ISSN 2580 6378
E-ISSN 2580 7048

JURNAL ASIA PACIFIC STUDIES

Journal of International Relations Study Program
Faculty of Social and Political Sciences
Universitas Kristen Indonesia

Volume 4 | Number 2 | July - December 2020

Jurnal Asia Pacific Studies
https://doi.org/10.33541/japs.v4i2.2800

Volume 4 Number /July - December 2020
pp. 100-111

STRATEGIC ANALYSIS OF CAPACITY BUILDING FOR THE CYBER SECURITY OF THE UNITED STATES IN ASIA

Seiko Watanabe

Yokohama National University, Yokohama, Kanagawa Japan

seikowatanabynu@gmail.com

Abstract

In recent years, cyber-attacks in virtual spaces have been rapidly increasing, and modern centralized states have proven to be incapable of effectively responding to cyber-attacks on their own. To resolve cyber issues, the United States has started cooperating with allied countries such as Japan and the ASEAN countries through Capacity Building (CB). Cyber-attacks include online and physical infrastructures, often referred to as electronic warfare and "hybrid wars." In this paper, I show the importance of revisiting deterrence theory for cyber security issues. Deterrence theory derives from a traditional International Relations (IR) theory, realism, which emphasizes that states always act to maximize military power. However, in explaining the CB in cyberspace, key concepts and different theoretical frameworks which both scholars of liberalism and neoliberalism advocate, must be incorporated because not only military power, but also economic power has to be taken into account. This paper takes the United States as one case in which infrastructural support in cyberspace is observed. More specifically, I argue that in order for CB to happen, cooperation in cyberspaces must emerge, especially in the realm of economy, legislation, and military support to allied countries. This paper intends to determine the utilities of cyber CB. To do so, I collected data from more than 200 countries and inspected the correlations between cyber-attacks and CB using statistical software R. I also examines other factors such as Internet population, GDP growth rate, war expenditures, economy, military, and law regimes, to determine which are statistically significant in mitigating cyber-attacks.

Keywords: cybersecurity, international relations, realism, liberalism, capacity building

Abstrak

Dalam beberapa tahun terakhir, serangan siber dalam ruang virtual telah meningkat pesat dan negara terpusat modern telah terbukti tidak mampu me-respon secara efektif oleh negara kesatuan. Untuk menyelesaikan masalah cyber, Amerika serikat bekerja sama dengan negara sekutu seperti Jepang dan ASEAN melalui *Capacity Building* (CB). Serangan siber mengintegrasikan infrastruktur online dan fisik, sering disebut sebagai peperangan dan "perang hibrida". Istilah-istilah ini secara khusus merujuk pada pertempuran menggunakan operasi militer dan tekanan ekonomi. Selain itu, dalam situasi seperti itu, sulit untuk mengidentifikasi penyerang yang melakukan serangan tersebut mengingat sifat dari anonimitas online. Dalam makalah ini, sarjana dalam studi sebelumnya menggunakan teori pencegahan berdasarkan Realisme pada penelitian Keamanan Siber. Realisme, teori Hubungan Internasional, telah didirikan di bidang Hubungan Internasional untuk negara-negara yang mendukung status quo agar memaksimalkan kekuatan politik dan kekuatan militer mereka. Namun *Cyber Capacity Building* ternyata bukan hanya realisme tapi juga Liberalisme dan Neoliberalisme, yang menekankan kekuatan ekonomi, yang terbukti di dunia maya. Khususnya, Amerika serikat mengarahkan dukungan siber melalui kerja sama dengan menggunakan kekuatan ekonomi, perundang-undangan, dan memberikan dukungan militer kepada negara-negara sekutu. Untuk menentukan keperluan *Cyber Capacity Building*, makalah ini bermaksud untuk meneliti secara kualitatif dan kuantitatif pada CB. Untuk melakukan hal tersebut, makalah ini mengumpulkan data dari lebih dari 200 negara dan memeriksa pemanfaatan indeks korelasi bahasa pemograman R. Dengan mengamati variabel tujuan dengan jumlah komputer yang terinfeksi setelah penyerangan siber, kami menemukan faktor lain seperti populasi Internet, tingkat pertumbuhan GDP, pengeluaran perang, ekonomi, militer, dan rezim hukum yang berguna dalam mengurangi serangan siber.

Kata Kunci: keamanan siber, neoliberalis, studi keamanan, *Capacity Building*

1. Introduction

Cyber-attacks have been increasing, causing political instabilities among many countries. Tremendous damage continues to be perpetrated on companies and organizations. As fake news issues illustrate when Russia allegedly intervened in the UK Brexit election, the issues related to cyber-attacks have become more complex than what it used to be; hence, the global trend of cyber-attacks seems to be on the rise. Cyber-attacks mean attacks on both physical spaces where we, human beings, live and virtual spaces where many controls over infrastructures and our human life have been operation. Some call it electronic warfare, and others use the term “hybrid” war, specifically referring to fighting with military campaign means and economic pressure. It is difficult to identify an assailant who has carried out a cyber-attack given the possibility of anonymity and deception online.

1.1. Background

After the 1960s, the Internet spread rapidly worldwide. Internet literacy has improved so much that the majority of the world’s population could access the Internet in 2018 (United Nations Population Division 2019). Nowadays, the Internet has become an essential medium for both formal and informal communication. International Relations (IR) scholars such as Wilhelm (2000, 14) have noted that the Internet is both a virtual and cognitive space, which is distinct from reality. However, as technologies have developed, the Internet has become an essential tool across all fields, including business, politics, and society. According to a report created by the Ministry of Internal Affairs and Communications in Japan (2016), both developed and developing countries and private organizations have invested in Information Technology (IT) services. The report notes that the index of growth until 2016 was predicted to be 5.4%, and investments were projected to increase in the future. A technical report issued by the Information and Communication Technology (ICT) also says that the investments made by the United States and France in 2015 were ten times larger than that of 1980. In 2015, the ICT attributes to investments of the United States and France, which were compared to those from 1980, and a tenfold increase was observed. Additionally, the Ministry of Internal Affairs and Communications in Japan reported that Japanese investments approximately doubled within the same timeframe. Communication has become cheaper, and the transaction cost has become almost free with the Internet. It is commonly understood that the Internet has become a global infrastructure; therefore, it is impossible to separate the Internet from our society and daily life.

However, in recent years, malign cyber-attacks such as hacking and the stealing of personal information have highlighted problems with the Internet through two main avenues: fake news and data collection. Fake news is the intentional manipulation of public opinions or facilitation of propaganda movements (Khaldarova and Pantti 2016, 893). Through fake news, spin-doctors manipulate public opinion, which in turn causes confusion among the population. A prominent example is the diffusion of fake news stories supporting U.S. presidential candidate Donald Trump via Facebook (Wilhelm 2000, 245). Fourney and Miklos (2017, 3) pointed out that Cambridge Analytica collected personal information via the “big five” with the purpose of academic investigation, in turn providing useful strategies to then-candidate Trump. The big five is a Facebook application obtaining personal information without permission. It is said that the techniques used by the big five led Trump to victory in the U.S. presidential election through effective advertisements based on data analyses (Khaldarova and Pantti 2016, 893). The analysis followed three methods: the analysis of eligible voters’ preferences, the analysis of big data regarding society, and advertisements matching individual preferences. In addition, Cadwalladr and Graham-Harrison note that Brexit in the

UK was affected by Russian cyber maneuvering (2018). Given this, developing capabilities of countermeasures against these cyber-attacks is an urgent global issue. My paper addresses the question of how these cyber-attacks can be prevented from happening and what countermeasures are available on a global scale.

1.2. Research Question

The U.S. Government carries out a comprehensive policy to include USA allies. In *US-Japan Relations and Southeast Asia* (Limaye and Kikuchi 2016,15), authors state that the cyber situations in accordance with the military balance in the Indian Pacific region play a vital role, and United States' allies such as Japan, Australia, and ASEAN heavily rely on the United States. In effect, the United States actually supports CB for Southeast Asian countries under the Japan-U.S. alliance. Cyber support based on the Japan-U.S. alliance for the ASEAN countries valid as well as for corporations from Australia, which the United States recognizes to be an important ally. This paper will employ statistical analysis to determine the relationship between cyber-attacks and Capacity Building using the software R. The following sections explore key important variables, such as GDP growth, armaments, the degree of the democracy, and military spending to see the correlation between infection Counts (the PC which received a cyber-attack and was transmitted) and cyber-attacks. The chapter sees the coefficient of the correlation of Capacity Building (i.e. the capability of cyber) and its efficiency. Hence, a central question in this article asks; Is CB correlated with decreasing cyber-attacks? The hypothesis that I have specifically tested is that the measure of Capacity Building should be associated with cyber-attacks, resulting decreases of the cyber-attack.

2. Literature Review

This section surveys the literature in the field of cybersecurity studies. A number of studies suggest that cyber threats across academic disciplines, including the study of computers, media, literature, engineering, and policy (Sobiesk 2017, 43). However, IR studies are limited only to address real political situations, failing to explain politics happening in virtual spaces and developing inappropriate theories, despite the present circumstance of cyber-attacks being emergent. According to Eriksson and Giampiero (2006, 221), very few attempts have been made to apply IR theory in analyzing these cyber securities' problems. Research that has focused particularly on aspects of the creation of information-age security threats has not been produced enough and a lot of theories and concepts are outdated. Only a few scholars have introduced deterrence theory and applied it to the issues of cyber warfare and cyber security. The following section introduces some of the theories relevant to cyber warfare and CB with alliance politics.

2.1. Cyber Wars

Thomas Rid would be one of the pioneering scholars who have shaped the field of study and formulated an analysis of cyber war. His book, Cyber War Will Not Take Place (Thomas 2013, 75), states that cyber is the "fifth domain" of warfare. However, the author proposed that cyberwar have never occurred before and will not break out in the future as well. He summarized a cyberwar as comprising a potentially lethal, instrumental, and political act of force conducted through malicious code. Rid also provided nuanced terminology for cyberattacks. All cyberattacks are merely refined versions of three activities: sabotage, espionage, and subversion. He defined wars as triggering lethal problems, which is not observed in cyberspace. Rid also argues that this core issue in cyber is a political issue rather than a technical matter (Thomas 2013, 102).

A similar notion has been advanced by Clit et al. In their book, Cyber war versus cyber realities: Cyber conflict in the international system, Watts (2018, 58) discusses that nations politically utilizes cyberattacks, which can yield a high return for low costs for nations. He claimed that the offensive nation in a cyberattack agitates people, creating disruptive social movements in defensive countries through cyber-attacks such as fake news. Several lines of evidence indicate that some malefactors abuse the information on users' family members, friends, and colleagues that is available on social media and identify their preferences and personal information for specific purposes. The author also alarms that cyber-attacks with artificial intelligence will be used in the near future.

2.2 Deterrence Theory and Alliances for Cyber Security

Recently, a decent number of IR scholars have reexamined the usefulness of Deterrence Theory, emphasizing its value for applying the theory to many cyber issues I have pointed out in the previous section. Today, in the arena of cybersecurity, scholars have begun to consider whether the concepts and specific strategies proposed in Nuclear Deterrence Theory might be applicable since the theory could fill the gap between what is happening in cyber spaces and policy discussions in the academia. Nuclear Deterrence Theory was developed during the Cold War, which is a theory that explains patterns – similarities and differences – in nuclear states and their policy outcomes. Several studies suggest that nuclear weapons can ensure the security of the country. According to a nuclear deterrence theorist who wrote "A theory of security strategy for our time: Defensive Realism'' (Shiping 2014, 28), global political stability can be accomplished because countries know that the costs of using nuclear weapons are greater than the gains. In addition, the idea of Mutually Assured Destruction (MAD) serves as a base for the offense-defense theory, which is an essential defensive realist theory. Defensive realists, one of IR school scholar, making a similar argument that a nuclear umbrella is a safeguard against a non-nuclear allied state because structural realists, especially defensive realists assume that states support the status quo to maximize political and military power. Deterrence Theory suggests that nations, especially nuclear states, prepare for external threats and defend their allies from the threats. However, the issue with this theory is that states are not fully capable of identifying the source of threats, here I mean cyberattacks because whoever uses T can disguises their Information Provider (IP) addresses.

Despite the anonymous IP address through Tor, much of this variation in the results can be attributed, shining new light on these debates through an examination of cyber-attacks. With the theory of deterrence and the logic used in the MAD, I attempt to create room for a new debate and study on cyber-attacks because they serve as a base for the offense-defense theory. The offense defense theory suggests that even smaller allied countries benefit from being allied with nuclear states and can ensure the safety of cyberspace. Seeking to explain high engagements from cyber-developed states into capacity building for less cyber-developed countries, deterrent theorists such as Torrence argue that a strong desire to deter external nuclear threats drives certain states to build capacities and do attack through cyber methods (Torrence 2017, 185). Scott (2017, 19) states that countries that foresee the possibility of the compromising or even destruction of their infrastructure or financial institutions or fear cyberwar ally with one another prepare for such attacks.

2.3 Liberalism and Capacity Building

In spite of the fact that research regarding present cyber security is derived from the Deterrence Theory of Realism (Scott 2017, 19), liberalism perspectives on cyber security also exist because economic Capacity Building is present. According to Gilpin (2016, 59), Liberalists has been subject to intense economical debate that a market arises spontaneously in order to satisfy human demands. In the following sections, the types of capacity building are explained in details.

3. Research Design

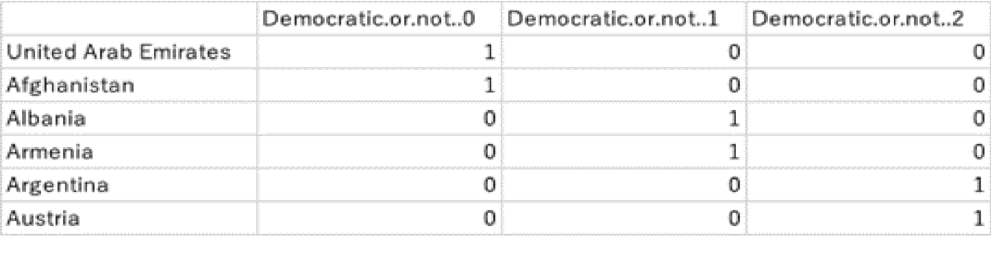
My central hypothesis concerns the relationship between the number of cyber-attacks and degree of cyber CB. Several analyses of the cyber-attack data, collected from the websites of International Telecommunication Union (ITU), military balance, and (IMF) are presented below.

3.1. Research Findings

Figure 1 shows significance probability between cyber-attacks and capacity buildings by using R programming language. The correlation coefficient represents the correlation between the numbers of Capacity Building and infected PCs, suffering from cyber-attacks. The data I utilized is the infection count, which is the number of computers infected by cyber-attacks, and the capacity building representing the ability of cyber securities. Survey collected information from ITU, Military Balance, and IMF websites. This data has the infection count of the computers infected by cyber-attacks in 204 countries.

Then, I run a multiple regression analysis, setting the number of the infected computers as a purpose variable and, set the followings as explanation variables: the Internet population, a GDP growth rate, the war expenditures, the degree of democracy, an index of the cyber security, and military spending costs. In this section, I investigate the causality of the data with multiple linear regression analyses. This section carries out a conversion of "democratic or not" which are variable of the factor type in the following figure. The following has established a dictatorship system wherein 0 is a dictatorial government, and 1 is a mixed government between dictatorial and complete/defect democratic nations.

Figure 1. Defect or A Complete Democratic Nation



	Democratic.or.not..0	Democratic.or.not..1	Democratic.or.not..2
United Arab Emirates	1	0	0
Afghanistan	1	0	0
Albania	0	1	0
Armenia	0	1	0
Argentina	0	0	1
Austria	0	0	1

Also, Figure 2 indicates a defect or a completely democratic nation. The purpose variable is the number of infected computers by cyber-attack. The explanatory variables are the number of the Internet users, GDP growth, armaments (Active Armed Force), the degree of the democracy, and military spending (performed a multiple regression analysis as military expenditure to the GDP ratio). By utilizing the above factors, multiple linear regression analysis reaches the following conclusion.

Infection Count=144557-1830×InternetPopulationPercent-5401×GDP growth+466×Active Armed Force-98616 × Democratic.or.not..0-50493×Democratic.or.not..1+100818 × Scores of Global cybersecurity index -3512 × Military expenditure (% of GDP)

The above formula indicates that the number of cyber-attacks becomes small when the followings are larger: the number of Internet users, the GDP growth, military budget. In addition, the number of cyber-attacks decreases when the followings are small: the democratic coefficient, the dictatorship system, mixed political system. The tendency that the computers in a dictatorship system and the mixed political nations are not attacked by hackers might be explained that these countries are not economically rich compared with developed nations. It might be assumed that these low levels of infected computers in a dictatorship system and the mixed political nations are because these countries are not economically matured compared with developed nations. Hence, the analysis is limited to employ ineffective factors above mentioned. Overall, the formula reveals that the population of the Internet, the GDP growth figure, and the military budget play a vital role in decreasing cyber-attacks.

4. Capacity Building: Military Power, Economic Power, and Norms

The purpose of this section is to illustrate what constitutes of cyber CB. I argue this from military, economic, and governance perspectives. The CB, as a concept itself, is derived from the UN's Agenda 21. It aims at stabilizing cyber conflicts worldwide. The UN's Agenda 21 is an action plan wherein international society should cooperate in addressing the increased numbers of cyber-attack cases on a global scale. Also, the Agenda 21 (1992) was established for creating a sustainable society in which developed countries such as the United States and other European countries would be able to help developing countries. Accordingly, CB is intended to strengthen the cyber capabilities of respective sovereign countries as a public-private sector joint model. This has meant to serve not only for governments but also private organizations and Non-Governmental Organizations (NGOs), as well. However, in cyber security, the decision-making process and decision itself has to be extremely top-down among countries to reach bilateral and multilateral agreements. Therefore, it is said that mutual trust is necessary for countries to cooperate together.

As for conceptual clarity for CB, I incorporate three aspects of CB construction, which often is rigorously discussed in the field of grand theory, to advance the existing conceptual framework: (1) military, (2) economic, (3) governance capacity. Table 1 shows a summary of the respective conceptual components.

Table 1. Capacity Building (CB) Concepts

Types	Explains	Applicable IR Theory
CB for military affairs	Conducting operations, conflict prevention, and doctrine enforcement	Realism

CB for economics	Providing financial support to share the same Internet infrastructures and technologies	Liberalism, Neoliberalism
CB for administration/ norms of law enforcement	Helping developing countries' systems of law enforcement	

An IR scholar, Hall (2005, 67) sought to trace the source of military capacity for international peace, claiming that as realists propose. On the other hand, neoliberalists such as Gilpin (2016, 59) argued that the economy has greatly relied on nations' relationships. In addition, Capacity building for aids developing countries' systems of law enforcement plays an important role in geopolitics by increasing capacities (Greenwood 2012, 129). Hence, the stability of international relations is delivered via CB.

4.1. Military Capacity Building

It is not surprising that the Deterrence Theory in Realism can also apply with Capacity Building for the balance of power in cyber security. Sanger (2018, 57) laid out that building military capacity aims to enforce armed exercises, prepare for cyber-attacks from enemies, conduct operations, prevent conflict, and enforce doctrine, which is the same as traditional Realism. Hall (2005) evaluated Realist theories as being mainly attributed to armed powers. According to Akimoto in *The Diplomat* (2012), ASEAN states concur with Japan to boost their cyber capabilities. In fact, according to CCDCOE (2019), Singapore's new ASEAN Cyber Capacity Program was established, initiating ASEAN Ministerial Conference on Cybersecurity in October 2016. The Philippines also announced the launch of a cybersecurity working committee within the ASEAN Defense Ministers Meeting Plus in 2016. Another key movement for cyberspace is the ten-million-USD ASEAN Cyber Capacity Program (launched by Singapore in 2016). This program enhances cybersecurity expertise across the region. In order to pursue a peaceful cyber world, the program also launched the Singapore-ASEAN Cybersecurity Centre of Excellence in 2019. The center is based in Bangkok at the ASEAN-Japan Cybersecurity Capacity Building Centre, launched in September 2018, which seeks to prevent cyberattacks. Almost 700 of the cybersecurity personnel who work there are from Southeast Asia and have graduated from Japanese-designed programs that include instruction in cyber defense, digital forensics, and malware analysis.

4.2. Economic Capacity Building

Capacity building has a different meaning; it serves to develop economy in both countries, those that are CB providers as well as receivers. Capacity building for economics aims to improve Information communications technology (ICT) for allied nations in order to be a buoyant economy. This idea is grounded in Liberalism, a concept of International Relations, in which the economy greatly influences nations' relationships. According to Gilpin (2016, 59), Liberalists have been subject to intense economical debate that a market arises spontaneously in order to satisfy human demands. CB also aims to satisfy citizens' demands by aiding cyber infrastructure between developing countries and developing nations. For example, according to the U.S. Department of House (2019), the United States determined to enforce relations with ASEAN through strong partnership, providing information communications technology (ICT) environment for economic prosperity. Siripong (2019,55) provides that the erection of boosting information structures' investments led to a robust economy since managing information is necessary for cyber-developing countries. In fact, cyber capacity building and digitalization of the infrastructures generate a buoyant economy, concluding with enthusiasm that the United States accelerates CB to allied nations such as ASEAN and Japan. By doing so, the United States has built policy and strategy-building capabilities within ASEAN member states through workshops, seminars, and conferences, in collaboration with partners such as Japan, government agencies, industry players, and Non-Governmental Organizations (NGOs), including the US Department of State and the MITRE Corporation, Cyber Law International. According to Japan-ASEAN Integration Funds (JAIF), in December 2017, both Japan and ASEAN determined that they would establish a training center including training for 44 individuals from ASEAN countries to learn the ins and outs and fill the knowledge gap.

4.3. Governance Capacity Building

Lastly, capacity building is related to the governing body and the quality of the governance systems of the two countries involved. Capacity building for administration and norms aids developing countries' systems of law enforcement, improving a whole society. An empirical study by Greenwood (2012, 129) reveals that rules play a vital role in society, providing people with perspectives about how they should behave. By doing so, developing nations would be able to leave a category of periphery states (dependency theory) and partially join in a group of core states, thus the enforcement of rules of laws would be improved even in developing countries. For instance, according to McGuinness (2017), the Estonian government, which is a cyber-developed country, emphasizes the importance of capacity building for fighting cybercrime, and it introduced the European Council Convention on Cybercrime (also known as the Budapest Convention) to developing countries. Estonia and partner institutions from the United Kingdom and the Netherlands have been supporting the cyber development of countries in Africa and Asia. The Cyber Resilience for a Development project will last until June 2021; the project appears in the cybersecurity yearbook published by the Estonian Information System Authority. The purpose of the mission is to increase awareness about cybersecurity from Estonia, assisting in fostering cyber strategies and action plans, enhance the capability of the teams for handling cyber incidents, and share the experience with providers of vital services and institutions of the state. Same as European countries, the United States regards the well governed society by rules as legitimate nations. As U.S Indio-Pacific Command (2019) puts it: law Enforcement is critical in domain areas including sea, land and cyber.

5. Conclusion

The prevalence of cyber-attacks in the 21 century would be mainly the result of lack of Capacity Building (CB) across the globe, and the United States as a global hegemon although it is in decline, should be responsible for global CB policy in order cyber security function properly. First, this paper has introduced the idea that cyber-attacks have two characteristics: (1) attacks on a nation's decision-making capabilities without weapons, and (2) attacks on important infrastructure with weapons given the nature of online anatomy. Furthermore, this paper has pointed out that it is difficult to identify an assailant who has exerted a cyber-attack. Second, this paper has introduced the deterrence theory and applied it to cyber issues. Also, this paper has shown that the relationship between Capacity Building and cyber-attacks was not statistically significant by examining the means of collecting data from more than 200 countries and inspected the correlation index in the R programming language. It has also done so by observing purpose variables with the number of infected PCs by a cyber-attack and other factors such as Internet population, GDP growth rate, war expenditures, economies, and military and political regimes. Third, this paper has briefly introduced the ongoing CB building between the United States and allied nations such as ASEAN and Japan by looking at three aspects of CB—change in military assists to an ally country, economic power, and legislation. The United States and those in alliance with it engage heavily in cyber space, which is geopolitically important.

REFERENCES

Book

Greenwood, Nicholas. 2012. *World of Our Making: Rules and Rule in Social Theory and International Relations.* London: Routledge

Gilpin, Robert. 2016. *The Political Economy of International Relations.* New Jersey: Piston University

Hall, Martin. 2005. *Essence of diplomacy.* New York: Springer

Limaye, Satu, and Tsutomu, Kikuchi. 2016. *US-Japan Relations and Southeast Asia: Meeting Regional Demands.* Washington: East-West Center

Sanger, David. 2018. *The Perfect Weapon: war, sabotage, and fear in the cyber age.* Melbourne: Scribe Publications

Scott, Jasper. 2020. *Strategic Cyber Deterrence: The Active Cyber Defense Option.* Maryland: Rowman & Littlefield

Shiping, Tang. 2014. *A Theory of Security Strategy for Our Time: Defensive Realism.* London: Palgrave Macmillan

Torrence, James. 2017. *Strongpoint Cyber Deterrence: Lessons from Cold War Deterrence Theory & Ballistic Missile Defense Applied to Cyberspace.* New York: Xlibris Corp

Thomas, Rid. 2013. *Cyber War Will Not Take Place.* Oxford: Oxford University

Watts, Clint. 2018. *Messing with the Enemy: Surviving in a Social Media World of Hackers, Terrorists, Russians, and Fake News.* New York: Harper

Wilhelm, Anthony. 2000. *Democracy in the Digital Age: Challenges to Political Life in Cyberspace.* London: Routledge

Journal

Eriksson, Johan, and Giampiero, Giacomello. 2006 "The Information Revolution, Security, and International Relations: (IR) Relevant Theory?." I*nternational Political Science Review* 27:221-224.

Khaldarova, Irina, and Mervi, Pantti. 2016. "Fake News. The Narrative Battle Over the Ukrainian Conflict." *Journalism Practice* 10: 891-901.

Ratner, Ely. 2013 "Rebalancing to Asia with an Insecure China." *Washington Quarterly* 21-38.

Website

Akimoto, Daisuke. 2012. "Japan's Emerging 'Multi-Domain Defense Force'" *Diplomat,* Accessed on 2 April 2020. https://thediplomat.com/2020/03/japans-emerging-multi-domain-defense-force/

Cadwalladr, Carole, and Emma, Graham-Harrison. 2018. "Cambridge Analytica: Links to Moscow Oil Firm and St. Petersburg University." Accessed on 5 February 2019. https://www.immagic.com/eLibrary/ARCHIVES/GENERAL/GMGP_UK/G180 3 17G.pdf

CCDCOE. 2019. "ASEAN Cyber Developments: Centre of Excellence for Singapore, Cybercrime Convention for the Philippines, and an Open-Ended Working Group for Everyone.” Accessed on 25 February 2019. https://ccdcoe.org/incyder-articles/asean-cyber-developments-centre-of-excellence-for-singapore-cybercrime-convention-for-the-philippines-and-an-open-ended-working-group-for-everyone/

Fourney, Adam, and Miklos, Racz. 2017. “Geographic and Temporal Trendsin Fake News Consumption During the 2016 US Presidential Election.” Accessed on 12 April 2017. http://erichorvitz.com/CIKM2017_fake_news_study.pdf

International Monetary Funds (IMF). 2020. Accessed on 15 March 2020. https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD

International Telecommunication Union (ITU). 2020. Accessed on 16 March 2020. https://www.itu.int/en/Pages/default.aspx

Japan ASEAN integration funds. 2019. Accessed on 15 December 2019. https://jaif.asean.org/support/project-brief/asean-japan-cybersecurity-capacity-building-centre.html

McGuinness, Damien. 2017. “How a cyber attack transformed Estonia.” *BBC News,* Accessed on 17 April 2017. https://www.bbc.com/news/39655415

Ministry of Economy, Trade and Industry. 2019. “Japan - US Industrial Control Systems Cybersecurity Training for Indo-Pacific Region Held.” Accessed on 25 October 2019. https://www.meti.go.jp/english/press/2019/0912_002.html

Ministry of Foreign Affairs in Japan. 2019. Accessed on 15 December 2019. https://www.mofa.go.jp/mofaj/press/release/press4_007911.html

Ministry of Internal Affairs and Communications in Japan. 2017. Accessed on 12 December 2019. https://www.soumu.go.jp/johotsusintokei/whitepaper/ja/h30/html/nd251300.html

Military Balance. 2017. Accessed on 12 December 2019. https://www.iiss.org/publications/the-military-balance

Prime Minister of Japan and his Cabinet. 2013. “ASEAN-Japan Ministerial Policy Meeting on Cyber Security Cooperation.” Accessed on 25 February 2013. https://japan.kantei.go.jp/96_abe/actions/201309/12asean_e.html

Sobiesk, Edward. 2015 “Cyber Education: A Multi-Level, Multi-Discipline Approach.” *Proceedings of the 16th Annual Conference on Information Technology Education,* Accessed on 2 April 2020. file:///C:/Users/owner/AppData/Local/Packages/Microsoft.MicrosoftEdge_8wekyb3d8bbwe/TempState/Downloads/2808006.2808038%20(1).pdf

Siripong, Charoensuk. 2019. “The Impact of the Internet on Buyer Behavior in Globalization.” Accessed on 25 October 2019. https://www.academia.edu/14035361/The_Impact_of_the_Internet_on_Buyer_Behavior_in_Globalization_The_Case_of_Thai_Telecommunication_E-Services_บทคั_ดย_อ

United Nations Population Division. 2019. “World Population Prospects: 2019 Revision.” Accessed on 1 April 2020. https://data.worldbank.org/indicator/SP.POP.TOTL?end=2018&start=1960&view=chart

U.S. Department of State. 2019. “Co-Chairs’ Statement on the Inaugural ASEAN-U.S. Cyber Policy Dialogue.” Accessed on 25 October 2019. https://www.state.gov/cochairs-statement-on-the-inaugural-asean-u-s-cyber-policy-dialogue/

U.S. Indo Pacific Command. 2019. "The United States and ASEAN: Expanding the Enduring Partnership." Accessed on 25 October 2019. https://www.pacom.mil/Media/News/News-Article-View/Article/2010406/the-united-states-and-asean-expanding-the-enduring-partnership/

White House. 2018. "The Cost of Malicious Cyber Activity to the U.S. Economy." Accessed on 25 February 2019. https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf