IAIC Transactions on Sustainable Digital Innovation (ITSDI)
Vol. 4 No. 2 October 2022

p-ISSN: 2686-6285
e-ISSN: 2715-0461

Analysis of Cyber Diplomacy and its Challenges For The Digital Era Community

Yusril Ihza Maulana[1], Irfan Fajar[2]

Faculty of Management, Universitas Al Khairiyah [1,2]
Citangkil, Cilegon, Banten 42441
Indonesia
e-mail: yusihmaulana@gmail.com

Author Notifications
28 March 2023
Final Revised
29 March 2023
Published
29 March 2023

To cite this document:
Maulana, Y. I., Fajar. I. (2023). Analysis Of Cyber Diplomacy and Its Challenges For The Digital Era Community. IAIC Transactions on Sustainable Digital Innovation (ITSDI), 4(2), 169-177. Retrieved from http://aptikom-journal.id/index.php/itsdi/article/view/587

Abstract

This paper looks at digital strategy and what it can do to promote a peaceful global local area in the age of computers. Cyberspace holds a key position and particular relevance in international affairs. This subject has gained popularity as most international entertainers have developed their global strategy and implemented various tactics to pursue their primary goals online. For instance, the Ministry of Foreign Affairs' use of social media to promote the country, its policies, and its ideals are clear evidence of this. Unfortunately, not all online activities are calm. China and the US are at odds over cyber security, and two groupings of countries are vying for control of the field internationally. Because of this conflict of interest between the countries, cyber diplomacy is required to arbitrate and prevent open cyber war. Cyber diplomacy is an international practice that results from efforts to create an international cyber community by connecting the national interests of nations with the dynamics of the global community. To fulfill the traditional duties of diplomacy in cyberspace, such as promoting trust and peace among stakeholders, cyber diplomacy is to do so. This paper uses English School diplomacy theory to analyze the potential of cyber diplomacy for peaceful cyberspace use. Digital tact consists of two main components: an effort to prevent internet deterioration and a globally coordinated apparatus for creating common digital standards.

Keywords: Cyber Security, Cyber Diplomacy, Digital Era

1. Introduction

Cyberspace is already a reality that has sophisticated networks that span the entire planet and is expanding so quickly that people and corporations need to take the necessary security precautions[1][2]. This is challenging because cybersecurity problems differ significantly from conventional security problems in that dynamics, structures, and players in complex networks characterize them. Kim noted that as cyber threats evolve, determining where a threat originates is becoming more difficult. If cybersecurity concerns remain central to international politics, the risks will escalate along with the regularity with which confrontations and tensions occur[3].

Cyberspace is already a reality that has sophisticated networks that span the entire planet and is expanding so quickly that people and corporations need to take the necessary security precautions. This is challenging because cybersecurity problems differ significantly from conventional security problems in that dynamics, structures, and players in complex

networks characterize them. If cyber threats evolve, determining where a threat originates is becoming more difficult. If cybersecurity concerns remain central to international politics, the risks will escalate along with the regularity with which confrontations and tensions occur.

Two groups of nations, on the one hand, are vying for global cyber security governance: Western nations, who accept the web ought to be more open and free, and an alliance of nations, including Russia, China, and other emerging countries, who accept the web ought to be coordinated, have a reasonable vision, and be more constrained by the state[4]. This complicates the cyberspace debate even more. In contrast, two global powers in the 21st century, China and the United States of America (US), compete in cyber security. Tensions between the two nations are likely to rise as a result of their distinct approaches to cybersecurity in terms of technical standards, regulatory policies, and security discourse.

Prior to the conflict over global cybersecurity governance[5][6], a small number of organizations were responsible for managing the internet. In the early days, internet governance was handled by the network multistakeholder decentralized community of civil society organizations, the private sector, the government, academic and research communities, and national and international organizations[7]. The goal of this model of multistakeholder governance, also known as multistakeholderism or multistakeholder initiative (MSI), is to bring stakeholders together so that they can participate in discussion, decision-making, and the implementation of solutions to common problems or objectives. The global framework of Internet governance is based on the initiatives of multistakeholders primarily based in the United States, not on the consensus of government representatives in the diplomatic arenas of international organizations.

The Web Enterprise for Relegated Names and Numbers (ICANN) is an illustration of a multistakeholder model. California, USA, is home to the non-governmental organization ICANN's headquarters. However, the US Department of Commerce's continued involvement in final approvals for major issues raises the possibility that ICANN is a de facto instrument of US hegemony. ICANN was opposed by Russia, China, and other developing nations. They continue to advocate for the use of traditional international organizations, such as UN voting procedures, rather than the ICANN model and continue to defend their right to control domestic cyber activity (Kim, 2014, p. 330). They argue that, despite the fact that the United States' position as a pioneer in the early stages of the internet's development was upheld, the world should now establish a new intergovernmental agreement on global web administration due to the rapid growth of the internet and the fact that nations' preferences diverge.

The next step was to address the UN General Assembly about this objection. Russia presented a resolution proposal on information security to the First Committee of the United Nations General Assembly in 1998 (UNODA, t.t.). Since 2004, there have been five Gatherings of Legislative Specialists (GGE) that have continued to focus on the threats posed by the use of information and communication technology (ICT) in relation to global security and how to manage them (UNODA, t.t.). The following topics are the GGE's primary focus: dangers now and later on; how ICT usage is governed at the global level; the laws, rules, and principles of responsible behavior of the state; ways to increase trust; and increasing capabilities (UNODA, t.t.). Five GGE sessions were held on alternate days in New York and Geneva from 2004 to 2017. A subsequent hearing was not settled upon at a fifth preliminary in 2017. Regardless, in December 2018, the UN General Get-together spread out another GGE and a Genuine Working Social affair (OEWG) to continue with gatherings for the periods 2019-2020 and 2020-2021.

There is no doubt that there is a purpose behind the cyberwar. International conflicts of interest are to blame for this. He explained that Western nations, led by the United States, believe that trust, openness, and freedom should be built into cyberspace. They are also of the opinion that a variety of actors, including private individuals, businesses, the government, and civil society, ought to participate in the development of international norms and regulations. As a result, Western nations use digital warfare against other nations and rely on conventional laws of war. China and Russia, then again, affirm that for public safety, data control in the internet should be conceivable and that they can't acknowledge guidelines that unjustifiably favor Western countries. As a result, this organization does not employ cyber warfare as a weapon.

It was determined during the process of establishing a new cyberspace order that these two competing nations are attempting to maximize their respective national interests. Regardless of whether the challenge of a coalition of non-Western nations succeeds, it is unlikely that either of these two visions for the internet will change anytime soon. Over the next ten years, there will be numerous disagreements of a similar nature. Cyber diplomacy is essential for avoiding open cyberwar and aligning nations' interests.

Digital discretion is essential to alleviate logical inconsistencies of nations' internet orientations, which can ignite open conflict. This paper's central matters are as per the following: What precisely is digital strategy and what advantages might it at any point bring to the quiet use of the internet?

2. Literature Review

To answer the main question of this paper, the author uses Diplomacy theory from the English School school. For the English School school, diplomacy is the essence of international politics; diplomacy is a central institution in the definition and maintenance of international society[8]. The reason for choosing the Diplomacy theory is because this theory can be the basis for an explanation of diplomacy that occurs in cyberspace. In addition, the existence of something foreign, the condition of diversity, or simply the existence of other people, combined with the need for peaceful coexistence will require diplomacy.

Diplomacy is one of the important instruments to achieve the country's national interests in international relations. With diplomacy, the state builds its image and ideas about itself. In 1959, Avalon Hill, a US company that produced strategic board games, released Diplomacy. The aim of the game is to control supply points throughout pre-World War 1 Europe through negotiations, by “forming and betraying alliances” and determining"profitable strategy", without the random effects of the dice. The representation of diplomacy as a rational and calculated act of subduing the state through negotiations illustrates several important aspects of the meaning of the concept[9].

There are various concepts of diplomacy put forward by the authors. Researchers views diplomacy as a "behavior of relations between states and other entities in world politics carried out by

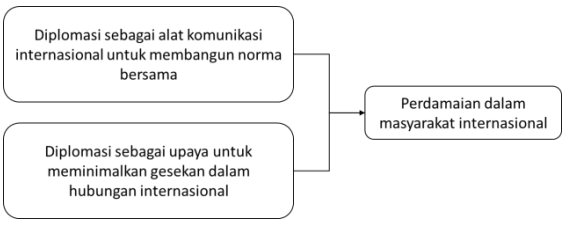

Figure 1. Theory Operationalization

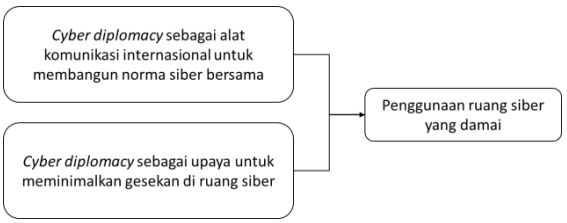

Figure 2. Analysis Model

2. Research Method

The author uses a qualitative method with analytical exploratory writing. Qualitative methods are used because they can cover various social issues and are able to provide explanations, conduct analysis, and provide an understanding of various social phenomena that occur. In simple terms, John W. Creswell defines qualitative research as follows:qualitative research begins with assumptions and the use of interpretive/theoretical frameworks that inform the study of research problems addressing the meaning individuals or groups ascribe to a social or human problem[10].

Qualitative methods emphasize the quality of analysis that refers to theories or concepts. The description in the qualitative method is descriptive or an explanation in the form of words and not a number. According to researcher that qualitative research method is a method that aims to provide a systematic description of the data, characteristics, and relationships of the phenomena to be studied[11]. There are two reasons for selecting qualitative methods in this paper. The first reason is because this paper is part of a social science study in the study of international relations as stated by Creswell[12]. The second reason, using qualitative methods, will obtain a clear and detailed picture or description of cyber diplomacy, all the dynamics that occur in cyberspace, and what cyber diplomacy can promise for the peaceful use of cyberspace. Then, the data collection method is carried out by analyzing documents such as books and articles from international journals, as well as from relevant website data[13].

3. Result and Discussion

3.1 Cyberspace

Cyber diplomacy takes place in cyberspace. Therefore, it is important to understand about cyberspace. A cyberspace has characteristics that frame diplomatic engagement among stakeholders. He further explained that cyber space is a global domain that connects various countries and people around the world in various ways, so that there can be interactions and also friction between countries and or people. According to him, cyberspace is also often seen as a global common, or a domain of resources that all countries have legal access[14]. Cyberspace can be compared to other global resources, such as the high seas, airspace and outer space. Thus, cyberspace requires a series of rules and regulations to ensure access for all and avoid conflicts. This can be achieved. The characteristics of cyberspace make international cyberspace relations and cyberspace governance very complex and fragile, but at the same time make diplomacy even more necessary, especially in the mechanism of building trust and developing international norms and values.

Then, attention to cyber issues also changed. Barrinha & Renard (2017) explained that cyber issues were initially considered as mere technical issues, then became external aspects of domestic policy, until finally they were recognized as the main topic of foreign policy. They further say that at the turn of the first decade of the twenty-first century, several major cyberpower countries issued their first cybersecurity strategies, as cyberspace and infrastructure were increasingly being regarded as strategic assets[15]. The US released a Cyberspace policy review in 2009, the UK released a Cybersecurity Strategy in the same year, while China published a White Paper on the internet in 2010 (Barrinha & Renard, 2017, p. 358).

News about cyber is also changing. According to Hodzic (2017), a decade ago, news about cyber was mostly related to the development of internet technology and advances in communication. Currently, most news about cyber is related to state cyber capabilities, security, and defense (Hodzic, 2017, p. 16). As well as demonstrating the increasing importance of cyber in everyday life and politics, this trend also illustrates that the common representation of cyber is largely technology-based, indicating an artificial space for the movement of activities such as communication or war[16]. Then, this trend also reflects the general approach in defining cyber, namely "Cyberspace is a formless, non-physical world that

theoretically exists because of the relationship between computers, computer networks, the internet, and other devices and components involved in internet use.".

In International Relations, currently cyberspace has become a significant focus[17]. This topic is becoming mainstream because most of the global actors have formulated their foreign policies and adopted various measures to pursue these goals.strategic in cyberspace. This can be seen, for example, in the use of social media by the Ministry of Foreign Affairs to promote the country, its policies and values[18]. Apart from that, there are also concerns about national security in cyberspace, so that cyberspace becomes a political space that is contested, shaped by different interests, norms and values. The politicization of cyber space has made diplomats have an important role in analyzing andrespond problems that arise.

3.2 Cyber Diplomacy

Along with the development of the internet, cyber diplomacy is also increasingly being carried out. Hodzic (2017) states that the term cyber diplomacy or cyber diplomacy is increasingly being used by key actors in global politics to describe the transformation in the implementation of diplomacy in the digital era. According to him, the evolution of diplomacy in cyberspace revolves around the use of new social media, orientation towards public actors, and the establishment of cyber threats and cyber behavior as a new area in international politics (Hodzic, 2017, p. 1). In addition, cyber diplomacy can also be said to be an evolution of public diplomacy and is often referred to as public diplomacy 2.0. The development of cyber diplomacy is a response to shifts in international relations[19].

Cyber diplomacy can be carried out by state and non-state actors. Cyber diplomacy carried out by the state exists at two levels, namely the Ministry of Foreign Affairs and embassies located around the world[20]. According to Manov and Segev, by operating at these two levels, countries can adjust their foreign policy messages and state images according to the characteristics of local audiences – for example their history, culture, values and traditions – in order to achieve foreign policy targets. the country and the image they want to build.

3.3 Use of Cyber Diplomacy

The use of cyber diplomacy can be seen from several perspectives, namely diplomats, states, and non-state actors. According to Sotiriu, from the perspective of practitioners such as diplomats, the use of cyber diplomacy can increase the audience of their messages, connecting them directly with the public, without going through media controlled by the government and the state which has the potential to change the initial message.

Once identified therethree main advantages in conducting public diplomacy, namely (1) offering a very effective instrument for conveying information;(2) allows the intended message to reach further into the target audience; and (3) enable two-way communication between diplomats and the foreign public. However, according to them, perspectiveholistic those that combine social media with more traditional forms of diplomatic interaction tend to produce better results.

Social media can help convey strong messages in a very effective way, but it cannot act as a substitute for good strategic planning, relationship and crisis management, which are hallmarks of professional diplomatic behavior.

Other efforts by the state to create peace through cyber diplomacy are also investigated by Bjola and Jiang. According to them, diplomats from the European Union (EU), Japan and the US at their embassies in Beijing creatively used social media, China's microblogging site Weibo, to reduce the suspicions of the Chinese government, and thereby succeeded in establishing open channels of communication with the people. China (Bjola, 2015, p. 6). They conclude that cyber diplomacy is used primarily as an instrument for disseminating information. This is for example done by the EU promoting European culture to Chinese citizens to increase EU visibility among Chinese citizens, who arguably do not yet have a clear understanding of the region (Bjola & Jiang, 2015, p. 86).

3.4 Threats in the Diber Room

The advancement of the internet has brought big changes in our lives today. All groups, from countries, businesses, to individuals are increasingly depending on the internet to carry out their daily activities. According to Roche, this dependence can pose a threat to infrastructure, political processes, and individual privacy (2019, p. 68).

3.5 Threats in Cyberspace Infrastructure

Cyberattacks carried out by both state and non-state actors are increasing in number. Putra and Punzalan cite that China, as the country of origin, accounts for 22 percent of the total attacks carried out against governments around the world (2013, p. 269). According to them, the most common form of attack against the government sector is a Denial of Service attack (DDoS). DDoS is a condition when the host computer (or web server), which hosts the targeted website, is unable to respond or communicate with other computers because its resources have been used by a series of requests from attackers (Putra & Punzalan, 2013, p. 270). Putra and Punzalan added that 28 percent of attacks originated in the US and targeted government sectors in Europe, the Middle East and Africa. In recent years and perhaps because of the global economic recession, hacking has turned from a personal hobby to an organized criminal business activity (Putra & Punzalan, 2013, p. 269). In addition to the proliferation of cyber crimes and cyber espionage, there has also been an increase in the number of incidents of international cyber warfare and cyber terrorism (2013, p. 269).

3.6 Threats to the Political Process

Threats to the political process can occur when information circulating online is made to benefit certain parties or corner political opponents. This threat can arise both from within the country and from other countries.

The intervention in the US election in 2016 is an example of how technology is used by foreigners to meddle in the internal affairs of rivals (Roche, 2019, p. 69).

Another example is information warfare. Chansoria (2012) argues that information warfare, especially digital, has made cyberspace a realm for crossing borders, challenging national boundaries, and most importantly, enabling a country's military to achieve certain political objectives, with more appropriate forms of propaganda. He also stated that the potential for future conflicts in the 21st century will not only be limited to the traditional military sphere, and the increasing dependence on cyberspace makes issues related to national security even more vulnerable (Chansoria, 2012, p. 106). According to him, this is because cyber warfare tactics are relatively low-cost and readily available, making it more attractive for both state and non-state actors to exploit the skills of hackers or so-called patriotic cyber warriors' (Chansoria, 2012, p. 106).

3.7 Threats to Privacy

The personal information that we store online makes us vulnerable to loss of privacy because this information can be easily accessed by parties who have certain interests. The amount of data on personal information available to governments, marketing companies, investigators, even criminals can be enormous (Roche, 2019, p. 70). Acts of violation of privacy such as intercepting internet messages, blocking content, recording telephone conversations, tracking whereabouts are also rife. In the US, government monitoring of personal communications and data is made possible by the Patriot Act (Roche, 2019, p. 70). Private companies also exploit huge amounts of personal data for sale (Roche, 2019, p. 70).

3.8 Data Security

Data security is a focus in cyberspace policy from the economic, development, and crime components. Data security is a set of standards and technologies that protect data from corruption, modification or exposure whether intentional or unintentional (Forcepoint, n.t.). Data security can be implemented using various techniques and technologies, incl administrative controls, physical security, logical controls, organizational standards, and other protection techniques that restrict access to unauthorized or malicious users or processes

(Forcepoint, t.t.).
Data security is important because all activities carried out by governments, businesses and individuals cannot be separated from data. Data plays a role in companies both large and small, from banking giants handling large amounts of personal and financial data to small businesses storing contact details of their customers on their phones (Forcepoint, t.t.). The main elements of data security are confidentiality, integrity and availability (CIA) (Buckbee, 2019). Confidentiality ensures that data is only accessed by authorized individuals; integrity ensures that information is reliable as well as accurate; and availability ensures that data is available and accessible to meet user needs (Buckbee, 2019).

3.9 Internet Governance

The focal point of the web administration part in the internet strategy is web administration. Web Convention, Transmission Control Convention (TCP), Client Datagram Convention (UDP), Space Name Framework (DNS), and Line Passage Convention (BGP) are some of the international standard information communication conventions that organize the vast network of freely managed networks that make up the Web (Web Administration Venture, t.t.). Internet governance (Internet Governance Project, t.t.) is the process of coordinating and shaping global cyberspace through a set of rules, policies, standards, and practices. The primary responsibility of internet governance is the development and implementation of solid policies regarding the technologies needed to keep the internet operational. Clients know nothing about the mind boggling institutional and specialized structure of web administration, which works in the background. For data collection and storage, the majority of internet governance is carried out by private companies and non-governmental organizations, such as the online advertising industry, search engines, and other information intermediaries. When it comes to internet governance, private businesses frequently act as actors as well. One example is when WikiLeaks stopped providing its services after the publication of private diplomatic correspondence.

4. Conclusion

Advances in information and communication technology provide many conveniences in carrying out daily activities, ranging from government, business, to individuals. This convenience is also what ultimately makes us very dependent on technology. This dependency then creates threats to infrastructure, political processes, and individual privacy. In addition, conflicts due to conflicts of interest between countries It also creates friction in international relations. Therefore, cyber diplomacy is important to minimize friction, prevent open cyber war, and realize the peaceful use of cyberspace.

The author asserts that there are two primary ways diplomacy contributes to international peace: as a means of international communication in an effort to establish common standards and lessen friction in international relations. In order to try to lessen friction in cyberspace and establish common cyber norms, cyber diplomacy must be utilized as a tool for international communication. It is possible to use cyberspace peacefully by carrying out functions of governance and communication in global cyberspace.

Efforts to build shared cyber norms have been initiated by various countries, international organizations, and private technology companies, including the NATO Tallinn Manual, Microsoft Norms Paper, Code of Conduct–which was initiated by China, Russia and other countries–US Government Policy, and United Nations Group of Governmental Experts on Information Security (UN GGE). In addition to developing norms, efforts to minimize friction in cyberspace can be carried out by developing international cyberspace policies. According to Wibisono, when viewed from the dimensions and focus, the components of cyberspace policy are dividedinto three, namely (1) an international peace and security component that focuses on cybersecurity; (2) Economic, development, and crime components that focus on data security; and (3) Internet governance component that focuses on internet regulation.

References

[1] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, 2021.

[2] I. H. Sarker, A. S. M. Kayes, S. Badsha, H. Alqahtani, and ..., "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big …*. Springer, 2020, doi: 10.1186/s40537-020-00318-5.

[3] M. Azmi, M. S. Shihab, D. Rustiana, and D. P. Lazirkha, "The Effect Of Advertising, Sales Promotion, And Brand Image On Repurchasing Intention (Study On Shopee Users)," *IAIC Trans. Sustain. Digit. Innov.*, vol. 3, no. 2, pp. 76–85, 2022.

[4] R. V. Yohanandhan, R. M. Elavarasan, P. Manoharan, and L. Mihet-Popa, "Cyber-physical power system (CPPS): A review on modeling, simulation, and analysis with cyber security applications," *IEEE Access*, vol. 8, pp. 151019–151064, 2020.

[5] M. Z. Gunduz and R. Das, "Cyber-security on smart grid: Threats and potential solutions," *Comput. networks*, vol. 169, p. 107094, 2020.

[6] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," *Futur. Internet*, vol. 12, no. 9, p. 157, 2020.

[7] U. Rahardja, N. Lutfiani, A. S. Rafika, and E. P. Harahap, "Determinants of Lecturer Performance to Enhance Accreditation in Higher Education," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*, 2020, pp. 1–7, doi: 10.1109/CITSM50537.2020.9268871.

[8] M. A. Ferrag, L. Maglaras, S. Moschoyiannis, and H. Janicke, "Deep learning for cyber security intrusion detection: Approaches, datasets, and comparative study," *J. Inf. Secur. Appl.*, vol. 50, p. 102419, 2020.

[9] S. Kim, "The Inter-network Politics of Cyber Security and Middle Power Diplomacy: A Korean Perspective," in *Korea's Middle Power Diplomacy: Between Power and Network*, Springer, 2022, pp. 97–123.

[10] A. Saveliev and D. Zhurenkov, "Artificial intelligence and social responsibility: the case of the artificial intelligence strategies in the United States, Russia, and China," *Kybernetes*, 2021, doi: 10.1108/K-01-2020-0060.

[11] I. H. Sarker, M. H. Furhad, and R. Nowrozy, "Ai-driven cybersecurity: an overview, security intelligence modeling and research directions," *SN Comput. Sci.*, vol. 2, pp. 1–18, 2021.

[12] H. M. Alzoubi *et al.*, "Cyber Security Threats on Digital Banking," in *2022 1st International Conference on AI in Cybersecurity (ICAIC)*, 2022, pp. 1–4.

[13] D. Chen, P. Wawrzynski, and Z. Lv, "Cyber security in smart cities: a review of deep learning-based applications and case studies," *Sustain. Cities Soc.*, vol. 66, p. 102655, 2021.

[14] J. Srinivas, A. K. Das, and N. Kumar, "Government regulations in cyber security: Framework, standards and recommendations," *Futur. Gener. Comput. Syst.*, vol. 92, pp. 178–188, 2019.

[15] I. Atamenwan and S. Warren, "Adaptive structuration theory used to examine organizational changes stemming from e-learning initiatives in higher education," in *E-Learn: World Conference on E-Learning in Corporate, Government, Healthcare, and Higher Education*, 2018, pp. 449–454.

[16] Q. Aini, S. Riza Bob, N. P. L. Santoso, A. Faturahman, and U. Rahardja, "Digitalization of Smart Student Assessment Quality in Era 4.0," *Int. J. Adv. Trends Comput. Sci. Eng.*, vol. 9, no. 1.2, pp. 257–265, Apr. 2020, doi: 10.30534/ijatcse/2020/3891.22020.

[17] A. G. Pamungkas, A. Suharko, D. Apriani, and E. A. Nabila, "Analysis of the Effect of Quality, Service Price and Satisfaction on Patients and Their Impact on Visits to Exclusive Dental Clinics in South Jakarta," *APTISI Trans. Manag.*, vol. 7, no. 1, pp. 8–14, 2023.

[18] D. Sunarsi, N. Rohaeni, R. Wulansari, J. Andriani, and ..., "Effect of e-leadership style, organizational commitment and service quality towards indonesian school

performance," *Syst. Rev* …. sysrevpharm.org, 2020, [Online]. Available: https://www.sysrevpharm.org/articles/effect-of-eleadership-style-organizational-commitment-and-service-quality-towards-indonesian-school-performance.pdf.

[19] M. Hernandez-de-Menendez, C. A. E. Díaz, and ..., "Engineering education for smart 4.0 technology: a review," *Int. J. …*, 2020, doi: 10.1007/s12008-020-00672-x.

[20] M. M. de Medeiros, N. Hoppen, and A. C. G. Maçada, "Data science for business: benefits, challenges and opportunities," *Bottom Line*, vol. 33, no. 2, pp. 149–163, Jan. 2020, doi: 10.1108/BL-12-2019-0132.