sarkar, A. (2014). Japan's prefectural digital divide: A multivariate and spatial analysis. *Telecommunications Policy, 38*, 992-1010.

OECD. (2011). *The Busan Partnership for Effective Development Co-operation*. Retrieved April 13, 2021, from OECD: https://www.oecd.org/development/effectiveness/busanpartnership.htm

OECD. (2012). *Cybersecurity Policy Making at a Turning Point: Analysing a New Generation of National Cybersecurity Strategies for the Internet Economy and Non-governmental Perspectives on a New Generation of National Cybersecurity Strategies.* Paris: OECD.

OECD. (2021). *Development Assistance Committee (DAC)*. Retrieved February 19, 2021, from OECD: https://www.oecd.org/dac/development-assistance-committee/

Park, D. (2016, January 12). *Cybersecurity Spotlight: South Korea*. Retrieved April 9, 2021, from The Henry M. Jackson School of International Studies University of Washington: https://jsis.washington.edu/news/cybersecurity-spotlight-south-korea/

Park, P. (2018, August 28). *Experts examine Asia's approach to cybersecurity*. Retrieved April 10, 2021, from Brookings: https://www.brookings.edu/blog/order-from-chaos/2018/08/28/experts-examine-asias-approach-to-cybersecurity/

Park, S. J. (2015). *The Korean Pivot and the Return of Great Power Politics in Northeast Asia.* Washington, D.C.: Atlantic Council.

Park, S., Chung, D., & Park, H. W. (2019). Analytical framework for evaluating digital diplomacy usingnetwork analysis and topic modeling: Comparing South Korea and Japan. *Information Processing and Management, 56*, 1468-1483.

Pawlak, P. (2016). Capacity Building in Cyberspace as an Instrument of Foreign Policy. *Global Policy, 7*(1), 83-92.

Pawlak, P., & Barmpaliou, P.-N. (2017). Politics of Cybersecurity Capacity Building: Conundrum and Opportunity. *Journal of Cyber Policy*, 1-22.

Pulse. (2020, October 28). *S. Korea boasts fastest internet connection, triples the global average*. Retrieved April 11, 2021, from Pulse: https://pulsenews.co.kr/view.php?year=2020&no=1106605#:~:text=Korea%20boasts%20fastest%20internet%20connection%2C%20triples%20the%20global%20average,-2020.10.28%2014&text=South%20Korea%20reigns%20in%20internet,by%20global%20internet%20analyst%20Ookla

Raska, M., & Ang, B. (2018). *Cybersecurity in Southeast Asia.* Paris: Asia Centre & DGRIS.

Robertson, J. (2007). South Korea as a Middle Power: Capacity, Behaviour, and Now Opportunity. *International Journal of Korean Unification Studies, 16*(1), 151-174.

Schia, N. N. (2016). *Teach a person how to surf: Cyber security as development assistance.* Oslo: NUPI.

Schmitt, M. N. (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge: Cambridge University Press.

Sedimo, N. C., Bwalya, K. J., & Plessis, T. D. (2011). Conquering the Digital Divide: Botswana and South Korea Digital Divide Status and Intervention. *South African Journal of Information, 13*(1), 1-10.

Smith, C. W. (2002). *Digital corporate citizenship : the business response to the digital divide.* Indianapolis: The Center on Philanthropy at Indiana University.

Soesanto, S. (2020). *Japan's National Cybersecurity and Defense Posture: Policy and Organizations.* Zurich: Center for Security Studies (CSS), ETH Zurich.

Tajima, Y. (2020, August 9). *Japan to lead first cyber defense drill with ASEAN, US and Europe*. Retrieved April 18, 2021, from NIkkei Asia: https://asia.nikkei.com/Business/Technology/Japan-to-lead-first-cyber-defense-drill-with-ASEAN-US-and-Europe

Tonami, A. (2018). Exporting the developmental state: Japan's economic diplomacy in the Arctic. *Third World Quarterly, 39*(6), 1-15.

Tran, T. T. (2017, November 7). *Pragmatism: How to Connect Positivism and Constructivism in Doing Research*. Retrieved March 3, 2021, from WebQDA: https://www.webqda.net/pragmatism-how-to-connect-positivism-and-constructivism-in-doing-research/?lang=en

UN General Assembly. (2021, March 10). *Open-Ended Working Group on Developments in the Field of Information and Telecommunications in the Context of International Security.* Retrieved March 28, 2021, from https://front.un-arm.org/wp-content/uploads/2021/03/Final-report-A-AC.290-2021-CRP.2.pdf

UN GGE. (2010, July 30). *Group of Governmental Experts on Developments in the Field of Information and Telecommunication in the Context of International Security.* Retrieved March 28, 2021, from https://undocs.org/A/65/201

UN GGE. (2013). *Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations General Assembly.

UN GGE. (2015). *Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security.* New York: United Nations General Assembly.

US Embassy and Consulate in the Republic of Korea. (2017, January 5). *01/05/17 – Key Outcomes of the U.S.-Japan-ROK Trilateral Vice Foreign Ministerial Meetings*. Retrieved April 10, 2021, from US Embassy and Consulate in the Republic of Korea: https://kr.usembassy.gov/010517-key-outcomes-u-s-japan-rok-trilateral-vice-foreign-ministerial-meetings/

van Puyvelde, D., & Brantly, A. F. (2019). *Cybersecurity: Politics, Governance, and Conflict in Cyberspace.* Cambridge: Polity Press.

Vosse, W. M. (2019). *Japan's Cyber Diplomacy.* Brussels: EU Cyber Diplomacy and Resilience Clusters.

Williams, V. (2020). *Foreign aid*. Retrieved February 11, 2021, from https://www.britannica.com/topic/foreign-aid

World Bank. (2019). *Global Cybersecurity Capacity Building: Lesson Learned and Recommendation towards Strengthening the Program.* Washington, DC: World Bank.

World Bank. (2020, June 1). *Global Cyber Security Capacity Program Phase I and II: Strengthening national Cyber Security Environment of Selected Developing Countries*. Retrieved April 19, 2021, from World Bank: https://www.worldbank.org/en/news/feature/2020/06/01/kwpfgscp

World Bank. (2021). *Individuals using the Internet (% of population)*. Retrieved April 24, 2021, from World Bank Open Data: https://data.worldbank.org/indicator/IT.NET.USER.ZS

Yasushi, W., & McConnell, D. (2008). *Soft Power Superpowers: Cultural and National Assets of Japan and the United States.* New York: M.E. Sharpe.

Yonhap News Agency. (2020, March 5). *Digital divide still high in S. Korea*. Retrieved April 9, 2021, from Yonhap News Agency: https://en.yna.co.kr/view/AEN20200305004400320