Theoretical, Empirical, and Normative Dimensions of State Involvement in Cybersecurity: The Case of Japan

Siber Güvenlikte Devlet Müdahalesinin Teorik, Ampirik ve Normatif Boyutları: Japonya Örneği

Elif Sercen NURCAN [1]

Araştırma Makalesi / *Research Article*
Geliş Tarihi / *Received:* 25.02.2022
Kabul Tarihi / *Accepted:* 23.06.2022
Doi: 10.48146/odusobiad.1079425

Atıf / *Citation:* Nurcan, E. S., (2022). "Theoretical, Empirical, and Normative Dimensions of State Involvement in Cybersecurity: The Case of Japan" ODÜSOBİAD 12 (2), 689-708, Doi: 10.48146/odusobiad.1079425

Abstract

Unlike other major liberal democratic countries where the states can be argued to have oriented their involvement in cybersecurity relatively more towards the national security aspect such as the US, the role of the state in the cybersecurity realm has a less clear-cut orientation in the case of Japan. This paper clarifies the nature of the role of state in cybersecurity in Japan using the framework utilized by Cavelty and Egloff's 2019 article (Cavelty & Egloff, 2019). Within this framework, the role of the state is analyzed in theoretical, empirical, and normative dimensions. The theoretical dimension analysis focuses on different theories in literature regarding the Japanese state whereas the data for the empirical dimension analysis come from publicly available records by key Japanese state and private organizations involved in cybersecurity. The normative dimension analysis emphasizes the time horizon aspect of cybersecurity policies the Japanese state should be directing its attention. In conclusion, it is found that the Japanese state embodies the roles of "knowledge creator/disseminator", "supporter/representative of society", "partner", and "guarantor and protector" in addition to a necessity for government bodies to turn towards proactive long-term policies and initiatives for better cybersecurity in Japan.

Keywords *Cybersecurity, state policies, Japan, security policies, technology policies*

Öz

Devletlerin siber güvenliğe katılımlarını nispeten daha fazla ulusal güvenlik yönüne (ABD gibi) yönlendirdiği ileri sürülebilecek diğer büyük liberal demokratik ülkelerden farklı olarak, Japonya'da devletin siber güvenlik alanındaki rolü daha az net bir yönelime sahiptir. Bu çalışma, Cavelty ve Egloft'un (Cavelty ve Egloft, 2019) geliştirdiği analiz çerçevesini kullanarak Japonya'da devletin siber güvenlikteki rolünün doğasını açıklamaktadır. Bahsedilen bu çerçevede devletin rolü teorik, ampirik ve normatif boyutlarda analiz edilmektedir. Teorik boyut analizi, Japon devleti ile ilgili literatürdeki farklı teorilere odaklanırken, ampirik boyut analizi için veriler, siber güvenlikle ilgili

[1] Responsible author: Elif Sercen Nurcan, Meiji University, Tokyo, e-mail: esnurcan@meiji.ac.jp, ORCID: 0000-0002-7104-0283

Bu makale araştırma ve yayın etiğine uygun hazırlanmıştır. iThenticate intihal incelemesinden geçirilmiştir.

önemli Japon devlet ve özel kuruluşlarının kamuya açık kayıtlarından alınmaktadır. Normatif boyut analizi, Japon devletinin dikkat sarfetmesi gerektiği düşünülen siber güvenlik politikalarının zaman ufku yönünü vurgulamaktadır. Sonuç olarak, Japon devletinin "bilgi yaratıcısı/yayıcı", "toplumun destekçisi/temsilcisi", "ortak" ve "garantör ve koruyucu" rollerini bünyesinde barındırdığı ve devlet kurumlarının Japonya'da daha iyi siber güvenlik için proaktif uzun vadeli politikalar ve girişimlere yönelmesi gerekliliği tespit edilmektedir.

Anahtar Kelimeler Siber güvenlik, devlet politikaları, Japonya, güvenlik politikaları, teknoloji politikaları

Introduction

Security is often considered as the absence of threats or a critical public good provided by the nation state to its citizenry per its *raison d'état* (Engerer, 2011). Due to the progression of technology, the same process of getting rid of threats by the nation states has to be implemented in cyberspace, the newest domain of national security which "… fuses all communication networks, databases and information networks into a global virtual system" (Liaropoulos, 2013). As *security in cyberspace*, cybersecurity can be broadly defined as "the practice of protecting systems, networks, and programs from digital attacks" (CISCO, 2020). When taken under the political science perspective, cybersecurity is built upon dynamic interactions, conflicts, and contestations that involve governments, private sector, religions, and civil society together with criminals (Deibert & Rohozinski, 2011). The existence of a multitude of actors and interactions within the cybersecurity field has enabled new types of contestations involving the nation-states. The reactions of the nation-states to such contestations exhibit great variety as well as the tools employed against them. Official cybersecurity policies hold different inclinations, leading to patterns in nation-state behaviors. The development of patterns in nation-state actions offers fertile grounds for political science research where this study takes its roots. Despite having other works that offer a descriptive list of various roles of the nation-state in cybersecurity (Cavelty and Egloff, 2019); the need in literature is now a body of case studies which showcase particular nation-states' adapted roles in cybersecurity. This study aims to provide a case study of the state's role in cybersecurity in Japan; a nation-state which has long provided alternative models in the political science field.

Methodology-wise, the role of the state in cybersecurity in Japan is identified by utilization of the analytical framework built by Cavelty and Egloff. In addition to the role identification, the theoretical, empirical, and normative dimensions of the Japanese state involvement in cybersecurity is discussed. A literature review of both English and Japanese sources which include press releases, academic and government publications is carried out to exemplify and support the identified roles and the three-dimensional analysis of the case. In sequence, the first section of this paper answers the question of why the nation-state is taken as the main factor of analysis by illustrating the linkage between the nation-state and cybersecurity. The second section introduces the principal analysis framework developed in the 2019 work of Cavelty and Egloff. Then, the case study of Japanese state's role in cybersecurity starts in the third section with the theoretical dimension analysis on the role of the state in Japan. The fourth section gives the empirical dimension analysis while the fifth section features the normative dimension analysis portion of the case study. Finally, overarching conclusions are drawn in the sixth section. By

following this flow, the goal is the provision of a comprehensive case study that highlights some of the prominent roles that the nation-states can adopt in the field of cybersecurity.

Analytical Framework

The Linkage Between The Nation-State And Cybersecurity

The first question of why look at nation-state's role in cybersecurity in the first place can be answered with the fact that the nation-state happens to be most significant actor in security provision. After the Cold War, there was the expectation that the globalization would usher in an era of global governance. "History" had seemingly ended, and capitalism was seen as the only viable road forward (Fukuyama, 1989). Growing trade, communication, and the moving of people were expected to elevate the role of multinational corporations and international organizations, pushing the nation-state into the backseat. By the end of the 2010s, these expectations have failed to materialize. The nation-state made a comeback in the political arena. Examples for this phenomenon include Russia's growing separation from international bodies such as the Group of Eight (G8) in 2014 and the suspension of membership from the United Nations Human Rights Council as a reaction to the country's unilateral invasion of Ukraine in 2022 (United Nations, 2022), Brexit in 2016, the rise of isolationism in the United States picking up speed since 2016 (Watson, 2016), and the lack of globally united management of the current COVID-19 outbreak crisis by international governance bodies (Bernes et al., 2020).

The same phenomenon of the nation-state's comeback resonates in the field of security. Despite the existence of international bodies of security alliances such as the North Atlantic Treaty Organization (NATO) or the recently inaugurated trilateral security pact between Australia, the United Kingdom, and the United States (AUKUS), it is the nation-state that still carries the primary responsibility of provision of national security. According to Kenneth Waltz, the fundamental ordering principle of the international political system is anarchy where individual state actors do not display relations of subordination, and where they are distinguished only by their varying capabilities (Waltz, 1979). This view allows a ranking to be created between various security actors based on their size, organizational complexity, and permanency as seen in **Figure 1**.

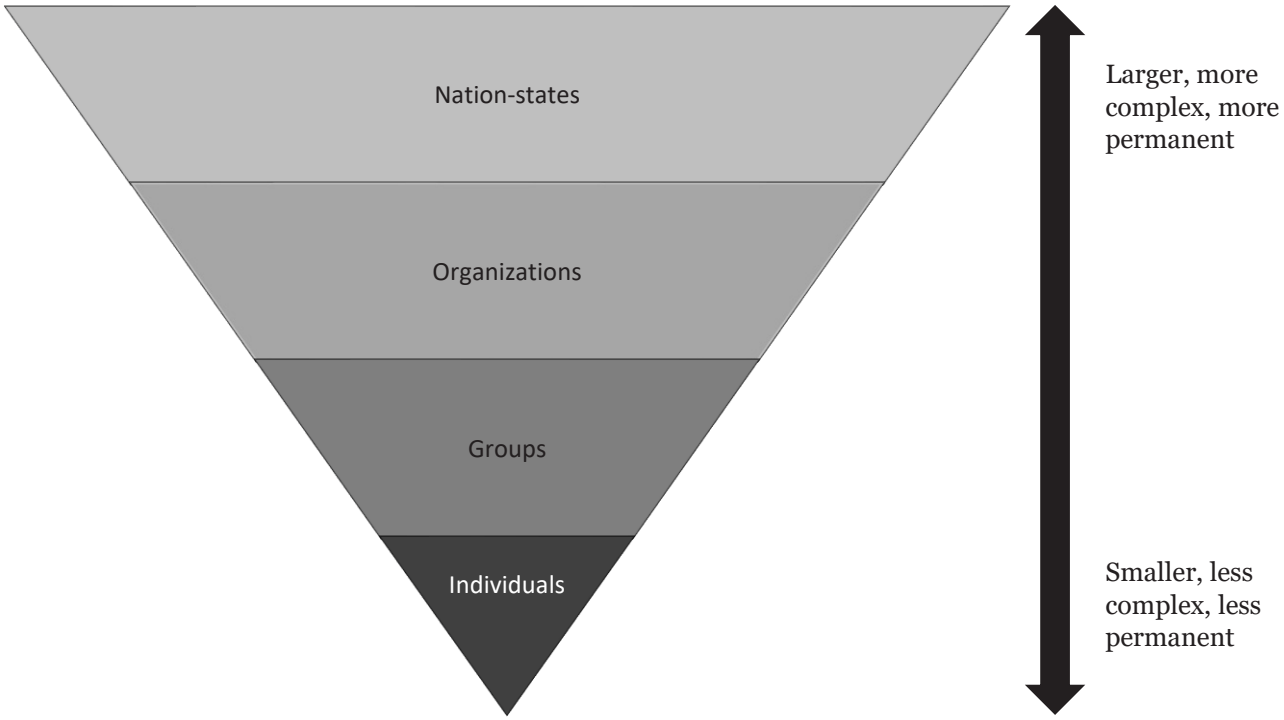

Figure 1: Fundamental groups of security actors based on their size, organizational complexity, and permanency (Adapted by the author from Kayama (2015) and Sigholm (2013) (Kayama, 2015; Sigholm, 2013).

Currently, different nation-states are at different levels of economic development. The Fourth Industrial Revolution is ongoing, and the level of economic advancement is linked to the adoption of information and communications technology (ICT). All nation-states and their economies rely on ICT, albeit at different levels. Thus, the level of significance of cybersecurity for each nation-state varies. In addition, a distinction can be made between whether a nation-state prioritizes the defense-based understanding of cybersecurity or the non-defense. Defense-based understanding of cybersecurity can be defined as the placement of the major focus of the nation-state on the security of military operations and critical public infrastructure. And the non-defense understanding of cybersecurity entails those economic aspects of cybersecurity provision such as the protection of intellectual property (IP), stock markets, and ensuring unhindered economic activities of private sector as well as the political aspects such as the continuation of governance processes such as free elections and the maintenance of state legitimacy, i.e., public's trust in government. Due to the fact that cybercrime carried out using instruments such as malware is a serious concern which is growing exponentially each passing year as seen in **Figure 2**, nation-states do have a legitimate interest in combatting the cyber threats via engaging in the defense-based understanding of cybersecurity. However, some nations including the US, Israel, and Iran tend to heavily engage in more offensive actions in cyberspace which can be grouped under cyberwarfare

(Deibert & Rohozinski, 2011). These actions can be exemplified by the US-Israel Stuxnet attack against Iran's nuclear program in 2010 and Iran's Shamoon attack against Saudi Arabia's petroleum producer Aramco in 2012. Other states such as Japan tend to put more emphasis on pursuing cybersecurity via non-defensive understanding as demonstrated in the case study portion of this study.

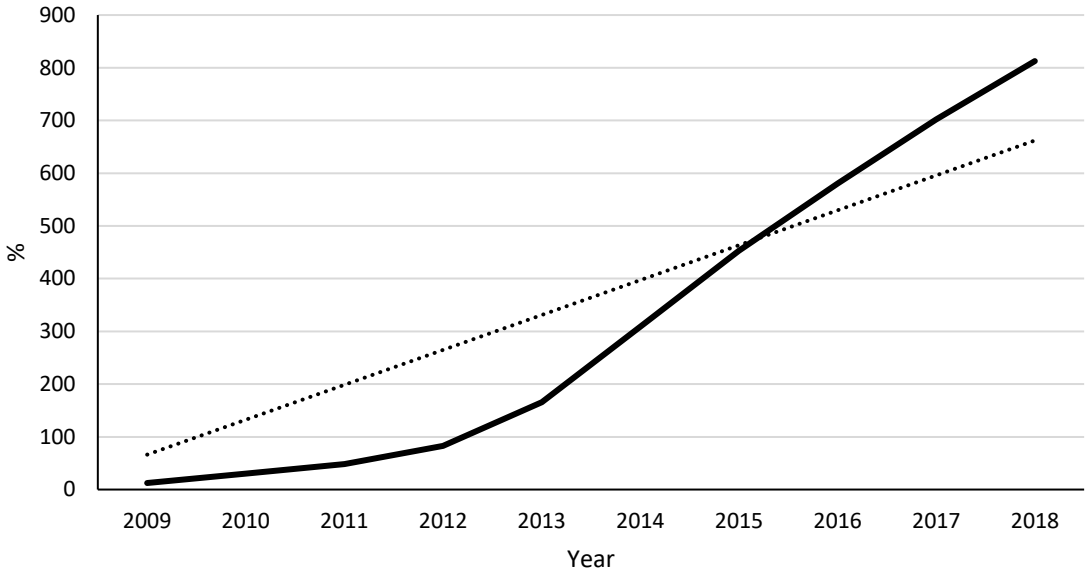

Figure 2: Trend of global malware infection growth rate, 2009-2018 (Data taken from PurpleSec's *2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends*. (PurpleSec, 2022)).

The three-dimensional analysis framework for the state's role in cybersecurity

Cavelty and Egloff's 2019 work provides an analytical framework through which further analysis of the role of the state in cybersecurity can be carried out in differing cases. To summarize, their framework consists of analyses of three dimensions: the first is the theoretical dimension analysis which investigates existing cybersecurity literature; the second is empirical and analyzes policy development in order to demonstrate the diversity of the roles the state imagines for itself; and finally, the third dimension is normative and investigates what the role of the state should be in authors' own opinion.

As for the methodology employed in this work, particularly in the empirical portion, the authors utilize bibliographical data, policy documents, and policy papers which are available on the World of Science (WoS) and Scopus databases. Quantitatively, they have determined the growth of the scientific output on "cybersecurity" between 2012 and 2014 to be approximately 100% (Cavelty & Egloff, 2019). In addition, the most cited articles about cybersecurity are inspected. The inspection results find that the computer science discipline tops the list of research fields (WoS: 72%, Scopus: 61%), followed by engineering (WoS: 36%, Scopus: 40%). The technical view is found to be predominant in majority of the works, with almost no demonstrated interest in understanding the context of cyber threats. As a side note, when the growth rate in the number of works is measured for the time period between 2014-2020

on the same databases, we find almost 700% growth on Scopus and 900% growth on WoS database (Scopus, 2021; Web of Science, 2021).

When Cavelty and Egloff derive their conclusions from bibliographical data analysis on social science literature however, they find the domination of the field by the idea of the nation-states being unable to provide security on their own since market interventions are undesirable and that the states are called upon as the actors to "… reestablish control over the use of cyber technologies through international norms, yet … (themselves) creating more insecurity" (Cavelty & Egloff, 2019). In other words, two focal points in top-cited social science research emerge. First, the state is thought to be incapable of providing the public good of security on its own, since state's market interventions are undesirable. The state is an important security actor, however there is an underlined necessity to take into consideration the preferences of other actors. Second, cybersecurity is understood as a political phenomenon and the aim is to understand how cyber technologies change conflict dynamics, thus influencing the overall security in the international system. As a link is established to the notion of national security, states are the actors called upon. Most of the literature defines cybersecurity as an international security problem which Cavelty and Egloff find to be too narrow.

Based on the analysis of the top-cited social science literature on cybersecurity which feature the state, the authors describe six different roles of the state in cybersecurity as summarized below:

1. *State as guarantor and protector*: State must secure its own civilian and military networks.

2. *State as legislator and regulator*: State creates the legal basis to clarify its hierarchical function and to regulate tension between citizens and businesses. This function depends on the historically developed relationship between the economy and the state.

3. *State as supporter/representative of society*: State advocates for beneficial international frameworks for the benefit of the whole society.

4. *State as a partner*: State provides protection via public-private partnerships. Voluntary cooperation- especially information exchange - between the industry and the state is often the case in point.

5. *State as knowledge creator/disseminator*: State raises awareness on cyber issues among the public as a major policy endeavor. For this, the state wants to be perceived as a trustworthy source of information. This role depends on the relationship of trust between society and state.

6. *State as the originator of more cyber-in-security*: State can create more cybersecurity issues via aggression. In some societies, a history of unjustified state interference in civil rights reinforced the perception of the state as a danger. This perception of state is also reinforced by the acts of hostile foreign nations. Thus, the state becomes the originator of more problems.

The main conclusion drawn in this framework is that the state has multiple roles and represents different interests at the same time. As there are different roles, various alliances are formed between departments of the state, interest groups, and the society. Within these alliances, there may be role conflicts. In democratic regimes, such role conflicts are dealt with at the political level and can be approached systematically. The recognition of the legitimacy of multiple roles of the state helps to recognize that decisions in this area take on an intrinsic political dimension. In other words, democratic states may shoulder conflicting roles at times when it comes to cybersecurity yet, it is possible to trace the political linkages of each role and approach the conflict accordingly.

In this paper, a modified version of the above framework is employed. A major difference is that the focus of this study is on the case of Japan where real life examples of how the Japanese state is carrying out its different roles are given. The reasoning behind the framework modification is based on the fact that Cavelty and Egloff's analysis focuses on American and European literature almost exclusively, leaving out alternative models of state involvement in cybersecurity. Also, the intention of this paper is not to serve as a guideline for policymakers, therefore the normative aspect has been scaled down appropriately. Having stated this, let us bring the discussion to the case of Japan in the next section.

The Case Study

Theoretical dimension analysis on the role of the state in Japan

When the concept of "Japanese state" is used, it is the *bureaucracy* that occupies the mind. Actions of the Japanese state has been determined by its powerful bureaucracy rather than elected officials. Bureaucratic agencies have been both determining and carrying out policies for the Japanese polity for decades, although there has been a backsliding in favor of the elected politicians in recent years. Nonetheless, the dominant view which accepts the state involvement in the industrial and economic catchup of Japan puts forth the argument that the Japanese industrial transformation was born from deliberate public policy (Rothwell 1986, 66). Bureaucracy's involvement in economic activities in Japan has been the subject of many academic works, the most famous one is Chalmers Johnson's "MITI and the Japanese Miracle". Pointing at the ways bureaucrats gave direction to the economic development, for example, Johnson describes the administrative guidance widely seen in Japanese economic administration. His work states that a wide range of economic activities is not covered by general laws or by detailed government ordinances, and is subject to administrative guidance; however, their existential basis lies in the state authorities stated in laws (Johnson 1982, 263). Unlike the previous tradition in Japanese studies, his work grounds the reality of bureaucratic intervention in the economy on observable factors instead of only "culture".

There have been many scholars who took up the ideas put forth by Chalmers Johnson and expanded on them further. For example, within the 'bureaucracy-led system,' Honda finds bureaucrats are often responsible not only for policy execution but also for the planning, planning, and coordination of the policy itself, in addition to administrative control. A key point he draws attention is that in Japan, bills prepped by the relevant ministries and submitted by the Cabinet have been passed at an extremely high

rate with no revisions (Honda, 2001). Therefore, it is not a mistake to perceive Japanese state's actions as actions by the bureaucracy or at least, carrying its approval.

The nature of state-industry relationship in Japan is intimately tied to how the role of the Japanese state in cybersecurity is perceived. Cybersecurity is positioned either as a national security issue or an industrial policy one **(Figure 3)**. Both positionings have logical rationale supporting them. Positioning cybersecurity as an industrial policy issue comes from the nature of cyberspace which does not spare the public from the ongoings. Cyberattacks are directed at private firms and public infrastructure; their readiness against such attacks is a gauge of the technological capacity of a given country. This capacity is built via market forces, where there is a demand, there is a supply. However, since cybersecurity is a very recent field that requires extensively trained human resources as well as technical capabilities, reliance on market may bring delayed results. There is often a need for the central policymaking to direct the flow of resources towards building the necessary capacities for cybersecurity implementation.

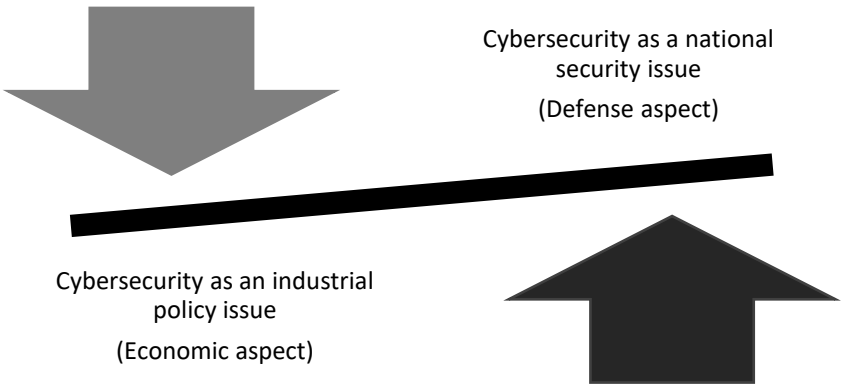

Figure 3: Conceptualization of the two different theoretical positioning of the cybersecurity issue

The emphasis on the economic aspect of cybersecurity in Japan can be linked to a long institutional heritage. In almost all high technology-related areas, Japanese private sector had originally lacked the experience, information, capital, and organizational capacity to build a market existence and therefore, cooperation with the central government was logical in such conditions (Okimoto et al., 1984). Many monikers have been adopted in naming this nature of Japanese political economic system, including "adaptive communitarian capitalism" (Khanna, 1997). Yong Wook Lee's identity-based situational understanding and conceptualization of Japan and US as two rivals promoting different models of economic development also features this naming tradition (Lee, 2008). However, the "Japan Inc." idea which describes Japan as a monolithic entity with entire cadres of bureaucracy, political representatives, and private firms strategically collaborating to take over world markets is a caricature among the

literature. There were industries and periods when industrial policies succeeded and there were times and areas where even the existence of a coherent policy was called in question.[2]

Currently, there is recognition of the change of state-industry relations in Japan, particularly regarding the influence of bureaucrats. One of the observed changes is the ministries putting more of its faith into the "business establishment" —that is, the top management of Japan's big-name firms (Inoue, 2012). Another change is reflected in how reformism has come to be featured heavily in the domestic political arena. Kawabata, for example, explains how Liberal Democratic Party's (LDP) reformist Ryutarō Hashimoto took on the prime minister role and pursued six large administrative reforms with the main target being the power held by the national bureaucracy. The number of ministries and agencies was reduced by these reforms while the number of political appointees was raised (Kawabata, 2006). The following prime ministers such as Democratic Party of Japan's (DPJ)[3] Yukio Hatoyama continued neutralizing bureaucracy's influence via founding the National Strategy Office and the Government Revitalization Unit while getting rid of the administrative vice ministerial meetings[4].

As for the defense aspect of state's role, explanations for Japan's general attitude towards defense-related issues help decipher the issue at hand. Regarding the Japanese perspective on necessity of national security rhetoric, Miyashita underlines that most opinion polls show that the Japanese people have consistently supported keeping the nation's defense forces at a minimum and limiting Japan's international contribution to economic assistance. However, he also points at public opinion poll results from the 1950s, 1960s, and 1970s in which public opinion shows less pacifist orientations in earlier decades. The regional ongoings, mainly the advancement of communism in the East Asian region may have led to insecurity in his understanding. (Miyashita, 2008).

States happen to be the least critical actor that builds and populates cyberspace when compared to the actions taken by the academics, civil society, programmers, and the private sector which owns and operates the physical aspects of Internet. However, Klimburg warns, states have the power to manipulate and destroy cyberspace (Klimburg, 2018). Most analysts agree on the possibility of a devastating electronic attack occurring only after severe deterioration of relations between the involved states. Furthermore, non-state actors may not be held to this logic while their capacity to launch an overwhelming attack tend to be much less than nation-states (Lowenthal, 2019). When these factors are put together, the understanding of defense aspect of the state's involvement in cyberspace in Japan can be based on 'soft nationalism' which was born in the sunny times of the 1980s. Pride in national economic success and higher standard of living, sense of equality with other advanced industrial nations had culminated in a new sense of nationalism (Higashi & Lauer, 1990), dubbed as 'technonationalism.' With this general theoretical background of the Japanese state's role in industry and defense-related issues in mind, the empirical dimension analysis can be carried out next.

---

[2] For a more detailed account on the industrial policy debate from a neoclassical perspective, please refer to: Komiya, Ryutaro. 1988. "Introduction." In *Industrial Policy of Japan*, edited by Ryutaro Komiya, Masahiro Okuno, and Kotaro Suzumura, 1-22. San Diego: Academic Press.

[3] DPJ is the abbreviation of the now-defunct Democratic Party of Japan (in Japanese: *Minshutō*).

[4] The significance of this move lays in the fact that it was the administrative vice ministers (in Japanese: *jimujikan*) who actually led the ministry by tradition, and the elected politician ministers playing only a symbolic role in policymaking.

Empirical dimension analysis on the role of the state in Japan

In this section, some of the key international relationships and policymaking that are actively shaping the Japanese state's involvement in the cybersecurity field are analyzed. The first part of this section focuses on significant developments in Japan's foreign affairs in relation to cybersecurity while the second part gives a summary of key policy initiatives and their implications. It is found that the key roles of the Japanese state are "state as the knowledge creator/disseminator" and "state as the supporter and representative of the Japanese society".

In the current state of affairs where fake news, whether based on intentional disinformation campaigns or as spontaneous phenomena, play a role in how societies engage with cyberspace, states take up as the role of creator and disseminator of knowledge as an effort to sustain their raison d'état. This is supplemented with the "supporter of the society" role when a state's actions and policies are geared towards aiding the representation of what the populace defines itself as. In this section, state organs that carry out the roles of knowledge creator/disseminator and Japanese state as the supporter and representative are explained.

There are notable examples of how the Japanese state has shouldered the role of knowledge creator and disseminator. Working under the Cabinet, National Center of Incident Readiness and Strategy for Cybersecurity (NISC) established in 2015, replacing the former NISC acting since 2005. The NISC acts as the Cybersecurity Strategy Headquarters in collaboration with the public and private sectors on a variety of activities to create a free, fair and secure cyberspace. Information coordination is one of the most important parts of the role of knowledge creator. In this area, Japan Information-Technology Promotion Agency's (IPA) IPA/ISEC (Information Security Early Warning Partnership) "serves as the vulnerability reporting organization, while Japan Computer Emergency Response Team (JPCERT/CC) serves as the coordinating organization." Their efforts at proper handling of the vulnerability-related information are compliant with International Standards Organization's (ISO) ISO/IEC 29147:2014 "Vulnerability Disclosure" specification (IPA, 2017). In particular, the focus on information gathering and dissemination to the political actors as well as the general populace carried out by these organs lends evidence to the Japanese state's taking up the particular role of knowledge creator and disseminator.

Adoption of certain tenets of "state as supporter and representative of society" has also been made apparent in Ministry of Foreign Affairs (MOFA) initiatives. Policy initiatives and projects by MOFA offer examples of how the Japanese state embraces the role of society's representative on the international stage. For example, MOFA has launched its Cyber Initiative Tokyo 2019 that entails the rule of law, confidence-building measures, and capacity building support as three pillars of cyber diplomacy. According to the lecture by Keisuke Suzuki who was the Deputy Minister of MOFA at the launching event of Cyber Initiative Tokyo 2019 on December 12, 2019: "In order for the cyberspace to continue to generate innovation and prosperity in the future, it will be extremely important for it to remain as a free, fair and safe space. To maintain this, an international order based on rules is indispensable, and in order

to form that international order, cooperation with the entire international community and cooperation beyond the boundaries of industry, academia and government is necessary. Therefore, Japan is promoting 'the rule of law,' 'confidence-building measures,' and 'capacity building support,' and these three pillars are the pillars of our cyber diplomacy" (Suzuki, 2019). Recently expanding in many other countries, cyber diplomacy is a concept which emerges from the national security aspect of cybersecurity, seeking an improved cyber political environment where foreign affairs are handled in the interests of the country. In Japan's case, the adoption of policies towards maintaining clear and uninterrupted dialogue and cooperation within cyberspace can be interpreted as acceptance of newer tools of diplomacy. Ministry of Internal Affairs has also acted as society's representative regarding personal information sensitivity. Examples include the coordination between the ministry and the Cabinet regarding the Amazon incident in 2019 and the LINE incident in 2021 where severe warnings were issued in reaction to personal information leakages at these companies by the Personal Information Protection Commission (a *gaikyoku* operating under the Cabinet which means a governmental body with high autonomy in Japanese) (Personal Information Protection Commission, 2019).

The presence of the latter role can be linked to the shifts in international relations priorities. Official attention in foreign relations has been shifting towards improving Japan's international standing since Prime Minister Nakasone's Maekawa Report spearheaded this shift in state focus, by establishing formal interest in Official Development Assistance (ODA) and Foreign Direct Investment (FDI) in less developed countries. Concentrated efforts in organizations such as Asian Development Bank (ADB), Asia-Pacific Economic Cooperation (APEC), and Association of Southeast Asian Nations (ASEAN) made Japan's demand to reconstruct its image and attain a leadership position evident (Hatakeyama & Freedman, 2010). In support of this demand, Japan's IPA has implemented a campaign called International Cybersecurity Campaign to be held every October since 2012. As part of this annual campaign, Japan has conducted joint awareness raising activities with ASEAN member states. In 2015, as part of the activities, the National Center of Incident Readiness and Strategy for Cybersecurity (NISC) and ASEAN counterparts have co–translated IPA's original posters regarding password safety into 8 languages that are used in the ASEAN member states **(Figure 4)**. The original posters were developed by IPA to enhance awareness regarding passwords among the young population in Japan (IPA, 2016). The provision of these posters and their translations to the international community serve as important examples of representation of the principles that Japan stands for when it comes to the state's role as a representative of the society on the international stage.

Figure 4: A sample of the English posters from the International Cybersecurity Campaign by IPA (Password Awareness Posters in Languages Used by ASEAN Member Countries website (IPA, 2016)

In addition, IPA's collaboration with ASEAN member countries is arguably favorable for the participant countries as well. For example, taking the percentage of organizations that had ransomware affecting their ICT systems as a basis, Vietnam faces with a great number of detections. Thailand is also featured as one of the top 10 countries where a high percentage of ICT systems faces malware and grayware detections (Matsukawa et al., n.d.). Indonesia, for example, Internet cafes provide network access to a significant portion of the population, however, the malware infection rates at these cafes are very high. In addition, 86% of Indonesians use pirated software compared to the global rate of 42% and 19% in the US (Myers, 2013). Therefore, collaborative projects that introduce better cyber hygiene and security practices to the general population can be certainly useful for ASEAN countries.

As for the evidence for the Japanese state adopting the role of "the state as the partner", the following examples can be given. Adoption of artificial intelligence (AI) and machine learning technologies in addition to robotics is strongly supported by the policies of Ministry of Economy, Trade and Industry (METI). However, as Lowenthal argues, the integration of such technologies to intelligence activities remains low even in the US. Furthermore, human analysts or policymakers would not be entirely comfortable with taking major decisions based on AI (Lowenthal, 2019). Human dependencies, especially on extensively trained and experienced experts will continue. Therefore, focusing on improving the human capital in the cybersecurity field can be readily accepted as a rational decision.

Japanese foreign affairs in relation to cybersecurity also demonstrate the state's role as the protector within the national security rhetoric. This is due to the country's geographical situation, prohibition of re-militarization by the Article 9 of the Constitution, and post-WWII relationship with major security actors. Akitoshi Miyashita points at that one of the unsolved puzzles about Japanese foreign policy since the 1970s is the gap between the nation's economic power and its military capability. The absolute

amount of defense expenditures of Japan is high, however the relative size of the expenditures in relation to gross domestic product (GDP) is one of the smallest among advanced nations. Miyashita also underlines the rationality of the argument that due to the alliance with the US, the Japanese government is often led by the pro-US and pro-business LDP which takes the dovish path rather than the hawkish one for the best interest of Japan which was first started by the Prime Minister Shigeru Yoshida (Miyashita, 2008) who is also known for laying down the principles of post-WWII Japanese foreign policy in the form of Yoshida Doctrine. The end of Cold War did not change this pattern and the US continues its security guarantee to Japan.

China has been the foremost focus point of cybersecurity policies of Japan. Due to the rise of Chinese cyber operative capabilities, there had been more attention paid to Chinese activities in this regard. A key example of this development is that the Cabinet Satellite Intelligence Center controls Japan's imagery satellites which in turn mostly focus on China. And it was due to these concerns with China's growing military power which led to increased tempo of cybersecurity capacity building, according to Lowenthal (Lowenthal, 2019). There have been media reports on Japan which announced the upcoming expansions of number of intelligence satellites from four to eight in 2023. Japan is also investing USD 372 billion over the next decade to expand its indigenous unmanned aviation vehicle (UAV) capability. Also, there have been reports of Japan creating a human intelligence service together with increased cooperation with the Five Eyes with specific attention to China's military and North Korean smuggling. Regional alliance against the growing clout of China between Japan and South Korea was initiated as both parties signed an intelligence sharing agreement in 2015. Most of these developments took part during Prime Minister Shinzo Abe's tenure, whose reforms may have been seen as limited to outsiders, yet controversial within the country.

Launched by either an organized non-state group or state-sponsored master hackers, cyberattacks have data-related and psychological effects even if they are unsuccessful. Therefore, it is in the interest of rogue states such as North Korea to launch easily traceable and flashy attacks. Effects of such attacks would achieve the goal of creating political leverage where otherwise none would exist; this point is especially relevant in considering the effect of North Korean-Japanese bilateral relations on state involvement in cybersecurity in Japan. Combination of showing off of cyber capabilities together with missile and nuclear technology increases rogue states' negotiation potential (Klimburg, 2018). Despite not being the original target, there was an incident which brought American political interests in close proximity of Japanese interests. Sony Pictures Entertainment operates under the umbrella of Japanese multinational conglomerate Sony Corporation. However, it was the US public outcry heard throughout in November 2014 when the North Korean regime carried out a concentrated attack which managed to hack and subsequently blackmail the company for the purpose of preventing the release of a parody movie about Kim Jong Un. Also, it was the US government who took the unheard step of revealing the source of its intelligence and attributing the cyberattack to North Korea (Klimburg, 2018). While Japan can be said to be more concerned about classic military threats, the intermingled nature of international

relations brings forth differing areas of concern. North Korea is growing more sophisticated in their attacks (Osborne, 2021).

As a more traditional organ of national security, the Japan Self-Defense Forces' (JSDF) Cyber Defense Group (CDG), part of the JSDF's Command, Control, Communication & Computers (C4) Systems Command, will increase its personnel from 220 to 290 by the end of March 2021. Spending on cyber activities more than doubled between 2018 and 2019 following the adoption of the 2018 defense strategy, rising from JPY 11 billion (USD 100 million) to JPY 25.6 billion (USD 235 million). However, this growth was from a very low base: the 2019 spending figure was less than half 1% of the country's defense budget. Lowenthal notes that there had been a certain resistance phase in intelligence agencies regarding the adoption of IT revolution. Although the phase has passed, the issue of adopting new technologies in the agencies is still ongoing (Lowenthal, 2019). In terms of defense capability building, there is a certain advantage of investing in cybersecurity capacities for the JSDF. This advantage stems from the fact that cybersecurity has been used in a defensive manner so far in Japan, involving no personnel shipments abroad or loss of life. There is no denying of classic tools and methods of national security, however, cyberspace allows a far less criticized field for the JSDF to operate in.

Overall, what Japan has been undertaking in the field of cybersecurity can be explained partly by the path dependency. As Guy Peters notes, path dependency helps minimize decision-making costs for the institution. There are, however, instances where policymaking simply involves habits (Peters, 2005). The centrality of US-dependence in defense and loosely cooperating agencies under different ministries are not set in stone, they are born from the long-term trends institutionalized in social norms of bureaucracy and foreign affairs of Japan. Discussion on formation of unwritten rules which dictate policymaking is the topic of another research, however, what needs to be underlined here is that Japanese state involvement in the cybersecurity field carries continued historical trends at least from the end of the Second World War.

Normative dimension analysis on the role of the state in Japan

Following the theoretical and the empirical dimension analyses of the role of the Japanese state in cybersecurity, we now turn to the normative dimension and answer the question "What changes should be made in Japanese state's involvement in cybersecurity realm for improvement?" As this section is normative in nature, it is not an analysis of the actual reality, but rather, what is ought to be done.

The cybersecurity issues the Japanese state should be focusing on solving can be summarized as below:

- Late-late comer to the cybersecurity field: Main issue is capacity building.
- Lack of necessary human capital which takes a long time to nurture.
- Beyond engineering: Germany's mandatory training of its civil servants in cybersecurity basics; Japanese central and local bureaucracy may stand to benefit from similar trainings.

- Actors behind cyberattacks target the weakest links in networks, an untrained official operating on a computer which is not up to date with malware protection is a perfect opening for infiltration.
- Demonstration of political will against cyber threats: Yoshitaka Sakurada Incident in 2018 cannot be repeated.

Japan is facing hurdles as a late-late comer to the cybersecurity field, in a manner that is not dissimilar to the country's entrance into the semiconductor industry. In this section, a normative discussion is carried out with the intention of pointing at such hurdles rather than laying out a complete roadmap. One of the main issues almost all latecomers face when entering a new industry is the lack of necessary human capital. In high technology fields such as cybersecurity, the required level of computer engineering, software skills, and analytical capabilities alongside attaining experiences with real life incidents take a long time to nurture. And the lack of properly trained human resources has been apparent for a while in the case of Japan. Improvement is not limited to engineer human resources of course. There are examples such as Germany's mandatory training of its civil servants in cybersecurity basics; Japanese central and local bureaucracy may stand to benefit from similar trainings. It needs to be remembered that actors that are launching cyberattacks often target weakest links in networks, an untrained official operating on a computer which is not up to date with malware protection can be said to constitute a perfect opening for infiltration.

In addition to the human capital investment, another aspect in which Japan needs to improve is the demonstration of political will against cyber threats. Aforementioned policies and initiatives by the Japanese government and the bureaucracy have been steps in the right direction. However, Yoshitaka Sakurada who was the deputy chief of the government's cybersecurity strategy office and the minister in charge of the Tokyo Olympic and Paralympic Games has caused a major setback in demonstration of political will. During a National Diet questioning session in 2018, Minister Sakurada admitted that he did not know how to use computers when questioned by the opposition party members on ICT. Minister's reply was in fact an additional confession to his admission of not knowing how USBs are operated. The situation was deeply troubling since the questioning itself was on the operation of nuclear power plants. As critical infrastructure, nuclear power plants have been the target of infamous Stuxnet attacks in the past which involved the usage of compromised USBs. Therefore, an admission of this scale has caused uproar both domestically and internationally. It has been speculated that the reason why Japan was left out of the multilateral security alliances such as the AUKUS and the Five Eyes is related to the amount of work the country has to accomplish on cybersecurity measures (Armitage & Cooper, 2021). This type of political incident cannot be repeated if Japan wants to prove its determination in pursuing cybersecurity.

The Yoshihide Suga and Fumio Kishida administrations which replaced the long serving Shinzō Abe administration have included cybersecurity as one of the main issues in their agendas. This development in policy prioritization is promising. However, these steps have been long due in the face of growing

tensions between superpowers. Most importantly, cybersecurity needs to be more concretely tied to national security. The cyber diplomacy initiative carries promise of improving Japan's national security, however, it is arguably a long-term strategy which may not be enough to protect Japanese interests during a major incident. There are many points that Ministry of Defense, METI, and MOFA can collaborate on. However, the most important role is on the shoulders of the government who has to actively push for more "cybersecurity as national security" message in a competent manner.

Conclusions

Cybersecurity is a new field and continuous change is the norm, rather the exception. It is of exceeding difficulty for states to keep up with the pace of evolution in the severity of threats and ICT technology in general. However, the critical significance of national security aspect of cybersecurity means that there is little choice for the nation states but to pursue continual improvement. In doing so, state shoulders responsibility alongside the private sector, civil society, academicians, and individuals. The case of Japan has been analyzed to lay out how the interactions between different states and initiatives taken by key policy implementation organs shape the state's role in cybersecurity. As the result of this undertaking, the following conclusions are derived.

1. Cybersecurity brings national security and industrial policy together; the roles Japanese state carry in cybersecurity reflect its general relation with industry which underwent great changes.

2. The most prominent roles Japanese state has been shouldering are those of the knowledge creator/disseminator, representative and supporter of society, and a partner to private sector.

3. Although not a complete list, there are steps Japan can afford to take towards a more robust cybersecurity presence which include but not limited to; human capital investments and putting forth of an actively involved government image.

A comprehensive discussion on whether the Japanese state is handling its roles well is left undiscussed here. This type of academic undertaking would require a through combing and analysis of performance data which would exceed the space and scope of this study. Furthermore, there is a myriad of issues this paper has not been able to focus on for the sake of clarity. As cybersecurity is a new field where interactions between the political and technical continuously take place, all in addition to countries differing in their policies and attitudes, there is almost unlimited research potential for those questions left out. By answering these questions in future studies, a deeper understanding of the role of the state in its differing forms and altitudes can be achieved while extending the scope of political science inquiry into the field of cybersecurity.

Conflict of Interest Statement

There is no financial conflict of interest with any institution, organization or person related to my article titled "Theoretical, Empirical, and Normative Dimensions of State Involvement in Cybersecurity: The Case of Japan".

References

Armitage, R., & Cooper, Z. (2021, November 14). *Japan should be admitted to the Five Eyes network*. Nikkei Asia. https://asia.nikkei.com/Opinion/Japan-should-be-admitted-to-the-Five-Eyes-network

Bernes, T., Brozus, L., Hatuel-Radoshitzky, M., Heistein, A., Greco, E., Sasnal, P., Yurgens, I., Kulik, S., Turianskyi, Y., & Gruzd, S. (2020, May 21). *Challenges of Global Governance Amid the COVID-19 Pandemic*. Council on Foreign Relations. https://www.cfr.org/report/challenges-global-governance-amid-covid-19-pandemic

Cavelty, M. D., & Egloff, F. J. (2019). The Politics of Cybersecurity: Balancing Different Roles of the State. *St Antony's International Review*, *15*(1), 37–57.

CISCO. (2020). *What Is Cybersecurity?* CISCO Homepage. https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html

Deibert, R., & Rohozinski, R. (2011). Contesting cyberspace and the coming crisis of authority. In *Access Contested: Security, Identity, and Resistance in Asian Cyberspace*. https://doi.org/10.7551/mitpress/9780262016780.003.0002

Engerer, H. (2011). Security As a Public, Private Or Club Good: Some Fundamental Considerations. *Defence and Peace Economics*, *22*(2), 135–145. https://doi.org/10.1080/10242694.2011.542333

Fukuyama, F. (1989). The End of History? *The National Interest*, *16*, 3–18.

Hatakeyama, K., & Freedman, C. F. (2010). Snow on the pine: Japan's quest for a leadership role in Asia. In *Snow on the Pine: Japan's Quest for a Leadership Role in Asia*. World Scientific Publishing Co. https://doi.org/10.1142/7534/SUPPL_FILE/7534_CHAP01.PDF

Higashi, C., & Lauer, G. P. (1990). *The Internationalization of the Japanese Economy* (2nd ed.). Springer Science+Business Media.

Honda, M. (2001). *Gendai nihon no seiji to gyōsei (Government and Politics in Contemporary Japan)*. Hokuju Shuppan.

Inoue, K. (2012, May 8). *Elpida and the Failure of Japan Inc.* Nippon.Com. https://www.nippon.com/en/currents/d00032/elpida-and-the-failure-of-japan-inc.html#

IPA. (2016, March 18). *Password Awareness Posters in Languages Used by ASEAN Member Countries*. Japan Information-Technology Promotion Agency. https://www.ipa.go.jp/security/english/passwordposter.html

IPA. (2017). *IPA/ISEC: Information Security Early Warning Partnership*. Japan Information Technology Promotion Agency. https://www.ipa.go.jp/security/english/about_partnership.html

Kawabata, E. (2006). *Contemporary Government Reform in Japan: The Dual State in Flux*. Palgrave Macmillan.

Kayama, K. (2015). *Kōdo hyōteki-gata kōgeki taisaku ni muketa shisutemusetsukei gaido ~ kansen suru koto o zentei to shita `bōgyo gurando dezain' ni muketa shisutemusetsukei no kandokoro ~ (System design guide for highly targeted attack countermeasures-The key points of system design for "defense grand design" on the premise of infection-).*

Khanna, D. M. (1997). *The Rise, Decline, and Renewal of Silicon Valley's High Technology Industry* (1st ed.). Routledge.

Klimburg, A. (2018). *The Darkening Web: The War for Cyberspace*. Penguin Books.

Lee, Y. W. (2008). *The Japanese Challenge to the American Neoliberal World Order: Identity, Meaning, and Foreign Policy*. Stanford University Press.

Liaropoulos, A. (2013). Exercising State Sovereignty in Cyberspace: An International Cyber-Order under Construction? *Journal of Information Warfare*, *12*(2), 19–26.

Lowenthal, M. M. (2019). *Intelligence: From Secrets to Policy* (Eighth). CQ Press.

Matsukawa, B., Flores, R., Remorin, L. A., & Yarochkin, F. (n.d.). *Top Countries With ICS Endpoint Malware Detections*. Trend Micro. Retrieved April 12, 2022, from https://www.trendmicro.com/en_be/research/21/f/top-countries-with-ics-endpoint-malware-detections-.html

Miyashita, A. (2008). Where Do Norms Come From? Foundations of Japan's Postwar Pacifism. In Y. Sato & K. Hirata (Eds.), *Norms, Interests, and Power in Japanese Foreign Policy* (pp. 21–46). Palgrave Macmillan. https://doi.org/10.1057/9780230615809_2

Myers, L. (2013, October 23). *Is this how Indonesia topped the malicious traffic charts?* WeLiveSecurity by ESET. https://www.welivesecurity.com/2013/10/23/is-this-how-indonesia-topped-the-malicious-traffic-charts/

Okimoto, D. I., Sugano, T., & Weinstein, F. B. (1984). Technological Resources. In D. I. Okimoto, T. Sugano, & F. B. Weinstein (Eds.), *Competitive Edge: The Semiconductor Industry in the U.S. and Japan* (pp. 35–77). Stanford University Press.

Osborne, C. (2021, April 1). *Google: North Korean hackers are targeting researchers through fake offensive security firm*. ZDNet. https://www.zdnet.com/article/google-north-korean-hackers-targeting-researchers-now-pretend-to-be-from-offensive-security-firm/

Personal Information Protection Commission, G. of J. (2019, October 11). *About the incorrect display of users' personal information that occurred on Amazon's mail order site (Japanese: Amazon no tsūhan saito de hassei shita riyōsha no kojin jōhō no go hyōji ni tsuite)*. Personal Information Protection Commission. https://www.ppc.go.jp/files/pdf/191011_houdou.pdf

Peters, B. G. (2005). *Institutional theory in political science: the "new institutionalism"* (Fourth). Edward Elgar Publishing.

PurpleSec. (2022). *2021 Cyber Security Statistics: The Ultimate List Of Stats, Data & Trends*. PurpleSec LLC. https://purplesec.us/resources/cyber-security-statistics/

Scopus. (2021, April 7). *Scopus - Analyze Search Results*. Scopus. https://www.scopus.com/term/analyzer.uri?sid=6e7586bbd400032e5385837b9747777f&origin=resultslist&src=s&s=TITLE-ABS-KEY%28cybersecurity%29+AND+PUBYEAR+%3E+2013+AND+PUBYEAR+%3C+2021&sort=plf-f&sdt=b&sot=b&sl=66&count=8572&analyzeResults=Analyze+results&txGi

Sigholm, J. (2013). Non-State Actors in Cyberspace Operations. *Journal of Military Studies*, *4*(1), 1–37. https://doi.org/10.1515/JMS-2016-0184

Suzuki, K. (2019). *Opening Speech of Cyber Initiative Tokyo 2019 on December 12, 2019*. Cyber Initiative Tokyo 2019. https://www.mofa.go.jp/mofaj/files/000550682.pdf

United Nations. (2022, April 7). *UN General Assembly votes to suspend Russia from the Human Rights Council*. UN News. https://news.un.org/en/story/2022/04/1115782

Waltz, K. N. (1979). *Theory of International Politics* (1st ed.). McGraw-Hill.

Watson, N. (2016). *US Election: Isolationism and Global Power*. Australian Institute of International Affairs. https://www.internationalaffairs.org.au/us-election-isolationism-and-global-power/

Web of Science. (2021). *Web of Science [v.5.35] - Citation Report*. Web of Science Website. https://apps.webofknowledge.com/CitationReport.do?product=WOS&search_mode=CitationReport&SID=F1EceKdecdlogQLOM34&page=1&cr_pqid=6&viewType=summary

Genişletilmiş Özet

Siber güvenlik yeni bir güvenlik alanıdır ve bu alanda sürekli değişim istisnadan ziyade bir normdur. Siber tehditlerin ve genel olarak bilgi iletişim teknolojilerinin (BİT) evrim hızına ayak uydurmak devletler için oldukça güç bir girişimdir. Bununla birlikte, siber güvenliğin ulusal güvenlik için kritik önemi, ulus devletlere sürekli kapasitelerini ve araçlarını iyileştirmeyi sürdürmekten başka çok az seçeneğin olduğu anlamına gelmektedir. Bu tür iyileştirmeleri yürütürken, devlete ek olarak özel sektör, sivil toplum, akademisyenler ve bireyler de siber güvenlik alanında sorumluluk üstlenir. Bununla birlikte, ulus-devletin Soğuk Savaş sonrası dönemde geri dönüşü olgusu, güvenlik alanında güçlü bir yankı uyandırmaktadır. Kuzey Atlantik Antlaşması Örgütü (NATO) veya Avustralya, Birleşik Krallık ve Amerika Birleşik Devletleri (AUKUS) arasında yakın zamanda başlatılan üçlü güvenlik anlaşması (AUKUS) gibi uluslararası güvenlik ittifakları kuruluşlarının varlığına rağmen, hâlâ ulusal güvenliğin sağlanması birincil sorumluluğudur. Realist uluslararası ilişkiler teorisi tarafından tanımlandığı gibi, uluslararası siyasi sistemin temel düzenleyici ilkesi, bireysel devlet aktörlerinin tabi olma ilişkileri sergilemediği ve yalnızca değişen yetenekleriyle ayırt edildikleri anarşidir. Bu görüş, çeşitli güvenlik aktörleri arasında

büyüklüklerine, organizasyonel karmaşıklıklarına ve ulus devletin listenin başında olduğu kalıcılıklarına göre bir sıralama oluşturulmasına izin verir.

Japonya örneği, farklı devletler arasındaki etkileşimlerin ve kilit politika uygulama organları tarafından alınan inisiyatiflerin devletin siber güvenlikteki rolünü nasıl şekillendirdiğini ortaya koymak için analiz edilmiştir. Devletlerin siber güvenliğe katılımlarını nispeten daha fazla ulusal güvenlik yönüne (ABD gibi) yönlendirdiği ileri sürülebilecek diğer büyük liberal demokratik ülkelerden farklı olarak, Japonya'da devletin siber güvenlik alanındaki rolü daha az net bir yönelime sahip olduğu gözlemlenmektedir. Bu çalışmada Cavelty ve Egloft'un (Cavelty ve Egloft, 2019) geliştirdiği analiz çerçevesi kullanılarak Japonya'da devletin siber güvenlikteki rolünün doğasını açıklamaktadır. Bahsedilen bu analiz çerçevesinde devletin rolü teorik, ampirik ve normatif boyutlarda analiz edilmektedir.

Başlangıç olarak teorik boyut analizi, Japon devleti ile ilgili literatürdeki farklı teorilere odaklanmaktadır. Sırası ile, ampirik boyut analiz yürütülmekte ve bu analiz için gerekli veriler, siber güvenlikle ilgili önemli Japon devlet ve özel kuruluşlarının kamuya açık kayıtlarından alınmaktadır. Bu ampirik örneklere dahil edilen veriler, örneğin, "toplumun destekçisi ve temsilcisi olarak devletin" bazı ilkelerinin benimsenmesi, Dışişleri Bakanlığı (MOFA) girişimlerinde de belirgin hale getirilmesini içermektedir. Özellikle MOFA'nın politika girişimleri ve projeleri, Japon devletinin uluslararası sahnede toplumun temsilcisi rolünü nasıl benimsediğine dair örnekler sunulmaktadır. Japonya 'hukukun üstünlüğü', 'güven artırıcı önlemler' ve 'kapasite geliştirme desteği'ni teşvik ediyor ve bu üç sütun Japonya'nın siber diplomasisinin temel direklerini oluşturuyor. Son zamanlarda diğer birçok ülkede yaygınlaşan siber diplomasi, siber güvenliğin ulusal güvenlik boyutundan ortaya çıkan ve dış ilişkilerin ülke çıkarları doğrultusunda ele alındığı gelişmiş bir siber siyasi ortam arayan bir kavramdır. Japonya örneğinde, siber uzayda açık ve kesintisiz diyalog ve işbirliğini sürdürmeye yönelik politikaların benimsenmesi, daha yeni diplomasi araçlarının kabulü olarak yorumlanabilir. Örnekler arasında ayrıca, 2019'daki Amazon olayı ve 2021'deki LINE olayı ile ilgili olarak İçişleri Bakanlığı'nın bakanlık ile Kabine arasındaki koordinasyonu da sayılabilir.

Vaka analizinin son parçasını oluşturan normatif boyut analizi, Japon devletinin dikkat sarfetmesi gerektiği düşünülen siber güvenlik politikalarının zaman ufku yönünü vurgulamaktadır. Sonuç olarak, Japon devletinin "bilgi yaratıcısı/yayıcı", "toplumun destekçisi/temsilcisi", "ortak" ve "garantör ve koruyucu" rollerini bünyesinde barındırdığı ve devlet kurumlarının Japonya'da daha iyi siber güvenlik için proaktif uzun vadeli politikalar ve girişimlere yönelmesi gerekliliği tespit edilmektedir.