International Conference on Business Economics, Social Sciences & Humanities

CONSTRUCTIVIST THEORY IN ANALYZING CYBERWAR BETWEEN THE UNITED STATES AND CHINA

Kharisma Putri Nur Fatima
Department of International Relations, Universitas Komputer Indonesia, Bandung, Indonesia

Dewi Triwahyuni
Department of International Relations, Universitas Komputer Indonesia, Bandung, Indonesia

ABSTRACT

This research aims to analyze cyberwar between the United States and China based on a constructivist perspective. Constructivism is an alternative view that offers the basic idea that international structure is a social construction. By using a qualitative approach, the results of this research show that according to a constructivist perspective, cyberwar is seen as anarchy, which means that war in cyberspace will remain a fantasy if the United States views China cooperatively. On the contrary, cyberwar will become a reality and have the impact of becoming a real war if the United States views China in a conflictual manner. The conclusion is, to ensure peace in cyberspace, the two countries need to interact with each other, so that there will be similarities in perception which can foster an attitude of mutual understanding, shared norms, and respect for identity which ultimately changes their perception as friends rather than enemies.

Keywords: China, Constructivism, Cyberspace, Cyberwar, United States

INTRODUCTION

Basically, in International Relations, any form of space that provides opportunities to expand power and influence in the political world can become an important variable, when the activities of one actor in that space threaten the sovereignty, stability or security of other actors. The term “space” refers to interactions that give rise to potential sources of power, provide expansion of influence and advantage, and realize further potential if strengthened and maintained by technological advances. Cyberspace refers to interconnected global electronic media that facilitates online communication and information exchange.

Research on cyberwar between the United States and China is important to understand the dynamics of technological change, developing cyber capabilities, and their impact on national security and social stability. Cyberwar has become part of modern warfare, and cyber space is increasingly used by both countries to achieve some of their goals in the fields of defense, economics, and politics.

The cyberwar conflict between the United States and China began with a situation of mutual accusations leveled against each country. Both countries consider that security in cyberspace is as important as security in physical space. So, the United States and China signed a security agreement in cyber space. However, as if it had never happened, the United States suspects and accuses China of carrying out cyberattacks against United States

companies, government institutions and critical infrastructure. This situation of mutual accusations has worsened bilateral relations. Despite the fact, both the United States and China carry out espionage and cyberattacks on each other (Aulia, 2018). The data according to the Council on Foreign Relations Cyber Operations Tracker, the United States adversaries which are suspected of sponsoring cyberattacks from 2005 to 2021, can be seen in figure 1 below:

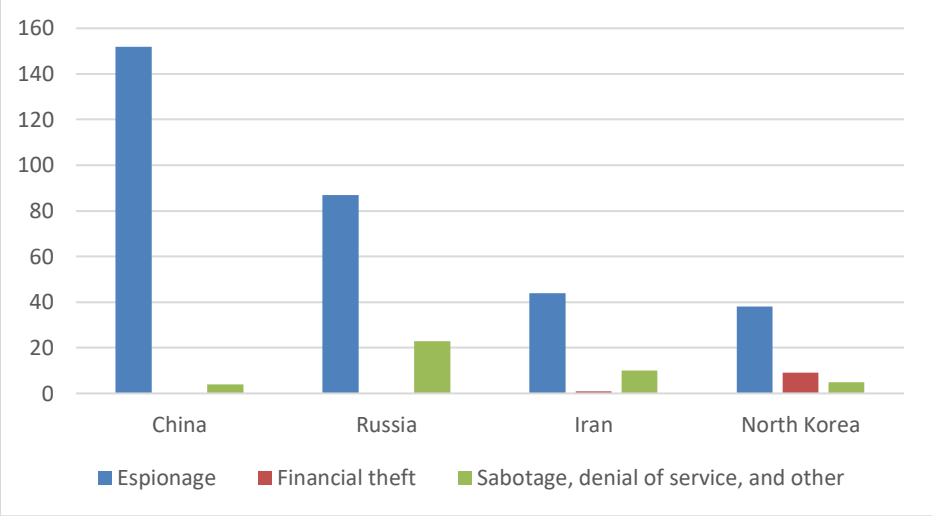

Figure 1: U.S. Adversaries are Sponsoring Cyberattacks

Source: Council on Foreign Relations Cyber Operations Tracker (2021).

If seen from the data above, China has carried out 152 espionage and 4 sabotage attacks against the United States. Followed by Russia with 87 espionage and 23 sabotage, Iran with 44 espionage, 1 financial theft and 10 sabotage, and North Korea with 38 espionage, 9 financial theft and 7 sabotage (Council on Foreign Relations Cyber Operations Tracker, 2021).

The cyberwar between the United States and China has been going on for more than a decade. China has reconfigured its hacking strategy using advanced techniques, including exploiting and searching for hidden security holes in widely used software to carry out stealth and impactful cyberattacks against US companies and interests around the world. China is known to have a large-scale cyber army that targets private companies and government entities, with the aim of stealing intellectual property, disrupting critical infrastructure and making a profit. This cyberattack carried out by China is very aggressive and shows that China has transformed into an enemy in cyberspace that is more sophisticated and mature than the attacks that confused United States officials a decade ago, during Operation Aurora which China carried out against well-known companies from the United States such as Google, Adobe, Microsoft, and others in 2009.

Three international relations prespectives : Liberalism, realism and constructivism, were examined in 2016 journal article written by Rika Isniarti (2016). The article entitled *"A Comparison of Neorealism, Liberalism, and Constructivism in Analyzing Cyber War.* This article explains the meaning of cyberwar in the framework of international relations (IR) and explains how the three theories of IR examine actors and interactions in cyberspace. The constructivism-based discussion of cyberwar is commonality between this study and Isniarti's research. But without any case studies, Isniarti's research explains cyberwar generally. In the meantime, the cyberwar involving china and the United States is the subjects of this study.

Other previou studies were authored by Arry Bainus and Junita Budi Rahman (2023) with the title "*Editorial: Digital International Relations)"* analyzed digital international relations based on several international relations theories such as realism, liberalism, constructivism, and feminism. Arry and Junita also compared these perspectives using several case studies. The similarities between Bainus and Rahman's research and this research are discussing cyberspace and the behavior of these countries in utilizing cyberspace based on constructivist theory. However, Bainus and Rahman focus on discussing how several perspectives view digital international relations and compare them. Meanwhile, this research focuses on cyberwar between the United States and China using only one theory, that is constructivism (Bainus and Rahman, 2023).

Magnus Hjortdal (2011) wrote *"China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence"* and analyzed China's strategy to become dominant in the international system by exploiting cyberspace. It was explained that China uses cyberspace more aggressively than any actor, including the United States. The similarities between Hjortdal's research and this research are discussing China's strategy in utilizing cyberspace. However, Hjortdal's research focuses on discussing China's strategy specifically. Meanwhile, this research focuses on cyberwar between the United States and China from a constructivist perspective (Hjortdal, 2011).

Asimiyu Olayinka Adenuga and Temitope Emmanuel Abiodun (2023) examined cyberattacks between China and the United States in a journal article titled *"China-US Cyber-attacks and International Security"*. These cyberattacks are predicted to be a major danger to international security, especially given the fact that these attacks could turn into a nuclear confrontation. The similarities between Adenuga and Abiodun's research and this research are discussing cyberattacks between the United States and China. However, Adenuga and Abiodun's research focuses on discussing the impact of these cyberattacks on international security. Meanwhile, this research focuses on cyberattacks between the United States and China based on a constructivist perspective (Adenuga and Abiodun, 2023).

Travis "TJ" Siemion (2023) argued in his research entitled *"Rethinking US Concepts and Actions in Cyberspace: Building a Better Foundation for Deterring China's Aggression"* that in cyberspace, China is a significant threat to the United States. Siemion discussed how China can outperform the United States, which has more capacity and capabilities than other countries, so that the United States' concepts and actions in cyberspace need to be reconsidered. The similarities between Siemion's research and this research are discussing the rivalry between the United States and China in cyberspace. However, Siemion's research focuses on discussing United States concepts and actions that need to be reviewed considering China's aggressiveness in cyberspace. Meanwhile, this research focuses on cyberwar between the United States and China based on a constructivist perspective (Siemion, 2023).

The aim of this research is to analyze and understand the cyberwar between the United States and China which has been going on for more than a decade based on a constructivist perspective. Constructivism is an alternative view that offers the basic idea that international structure is a social construction. Social construction in constructivism refers to the process in which social structures and relationships between actors are formed and updated through social interactions and practices. This means that a collection of countries without any interaction, whether through gestures, words or other communication symbols, will not form anything. However, when interactive communication between these countries begins, a pattern or structure of social relations is formed.

LITERATURE REVIEW

The term cyberspace for *"widespread and interconnected digital technology"* was popularized by science fiction writer William Gibson in his short story *"Burning Chrome"* (Gibson, 1982), and then popularized the concept in his debut novel *"Neuromancer"* (Gibson, 1984). In the context of cyberspace, there is *"cybernetics"* which refers to the study of interactions between humans and digital technology. It includes the study of how humans interact with and are affected by computer networks, virtual reality, and other digital technologies. Cybernetic concepts can also be applied to the study of cyborgs. Cybernetics refers to the study of how information is communicated in machines and electronic devices, compared to how information is communicated in the brain and nervous system. So, if you

look at the way information is processed, there are similarities between humans, animals and computers (Gibson, 1984).

Cyberspace can be conceptualized as having 4 layers based on the Physical Digital Domain (Clark, 2010) include:

1) *Physical Layer*, is the basic layer where this physical layer includes geographic and physical network components, such as hardware and infrastructure that supports the network, for example: cables and computers.
2) *Logical Layer,* is the layer that supports the physical layer. The logical layer consists of logical connections between network nodes, for example: the internet and viruses.
3) *Information Layer*, is the layer where data or information is stored and even transmitted and then distributed through intermediaries such as the government, press and news agencies.
4) *User Layer*, is a person who participates in cyberspace and has roles and functions.

Cyberspace refers to an interconnected digital environment where countries, organizations, and individuals interact through information and communication technologies. This involves implementing international law, cyber security measures, and responding to cyber threats that impact global governance, security, and diplomatic relations. Cyberspace is a dynamic and continuously developing domain that can present opportunities and challenges. This has become a significant strategic risk for countries as cyber security threats target critical infrastructure, intellectual property, and democratic institutions. The United States Department of Homeland Security (DHS) and other governments have recognized the importance of securing cyberspace and have developed strategies to address the threats it poses.

Cyber security is very important in international relations because it protects economies, governments, and individuals from cyber threats. It plays an important role in government policy, defense strategy, and diplomatic relations. The implementation of cyber security policies in international relations has challenges caused by several factors, include:

1) Different perspectives, each country may have different perspectives on cyber security, privacy and internet governance, making it difficult to find common ground in diplomatic negotiations.
2) Lack of enforcement mechanisms, international agreements related to cyberspace often do not have effective legal enforcement mechanisms, so compliance is voluntary. This raises questions regarding the effectiveness of diplomatic efforts in ensuring compliance with agreed norms.
3) The challenge of attribution (assessing a person's character), in identifying the source of a cyberattack is often difficult because cyber perpetrators can hide their identity. These attribution challenges can hinder diplomatic efforts to hold perpetrators of digital attacks accountable.
4) Cyber security capacity, not all countries have the same level of cyber security capacity. Bridging the digital divide and helping least developed countries build their cyber security capabilities is a challenge.
5) Geopolitics, the level of trust between the government and the business world, national capabilities in managing cyber risks, and geopolitics can influence how a country reacts to cyber security problems.
6) Complexity, cyber security is a complex problem that requires a multi-faceted approach. This involves technical, legal, and diplomatic aspects, which can make it difficult to develop effective cybersecurity policies.

Cyberwar involves actions by a country or organization to attack and damage another country's computers or information systems. This includes cyber espionage, sabotage, and attacks on critical infrastructure. Additionally, cyberwar can cause losses comparable to actual warfare and/or disrupt critical computer systems. The impact of cyberwar includes not only financial losses, but also disruption to social, political, and economic stability, highlighting the need for robust cyber security measures to mitigate these risks.

Several types of cyberattacks commonly used in cyberwar include (Bustami & Bahri, 2020):

1) Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks, this type of cyberattack will flood the system with requests, resulting in the system being overloaded and unable to respond to legitimate requests.
2) Man-in-the-Middle (MITM) attacks, in a MITM attack, the attacker intercepts communications between two parties, allowing them to eavesdrop or manipulate the communications.
3) Phishing attacks, phishing involves sending fake emails that appear to come from trusted sources to trick individuals into disclosing sensitive information.
4) Malware attacks, malware, such as ransomware, trojans, viruses, worms, and spyware, is malicious software designed to damage computers, networks, or servers.
5) SQL Injection Attacks, in a SQL injection attack, hackers exploit vulnerabilities in data-driven applications to inject malicious SQL statements and gain unauthorized access to the database.
6) Zero-Day exploits, zero-day exploits target vulnerabilities that are unknown to the software owner or do not have a patch available, making them very effective for attackers.

Constructivism is a theory in international relations which says that important aspects of international relations are constructed by history and ideational factors, not just material factors. The theory of constructivism was created to fill the space between the perspectives of realism and liberalism.

According to constructivism, international structures are built by intersubjective activities between actors, giving rise to a relationship of mutual influence between the structure and the actors who create it. Constructivism considers how actors acquire their identities and how these identities influence behavior. Identity is how actors believe they are and how they are seen by others. Strong identities can influence how actors behave and fight for their interests. When the constructivist paradigm is applied, cooperation between countries becomes more dynamic, peaceful, equal and productive which has an impact on increasing the amount of cooperation at the bilateral, multilateral and regional levels (Wendt, 1992).

Constructivism focuses on analyzing how norms and beliefs influence actions and interactions between actors. Norms can become widely accepted standards of behavior and influence how actors behave and how relations between countries are constructed. Beliefs, on the other hand, are views held by actors and influence how they understand the world and how they act (Bilad, 2012).

METHODOLOGY

This research uses a qualitative approach method that focuses on analyzing the constructivist perspective in understanding cyberwar between the United States and China. The United States and China were chosen as research objects because in recent years, both countries have increased their resilience in cyberspace. Therefore, research on cyberwar between the United States and China can provide important insights in understanding global power dynamics in cyberspace.

This research uses a library study data collection method by searching for data through literature study. The author uses secondary data and information as reference sources in the form of scientific journals, books, previous research, and reports published by related organizations. Besides from using literature studies, the author also uses internet searching by utilizing information media to obtain data that is related and relevant to this research.

DISCUSSION

China's strategy when carrying out cyberattacks against the United States is to target critical infrastructure that can cause local to temporary disruption to United States sectors such as energy, defense and telecommunications. China also seeks to disrupt United States military operations and military assets, such as logistics to prevent American forces from responding to bilateral crises between the two countries, further exploiting vulnerabilities, where China

is known to use advanced persistent threats (APTs) such as Volt Typhoon to target government agencies and critical United States infrastructure. Additionally, China can influence public opinion by implementing cognitive domain operations that combine psychological warfare with cyber operations to shape adversary behavior and decision-making, aiming to influence public opinion and support its interests. These strategies are part of China's broader efforts to utilize cyberwar to achieve its national goals that often fall below the threshold of war (Hjortdal, 2011).

The United States responded to China's strategy by taking several actions, including through a national cyber security strategy and international cooperation. In 2015, the United States and China reached an agreement not to conduct economic espionage via computer networks. However, China's actions show that China's cyberattacks against the United States are still ongoing. The United States has also emphasized the importance of international cooperation in dealing with cyberattacks, including through cooperation with allied countries and international organizations (Siemion, 2023).

In response to China's cyber warfare strategy, the United States has The Cybersecurity and Infrastructure Security Agency (CISA) which works to ensure that the United States' critical infrastructure, government partners, and others have the information and guidance to defend against emerging cyber threats sponsored by China. CISA provides timely information, so that cyber threats from China can be acted upon quickly. Moreover, CISA also recommends the best strategies and ways to secure cyber space, including scanning the vulnerabilities of cyber space itself (Dawson, 2021).

The escalating tensions between the United States and China, fueled by cyberattacks, have significantly impacted their bilateral cybersecurity relationship. This tension is not only rooted in the cyber realm but also extends to broader geopolitical interests, economic competition, and national security concerns. The cyberattacks, particularly those targeting critical infrastructure in the United States, have led to a heightened sense of mistrust and conflict between the two nations. These attacks have not only disrupted economic activities but also raised concerns about the security of critical infrastructure, including water supply companies, major ports on the West Coast, and oil and gas pipelines. This has resulted in disruptions in the economy, supply chain issues, and increased risks of recession (Lieberthal & Singer, 2012).

A study conducted by S&P Global Market Intelligence suggested that coordinated cyberattacks on United States ports could result in the loss of 3.1 million jobs and a total investment loss of $2.8 trillion over five years. The United States government responds to these threats through public disclosure, information sharing, collaboration with allied countries, cyber security strategies, and providing support for Taiwan (Pagan, 2023).

According to constructivism, cyberwar is seen as anarchy, which means that war in cyber space will remain a fantasy if the United States sees China cooperatively. On the contrary, cyberwar will become a reality and will have the impact of becoming a real war if the United States views China in a conflictual manner. Securitization theory, pioneered by Barry Buzan, holds that security problems are the result of construction, in line with the constructivist perspective. This means that an issue becomes a security problem because there are actors who discuss it by saying that the issue is an existential threat to an entity (Buzan, 1998).

Constructivists believe that the international system is anarchy where the situation is created/constructed by the state, depending on what state the state wants to shape the construction of the international system. However, constructivists do not believe that anarchy is permanent and is solely formed based on material aspects. Anarchy can be changed depending on meaning and identity. If countries view other countries in a conflictual manner, then it can be said that the pattern of international anarchy is conflictual. However, if countries view each other cooperatively, then it appears that the pattern of international anarchy is cooperative (Saputera, 2015).

Cyberwar between the United States and China can be understood from a constructivist perspective which emphasizes that international security is not only influenced by material factors such as military power, but also by social factors such as norms, identity and perception. In this case, the United States and China have different perceptions regarding cyber security and accuse each other of cyberattacks. The United States believes that China

has carried out spying through cyberattacks to steal information about technology controlled by the United States, while China considers the United States to be a threat to its national security.

In this case, it can be seen that the United States and China behave 'mutually suspicious' of each other. So, to ensure peace in cyberspace, the two countries need to interact with each other, so that there will be similarities in perception which can foster mutual understanding, shared norms, and respect for identity which ultimately changes their perception as friends rather than enemies.

The existence of differences in perception regarding the concept of cyber space is inevitable. China uses the concept of *"cyber sovereignty"* to build internet governance and comply with international law in cyberspace. The concept of *"cyber sovereignty"* is not considered a violation of Human Rights by the United States in a general context. However, conflicts can arise when these concepts are applied in ways that violate individual rights or pose risks to internet freedom and security, such as restrictions on access to the internet or surveillance that violates privacy or *"internet censorship"*. Even though it is not considered to violate human rights, the United States has criticized the use of this concept several times because it is considered not to fulfill the United States' concept of *"internet freedom"*. According to Freedom House reports in 2021 and 2022, the internet in the United States is largely free from government censorship and the country's legal framework provides the strongest protections for freedom of expression in the world (Freedom House, 2022).

Some constructivist concepts relevant to the conflict between the United States and China include:

1) *Identity and Interest*: This concept emphasizes that the identity and interests of states play an important role in international relations. In the context of conflict in cyberspace between the United States and China, the identities and interests of both influence perceptions and actions taken.
2) *Agent and Structure*: This concept highlights how the state and social structures influence each other. In this case, the actions and policies in cyberspace taken by the United States and China are influenced by the international social structure and identity of each country.
3) *Process and Structural Change*: This concept shows that the process of interaction between countries can bring about structural changes in international relations. In the context of conflict in cyberspace between the United States and China, the interaction between the two can produce changes in the dynamics of their relationship.

According to constructivism, there are several factors that influence the conflict in cyberspace between the United States and China, such as the identity and perception of the country which plays an important role in the conflict between the United States and China. The two countries have different perceptions regarding cyber security and accuse each other of cyberattacks. The United States considers China to have carried out spying by carrying out cyberattacks to steal information about technology controlled by the United States, while China considers the United States to be a threat to its national security.

In addition, the two countries have different national interests in the field of cyber security. The United States has a very big interest in security in the cyber sector, because the United States will not allow its country's assets to be damaged or stolen through cyber networks, because this will harm the United States in its various strategic sectors. Meanwhile, China has an interest in protecting the free flow of information at the same time as protecting national network security.

To build a strong cyberdeterrence system, both countries need to establish international behavioral norms and increase international cooperation rather than imposing cyber governance structures globally. Interaction between the United States and China could bring about structural changes in international relations. The interaction between the two can produce changes in the dynamics of their conflict, such as peace efforts through dialogue or economic sanctions.

CONCLUSION AND RECOMMENDATION

The constructivism in international relations offers a different view of how international relations are shaped and managed, focusing on shared experiences, norms, and identities as key factors in the formation of relations between states. This research shows that in the context of cyberwar, the United States' perception of China and China's perception of the United States have a direct impact on how they respond and respond to cyberattacks. This reflects how constructivism can be used to understand the dynamics and consequences of cyberwar in the context of international relations. So, to ensure peace in cyberspace, the two countries need to interact with each other, so that there will be similarities in perception which can foster mutual understanding, shared norms, and respect for identity which ultimately changes their perception as friends rather than enemies. Constructivism can play a role in helping a country prepare human resources who have a deep understanding of cyber threats and are able to develop innovative and adaptive defense strategies. Constructivism also emphasizes that there needs to be interaction to form a social construction, if there is no interaction, understanding will not be established. Even though there is no real war, the losses from cyberwar are still felt. Therefore, the United States needs to focus on defense in cyber space because there is no sure way to prevent China from carrying out cyberwar.

REFERENCES

Adenuga, A. O., & Abiodun, T. E. (2023). China-US Cyber-attacks and International Security. *Nnamdi Azikiwe Journal of Political Science, 8(2), 86–97*. https://najops.org.ng/index.php/najops/article/view/36

Afila, Kiara Krisya. (2021). Serangan Siber China kepada Amerika Serikat Pasca Kesepakatan Keamanan Siber 2015. *Skripsi Ilmu Hubungan Internasional*. Bandung: Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Komputer Indonesia.

Aryodiguno, Harryanto & Ong & Havisaputra, Yohana Novencia. (2023). China's Economic Cyber Espionage toward The United States as a National Security Threat. *Jurnal Hubungan Internasional Indonesia Vol. 5 No. 2,* http://jhii.fisip.unila.ac.id/ojs/index.php/jhii

Ashraf, Cameran. (2021).Defining cyberwar: towards a definitional framework*. Journal Defense & Security Analysis, 37:3, 274-294*, https://doi.org/10.1080/14751798.2021.1959141

Bainus, Arry & Rahman, Junita Budi. (2023). Editorial: Hubungan Internasional Digital (Digital International Relations). *Intermestic: Journal of International Studies e-ISSN.2503-443X Volume 8, No. 1, November,* doi:10.24198/intermestic.v8n1.*1*

Bustami, Agustani & Bahri, Syamsul. (2020). Ancaman, Serangan dan Tindakan Perlindungan pada Keamanan Jaringan atau Sistem Informasi: Systematic Review. *Jurnal Pendidikan dan Aplikasi Industri (UNISTEK), Vol. 7 No.2*

Clark, David. (2010). Characterizing cyberspace: past, present, future. *Massachusetts Institute of Technology Computer Science and Artificial Intelligence Laboratory, Version 1.2 of March 12*. https://www.csail.mit.edu/

Darmayadi. Andrias, et all. (2022). *Mengenal Studi Hubungan Internasional*. Bandung: Zavara.

Davis. Elizabeth Van Wie. (2021). *Shadow Warfare: Cyberwar Policy in the United States, Russia and China*. United Kingdom: Rowman & Littlefield.

Dawson, M., et all (2021). Understanding the Challenge of Cybersecurity in Critical Infrastructure Sectors. *Land Forces Academy Review,26(1) 69-75.* https://doi.org/10.2478/raft-2021-0011

Desforges, Alix. (2014). Les représentations du cyberespace : un outil géopolitique. *Hérodote, vol. 152-153, No. 1-2, pp. 67-81*. https://www.cairn-int.info/revue-herodote-2014-1-page-67.htm&wt.src=pdf

Dugis. Vinsensio. (2018). *Teori Hubungan Internasional (Perspektif-Perspektif Klasik) Edisi Revisi*. Surabaya: Pusat Penerbitan dan Percetakan Universitas Airlangga (AUP).

Gibson, William (1984). Neuromancer. New York: Ace Books. p. 69. ISBN 978-0-441-56956-4.

Hitz, C., & Schwer, K. (2018). The role of IT governance in digital operating models. *Journal of Eastern European and Central Asian Research (JEECAR), 5(2), 19*. https://doi.org/10.15549/jeecar.v5i2.210.

Hjortdal, M. (2011). China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence. *Journal of Strategic Security*, *4*(2), 1–24. http://www.jstor.org/stable/26463924

Huang, Keman & Madnick, Stuart & Zhang, Fang. (2021). Navigating Cybersecurity Risks in International Trade. Retrieved February 20, 2024 from https://hbr.org/2021/12/navigating-cybersecurity-risks-in-international-trade.

Huda, Miftahul & Al – Fadhat, Faris. (2022). The Political Economy of the US-China Cybersecurity Relations and Trade War Under the Trump Administration. *Journal of Islamic World and Politics Vol. 6 No. 2.* DOI: https://doi.org/10.18196/jiwp.v6i2.15971

Institute of Data. (2022). How Important is Cyber Security in International Relations?. Retrieved February 20, 2024 from https://www.institutedata.com/us/blog/how-important-is-cyber-security-in-international-relations/

Isnarti, Rika. (2016). A Comparison of Neorealism, Liberalism, and Constructivism in Analysing Cyber War. *Andalas Journal of International Studies Vol. 5 No. 2 November 151-165.*

Maurer, Tim & Ebert, Hannes. (2017). International Relations and Cyber Security: Carnegie Contribution to Oxford Bibliographies. Retrieved February 20, 2024 from https://carnegieendowment.org/2017/01/11/international-relations-and-cyber-security-carnegie-contribution-to-oxford-bibliographies-pub-67672

Mitra, Ananda & Schwartz, Rae Lynn. (2001). From Cyber Space to Cybernetic Space: Rethinking the Relationship between Real and Virtual Spaces. *Journal of Computer-Mediated Communication, Vol. 7, Issue 1, 1 October.* https://doi.org/10.1111/j.1083-6101.2001.tb00134.x

Pagan, Cassandra. (2023). S&P Global Market Intelligence: The economic consequences of coordinated cyber-attacks. Retrieved February 20, 2024 from https://www.spglobal.com/marketintelligence/en/mi/research-analysis/the-economic-consequences-of-coordinated-cyberattacks.html

Permatasari, Dwiyani. (2021). Tantangan Cyber Security di Era Revolusi Industri 4.0. Retrieved February 20, 2024 from https://www.djkn.kemenkeu.go.id/kanwil-sulseltrabar/baca-artikel/14190/Tantangan-Cyber-Security-di-Era-Reavolusi-Industri-40.html

Reardon, Robert dan Nazli Choucri. (2015). The Role of Cyberspace in International Relations: A View of the Literature. *The 2012 ISA Annual Convention, San Diego, CA*. https://www.isanet.org/Conferences/San-Diego-2012

Saputera, Moehammad Yuliansyah. (2015). Pengaruh Cyber Security Strategy Amerika Serikat Menghadapi Ancaman Cyber Warfare. *Jom FISIP Vol. 2 No. 2 Oktober.* https://media.neliti.com/media/publications/32726-ID-pengaruh-cyber-security-strategy-amerika-serikat-menghadapi-ancaman-cyber-warfar.pdf

Siemion, T. "TJ." (2023). Rethinking US Concepts and Actions in Cyberspace: Building a Better Foundation for Deterring China's Aggression. The Cyber Defense Review, 8(1), 119–136. https://www.jstor.org/stable/48730576

Triwahyuni, Dewi & Yani, Yanyan & Bainus, Arry. (2018). Foreign Policy of The United States of America in Addressing China's Cyberpower. *Proceedings of the International Conference on Business, Economic, Social Science and Humanities (ICOBEST 2018).* 10.2991/icobest-18.2018.66.

Wahid, Abdurahman. (2022). Kebijakan China Dalam Menghadapi Cyber Warfare Pasca Serangan Amerika Serikat Tahun 2013. *Skripsi Hubungan Internasional*. Bandar Lampung: Fakultas Ilmu Sosial Dan Ilmu Politik Universitas Lampung.

ABOUT THE AUTHORS

Kharisma Putri Nur Fatima is an undergraduate student from Universitas Komputer Indonesia, Department of International Relations. She is a copywriter with expertise in social media strategy and writes scientific papers with a focus on International Relations.

Dewi Triwahyuni, is head of Department of International Relations at the Indonesian Computer University since 2018. Started her career as a lecturer since 2005. She obtained his Bachelor's, Master's and Doctoral degrees in the same field of International Relations. As a professional lecturer and has a Certified International Qualitative Researcher (CIQaR), Dr. Dewi Triwahyuni actively conducts research and writes scientific papers with a focus on International Relations, U.S. Foreign Policy and Cybersecurity.