Cyber Diplomacy in the Era of Internet and Social Media

Dr. Shahnawaz Muhammad Khan
Assistant Professor
Department of International Relations
Federal Urdu University for Science, Arts, and Technology
Karachi – Pakistan
shan_smart17@hotmail.com

Dr. Uzma Siraj
Assistant Professor
Department of International Relations
Federal Urdu University for Science, Arts, and Technology
Islamabad – Pakistan
uzma.siraj@fuuast.edu.pk

Rashida Abbas
Vice PrincipalInstitute Of Law Lahore
Ph.D Scholar
International Relations
School of Integrated Social Sciences, the University of Lahore
Lahore - Pakistan
rashda289@gmail.com

Abstract

A state's national interests in cyberspace are typically expressed in national cyber security policies, which include cyber diplomacy as a means of achieving such interests. It is important to note that cyber diplomacy involves a wide variety of diplomatic objectives, including the establishment of communication and interaction between government and non-actors, the avoidance of a cyber arms race, and the formation of global standards. On top of that, it discusses changes in the way diplomats do their duties, as well as restructuring of various agencies and ministries in foreign affairs to accommodate new technology in diplomacy, such as cyber security. In the era of the internet and the use of social media, the old diplomatic tactics are replaced by a new and modified form named 'cyber diplomacy.' This qualitative document analysis critically focused on the issues of cyber diplomacy in which the internet and social media are playing their proactive roles in the changing dynamics of international affairs.

Introduction

Cyber meaning is connected with the internet. Anything that is connected to the internet or performs with the help of the internet so is called cyber. We know about all these words like cyber café, cybercrime, cyberspace, cyber war, cyber law, etc. Any conflict which will be resolved by negotiation is diplomacy. Something that we resolve by using our soft skills or brain so that was saying that this particular conflict was resolved by diplomacy. In this world we have to solve the problems in one way or another, one is war and the other is table talk. So the way of resolving the conflict through table talk is called diplomacy. (Potter, E. 2002)

Cyber diplomacy is an agenda invented by researcher Bob Thomas back in the 1970s; he proposed this idea for the sake of security and stability to protect the digital space. The term "cyber diplomacy" describes the process of negotiations between states, representing & to protect issues like terrorist-type attacks, threats, and global progress as well. This will help to attain sustainable development in the making of the digital age. Cyber diplomacy is different from other diplomacies because it works on international humanitarian laws, confidence building, and cyber security. (Barrinha, A., Renard, T. 2017)

Cyber diplomacy provides modern tools and modes for more effective implementation of developing strategies. These tools are used to emphasize broader diplomatic issues. In cyber diplomacy, it is a must to include multi-state actors from both the private and public sectors. International laws are mainly highlighted in cyber diplomacy. Rules, effects, and norms are not clearly defined, in cyber diplomacy because there is competition between states. Thus, it is important to develop attention to cyber issues & to make them a priority which helps as mainstream in real national security & foreign policy concerns. (Cirnu, C.E., 2017)

Cyber diplomacy is important for decreasing future cyber-attacks and cybercrime risks, as well as preventing dangerous disputes between states and non-state actors. Cyber diplomacy is used for establishing healthy communication and conversation between the states and non–state actors. Developing good relationships and global standards and building new strategies.

The cyber issue is one of the most important issues all over the world because of its importance it is discussed in foreign policies and all the ministers give importance to this issue. Cyber diplomacy problem arises because of advancements in technology. With the advancement of technology comes the problem of cyber security and also the role of cyber

diplomacy is changing day by day in the digital age. (Barrinha, A., & Renard, T. (2017). Cyber insurance is the same as other insurance policies. It was used for saving the organization from the dangerous issues of cyber diplomacy and cyber issues. Cyber insurance is progressively proving to be a significant tool for cyber risk protection and mitigation. (Lubin, A. (2020). Different articles were written and research was conducted on the mental and physical health of people who are the patients of cyber-attacks and threats. It was informed that people who are coming across a world where they are getting a threat of cybercrime are more afraid of their bank accounts and personal data because these days this stuff is more important to them rather than the people who are terrorizing a public place for example like a terrorist shootout in a mall, it is equally effective with a cyber-crime which can turn upon a whole life. (Michael L. Gross. 2016)

Cyber-Diplomacy: A New Strategy of Influence
Nowadays, the successful implementation of cyber diplomacy ideas, as well as the examination of cyber diplomacy tools, is also among the prime apprehensions of government officials. Similarly, cyber-attacks have a major effect all over the world because of this it is the main concern all over the globe. Cyber risks have an international component because this is included in the foreign policies. (Dana, 2015)
Cyber diplomacy or cyber problem is a new subject for international relations students. In this, they cover the development of cyber diplomacy, human rights problem that arises because of cyberspace, advantages, disadvantages, internet issues, development policy, cyber era, challenges variety, and other policies as well. Cyber diplomacy's definitions and concepts are still evolving, and the field is fast evolving. (Tiirmaa-Klaar, H. 2013).

The government established several different policies for the development of cyber diplomacy. According to international relations, society is evolved around needs, priorities, and new tactics. Diplomatic practice evolves about the changing world, adapting to new difficulties and responding to new sets of national interests, as it has done throughout history. (Pahlavi, P. C. 2003)
Firstly, the most important thing in this world is survival, and as we know that survival is also very difficult in this difficult world. On the other hand, innovation in technologies creates other problems in cyber diplomacy and it has also introduced technological dynamics, but all these things in turn increase human awareness. (Minchev, Z. (2021).
Other states use the word "democracy diplomacy" to spread their moral norms & to serve their geopolitical aims, just like Japan; its partners who

are in this diplomacy stated that democracies can only be strong when their interest lies in expanding the diplomacies. In the modern era, Italy's ambassador said that democracy cannot spread with the use of weapons. Peace & sovereignty is the key. But to a larger context, they use cultural information as well to communicate and educate the population for their agenda. In general, democracy is a universal idea that leads to joining forces in the domain. (Pahlavi, 2003)

Cyber diplomacy has an impact on human life and also creates some problems and challenges. It also influences human activities and dominates governmental policies; like foreign policies. By analyzing government policy papers and examining evidence of cyber diplomacy activities on the Israel Ministry of Foreign Affairs (MFA) website, including that of the 'cyber ambassador' in Israel, the study aims to investigate cyber diplomacy in Israel – in terms of policy and practice – in comparison to other countries. According to the findings, cyber diplomacy in Israel has yet to be properly integrated and practiced, and the country is still waiting for its first cyber ambassador. (Pavel, T. 2020)

In the pandemic, humans face many difficulties in all fields. First time all over the world lockdown was imposed and many health issues were arises, at that time the pandemic was not under control, the vaccination of the virus was not discovered and death rates were also increased day by day. The impacts of pandemics were there in all the activities and on global events as well. The effects on cyberspace and the need for cyber diplomacy activities at the national or international level - including the involvement of international organizations such as the UN, OSCE, G20, and the EU, as part of the measures to address these crises are actively needed. This is to develop new diplomatic norms and regulations of cyber behavior in the face of this issue several other global crises arose. (Pavel, 2021)

In today's world, the news is spreading very fast because of globalization. Everyone is connected and interdependent with each other and with technology as well and also the use of social media apps like YouTube, Twitter, Facebook, etc. because of all these social media platforms news is spreading within a few seconds either the news is fake or real, so these are the key issues of addressing malign information maneuvers in cyberspace. (Goolsby, R. 2019)

Responding to cyber-attacks: Prospects for the international community
Technological advancement is increasing day by day because of this cyber activities are increasing and growing and all these things come with the

cyber threats because of the increase in hackers the concern towards cyber diplomacy is increased previous few years. So the European Union is also very active to secure all the problems and more developed its systems. EU member states, on the other hand, are willing to make some progress in developing a cyber-diplomacy tool that includes a variety of calculations ranging from preventative to sanctioning. This task must be completed for the Union's toolkit to become operational and usable. (Ivan, P. (2019).

As pressure arises between individual actors, the great powers are becoming more chronic in cyberspace these days, the vast need is mandatory to solve the conflict between international negotiations. For this, the EU (European Union) has played an important role in this field. e.g.; in September 2018 EU foreign policy called out Chinese authorities to work against illegal cyber activities. EU has developed different strategies to work in cyber diplomacy; they established work for freedom, equality & peace. In 2015 EU finally used the term cyber diplomacy and considers it the safest online environment all over the world. (Kasper, A. Vernygora, V. 2015)

The Shanghai Corporation Organization (SCO) came into being in 2001. The purpose of this organization is to fight against regional terrorism attacks, internationally. This organization also focuses on transactional, economic & political alliances. Its main objective is to build strong relations between state members & to stimulate unity in trade, political affairs, cultural, environmental protection & lastly educational spheres as well. SCO consists of 8 state members, namely; (China, Kazakhstan, India, Pakistan, Kyrgyzstan, Russia, Uzbekistan, and Tajikistan) & 4 observer states (Afghanistan, Belarus, Mongolia & Iran). SCO is interlinked with cyber diplomacy to prevent collision & conflict between states & to maintain equality while providing cyber security to every state. (SCO)

National & International laws can be in charge of the behavior of cyber security & justifies cyber-crime relating to different issues. This article focuses on the need to localize harmonization laws & outlines the relationship between human rights & foreign policies. Because of this harmonization, several rules have been made, and no illegal, explicit content will be shown on any user web page. The privacy of every user will be safe. This law was passed in the US back on 26 April 2016; moreover, there must be a strong relationship between the lawful aims pursued by state actors. In simple words, actions must be proportionate to be protected easily. (Sandle, Tim. 2016).

European Union has a massive impact on active cyber issues. They tend to make documents that have various strategies and foreign policies in them. It explains that they have distinct types of intentions for cyber diplomacy and defines power in depth. It defines that the EU not only focuses on

bisected corporations but also played a reflexive image. Whereas, interdependent partnerships aim to describe strengthen relations & global international governance system. In conclusion, these cyber diplomacies are more useful as they are inflected. (Renard, T., 2018)

Back in 2009, that time the president of the United Nation, Mr. Barrack Obama announced a policy for cyber security to maintain his defense of the country and to make the world a safe place. He said in 2008 that they are going to invest in cyber security which will be called a cyber-battle "Hidden warfare" which will help their country's defense to become safe and secure to the maximum, he was ready to back all the strikes and maintain a marking display of his cyber security he invested and created a challenge and network which carried throughout the state as a big opportunity for the state. (James A. Lewis 2008)

A few eras back there is no facility for the internet, and also the globalization perspective and the impact of globalization are not their people are not interconnected with each other as compared to at that time. So the security issues were no there so people are secure and easily maintained their privacy but nowadays because of the internet people know about everyone or every country they know about their culture, thoughts, strength, weakness, threats, opportunities, and foreign policies so they can easily threat the country and their people by the internet because of this the ASEAN promoted cyber security to secure their countries and their people as well. (Timur, F. G. C. 2017)

Cyber Diplomacy and Media

Cyber diplomacy or cyberspace is the most important or major component of modern society. The world is going online in every field the studies, trade, advertisements, marketing; shopping, grocery, and many more but all the advantages come with many disadvantages and cyber issues as well. So we have to take responsibility for everything and do our work with full security. (Berthelsen, E., 2021) International security and stability are increasingly threatened by cyber-attack. While national initiatives aimed at determining cyber violence may provide some relief in the short term, in the long term, it will create many difficulties for national cyber security. The risks are also increasing day by day and as soon as possible the cyber enemies are increased. (Van der Meer, S. 2015)

We can surely see that the internet and other social media platforms created a good image with a huge impact on individuals and government activities as well. This is an open platform for everyone to do their work with full freedom. But at the same time, this openness and freedom build some cyber issues in all the countries. This openness sometimes became a threat to everyone so it is important to do your work with dignity. (Mureșan, R. C.

2017) The world also witnessed that the freedom of the internet in the future will become a reason for war, because of the freedom cyber diplomacy or cyber security is disturbed very badly and many cyber attackers are dangerous or threaten all the countries. (Alatalu, S. (2019).

There is a debate on economical & political international institutes which carries a major amount of public diplomacy however they highlighted that the world has millions and billions of android and iPhone users. Are now accommodating to new varieties of social platforms they are interpreting into different apps like Twitter, Facebook, Quora, and many more, they also referred that by the period every individual can be an influencer, a publisher & what not, because of these advancements in all over the world people gaining more knowledge from every aspect. (Hanson, F., 2011)

The scholars also presented the idea of dialogic communication which defines the idea of digital diplomacy; they proposed the idea that now foreign policies can look up into cyber diplomacy in different ways, and they extended the analysis method of dialogic communication, where they observe that engagement & communication is very rare among foreign policies. Social media content defines that foreign policies present a continuous supply for targeting different policies apart from domestic issues. At last, results indicate that foreign policies fail to define the importance of cyber diplomacy through international laws perspectives. (Kampf, R., Manor, I., Segev, E., 2015)

Cyber power is the rapid growth of cyberspace in which they emphasized the new context of worldly politics. Actors that have embellished soft & hard powers may have many ways to enhance the foreign policies. Cyber diplomacy is a new and flexible environment. It helps people all around the world to state their issues of cyberbullying, threats, and whatnot. This diplomacy also draws the point of scattering the domain as long as they have powers it describes that by combining information with education diplomacy will develop more strong relations based on equality and justice. (Nye Jr, J.S., 2010)

In today's era, the human development is based on the positive impact of the internet, if the users are not making the most out of the internet they are doing wrong for their selves as well, through cyber diplomacy addressing the threats is a priority for the workers who are working on these issues. The organizational framework is legally optimized & aimed through the developed resources department. Where they analyze the affected users of cyber security, through their portals of cyberspace they help the users to see and make a difference in political transformation. (Pawlak, P., 2016)

We can see that in this century the stability is increased people are well aware and too much influenced by social media, websites, and apps and too

much interest in knowing and exploring new things because of all these things the ability and capacity of cyber attackers have increased because of this the importance toward cyber security is also increased so in this article the investigation on cyber security and cyber-attacks were there both the countries Japan and Australia working to strengthen their cyber security network and also fight for cyber-attacks as well. (Manantan, M. B. F. 2021)

Cyber Diplomacy and Diplomatic Security

Diplomatic security is a very old concept itself, it started in the Persian, Babylonian, Greek, Russian, & Aztec. The Europeans developed networks to convey their messages; moreover, the work has established more and developed into a policy called "cyber – diplomacy". After WW2 1812, the department expanded its international security more. Hamilton fish who was in the cyber diplomacy department upgraded the tools and adopted the telegraph for communication but they struggled with developing new security. The US Department of international affairs reflects more security procedures as compared to French cyber diplomacy. (Weber, 2010)

There is antagonism in cyber diplomacy of increasing threats to international security. Because there is a race going on between cyber arms and cyber growth rate. Diplomacy indeed has to offer few results, but the results and effects are long-lasting and have a strong impact on the users. Transparency and foreseeability from behavior in cyber diplomacy can reduce the danger of miscommunication & conflict. While developing cyber diplomacy norms and values of different countries should be measured throughout the process and development. (Van der Meer, S., 2015)

Cyber diplomacy plays a huge role in international relations because it gives importance to liberalism, globalization, vitality, protection & privacy issues. Many global powers have focused on cyber diplomacy as it argues that cyber diplomacy is a rising practice that helps in building an international security border worldwide, it's a domain for discussing technical issues related to IT departments. (Heinl, Caitríona H., 2013.) China and U.S have notable cyber diplomacy in which they share intellectual relations. More specifically we aim to understand why they adopted a new policy domain that eventually targets the changing role of diplomacy in the digital age. (Eriksson, 2007)

Cyberspace these days have been very effective as it is very useful and as well as very harmful for the society because now a day's cybercrime is at its peak and it can be done from anywhere in the world it is very dangerous as it can put a reputation of one's institute and life at stake. Much sensitive information and confidential reports can be taken in through a cyber-hacking into one's privacy, it can be done by any group, state, or person from anywhere around the world. It can affect the use of power to undo a

whole state with the help of cybercrime by getting into the cyber security of an individual state. (Dragomir, A. 2021)

Cyberspace can provide a great security tool to facilitate successful diplomatic strategies, and as diplomats' quality is as important as for government their understanding of techniques and mentality is important for the sake of security of one country's infrastructure and data. It is a worldwide issue these days that such kind of security has to well work with cyberspace to perform and secure the society from the cyber-attacks. (Riordan, S., 2019)

Findings

International relation is a type of global security in the world where all the countries interact with each other. The diplomatic actions in international relations provide a "global duty to protect" and it's the main objective for diplomats. As in the world right now there are newly challenging political problems, especially during the pandemic in time of the Covid situation where financial security, assets, and global competition everything rely on cyberspace as well as the political agendas of all countries. Cyber power is the main power these days for a country, even the technologies and everything rely on cyber diplomacy these days the consumers are mainly super-powered for example countries like China, the USA, Russia, and even Israel.

Cyber international relations aren't only a technical issue. Time has shown us how politics have made a difference globally the technological information, and now the defense management of all the countries has made a path of making cyberspace a stronghold for the country as in this new generation all the states need to do great warfare and they have called out all the cyber-attacks, crimes and threats as the main issue which can execute the importance of cyberspace protection on foreign soil. They have taken initiatives to maintain a fine place for cyber securities and spaces.

The world becomes a global village because of technological advancement because of the internet accomplishment of work is easy and much faster compared to other centuries. People are well aware of all the aspects of life and also well-known in all the countries, they know what's going on all over the world, and the influence level is also increased because of social media platforms. The number of nongovernmental organizations is increased and people share their opinion about everything. We all are standing in a new technological revolution world. Availability of news is increased people are interconnected with each other because all these things will create complexity in every field and the disturbance arrives in cyber security as well. The pattern of cyber diplomacy is also changed and disturbed the number of cyber attackers is increased.

These days, cyber-attacks, hacking, explicit data, and even technical issues of cyber problems are all over the internet and social sites. Divergent interests, norms, and beliefs have turned the internet into a thorny political terrain. Diplomats have entered the game as a result of this politicization. If the internet was formerly just used for technical debates among IT experts, that time has passed. Cyber diplomacy is different from other diplomacies because it works on international humanitarian laws and confidence-building and also with cyber security. As we define it, it is a relatively new concept. The phrase had been used before, but solely in the context of "e-diplomacy" operations.

Conclusion

The importance of cyber diplomacy among various countries has been highlighted via different aspects and scenarios which have been directed toward the possible solution for cyber-related issues. Since the internet usage has been growing rapidly, there has been an increasing trend toward its threats by the increasing number of internet users, internet facilities like online shopping, online banking, online gaming, online classes, online examination, online portals, digital/cryptocurrencies, online trade, etc., which are becoming common day by day. Due to the reason that the internet has successfully connected people along borders, it has also created chances of crimes, frauds, or illegal activities across the border which gives an advantage to the people who commit such crimes across the border as they are well aware that they are not from the same country and their authorities will have to face a hard time to resolve the issue.

To tackle these issues, various countries have acknowledged the need for Cyber Diplomacy and its importance to control cybercrimes and related issues to safeguard the facility of the internet and its enhancing activities. Superpower countries like the USA, China, and Russia highly depend on technology and the internet which has been acknowledged by the UN 2018 meeting in Paris. Though many of these countries are against each other for many reasons like problems between the USA with China and Russia, Pakistan and India problems, North Korea and South Korea, etc., despite the differences among these countries, they all agree on Cyber Diplomacy by realizing the priority and intensity and severity of the issues it may lead.

Various countries have announced their policies for Cyber usage and Cyber Security to control and limit the possible threats and punishments for offensive usage of internet against the innocent users. President of the USA, Mr. Barrack Obama announced the cyber security policy in 2009. The Major threat from Cyber Security is the legitimate crimes where one country may encounter cyber-attacks on another country like Indian Hackers may attack Pakistani Government Website or Pakistani Banks, or Russian Hackers

could attack USA Cyber activities or it could have been vice versa. This is the most severe threat from cyber activities which may trigger a war between countries. Different writers have written articles for this global network (internet) mentioning the advantages, disadvantages, and threats it brings along with it. Even though, realizing all the threats and problems, there has been a rapid increase in cyber-related activities and users.

Conclusively, there are numerous advantages of using cyber activities but at the same time, it brings lots of threats and problems which are not limited to the country itself or border. It may arise from abroad and may harm various people or organizations or even disrupt governmental activities. Cyber-related issues need to be dealt with through Diplomacy to find corrective measures for the betterment of everyone or this war may never end until everyone adopts the same conclusion which can only be done via diplomacy.

References:

Alatalu, S. (2019). Dealing with an Evolving Cyber Threat Picture–Developing a Joint European. *Cyber Defense-Policies, Operations and Capacity Building: CYDEF 2018*, *147*, 10.

Barrinha, A., & Renard, T. (2017). Cyber-diplomacy: the making of an international society in the digital age. *Global Affairs*, *3*(4-5), 353-364.

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749-766.

Berthelsen, E., & Nellerod, J. D. (2021). *Cyber Diplomacy at the United Nations: The Endeavours of the European Union and China to Determine 'Responsible State Behaviour in Cyberspace*. UNIVERSITY OF COPENHAGEN

Cirnu, C. E. (2017). Cyber Diplomacy–Addressing the Gap in Strategic Cyber Policy. *The Market for Ideas*, 7-8.

Dana, D. A. N. C. Ă. (2015). Cyber Diplomacy–A New Component of Foreign Policy. *Jurnalul de Drept si Stiinte Administrative*, *1*(3), 91-97.

Dragomir, A. (2021). Cyber Diplomacy. International Journal of Information Security and Cybercrime (IJISC), 10(2), 38-51

Eriksson, J., & Giacomello, G. (Eds.). (2007). *International relations and security in the digital age* (Vol. 52). London: Routledge.

Goolsby, R. (2019). Developing a New Approach to Cyber Diplomacy: Addressing Malign Information Maneuvers in Cyberspace. *Senior Leadership Roundtable on Military and Defence Aspects of Border Security in South East Europe*, *141*, 105.

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists*, *72*(5), 284-291.

Hanson, F., (2011). *The new public diplomacy*. Lowy Institute for International Policy.

Heinl, C. H. (2014). Regional cybersecurity: moving toward a resilient ASEAN cybersecurity regime. *Asia policy*, (18), 131-160.

Ivan, P. (2019). Responding to cyberattacks: Prospects for the EU Cyber Diplomacy Toolbox. *EPC Discussion paper*, 18 March 2019.

James A. Lewis et al., (2008). Securing Cyberspace for the 44th Presidency: A Report of the CSIS Commission on Cyber security for the 44th Presidency, Washington, D.C., *CSIS,* December 2008, Available at: https://www.csis.org/analysis/securing-cyberspace-44th-presidency

Kampf, R., Manor, I., Segev, E., (2015). Digital diplomacy 2.0? A cross-national comparison of public engagement in Facebook and Twitter. *The Hague Journal of Diplomacy 10*, 331–362

Kasper, A., Osula, A. M., & Molnár, A. (2021). EU cybersecurity and cyber diplomacy. *IDP: revista de Internet, derecho y política= revista d'Internet, dret i política*, (34), 8.

Lubin, A. (2020). Cyber Insurance as Cyber Diplomacy. *Asaf Lubin, Cyber Insurance as Cyber Diplomacy, Cyber War & Cyber Peace in the Middle East: Digital Conflict in the Cradle of Civilization*, 22-37.

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432-459.

Minchev, Z. (2021). Disruptive Effects of New Pandemic Age to Shifted Cyber Diplomacy due to Multilateral Mixed Transformation. *International Journal of Cyber Diplomacy, retrieved from https://www. researchgate. net/publication/351776173. Accessed*, 15.

Mureșan, R. C. (2017). Current Approaches of Diplomacy in the Cyberspace. *Studia Universitatis Babes-Bolyai-Studia Europaea*, *62*(2), 31-43.

Nye Jr, J.S., (2010). Cyber power. Technical Report. Harvard University. *Belfer Center for Science and International Affairs.* Cambridge, MA.

Pahlavi, P. C. (2003, May). Cyber-diplomacy: A new strategy of influence. In *Canadian Political Association, General Meeting, Halifax, NS* (Vol. 30).

Pavel, T. (2020). Israel's Cyber Diplomacy–Looking for Israel's Cyber Ambassador. *Diplomacy & Intelligence/Revistă de Științe Sociale, Diplomație și Studii de Securitate*, (14), 208-216.

Pavel, T. (2021). Cyber Diplomacy And The Covid-19–What Is Cyber Diplomacy And How Was It Affected By The Covid-19 Era?. *INTERNATIONAL ORGANIZATIONS AND STATES'RESPONSE TO COVID-19*, 191.

Pawlak, P., 2016. Capacity building in cyberspace as an instrument of foreign policy. *Global Policy 7*, 83–92.

Potter, E. H. (Ed.). (2002). *Cyber-diplomacy: Managing foreign policy in the twenty-first century*. McGill-Queen's Press-MQUP.

Renard, T., (2018). EU cyber partnerships: assessing the EU strategic partnerships with third countries in the cyber domain. *European Politics and Society 19*, 321–337

Riordan, S. (2019). *Cyberdiplomacy: managing security and governance online*. John Wiley & Sons.

Sandle, T. (2016). UN thinks internet access is a human right. *Business Insider*, *22*(07).

The Shanghai Cooperation Organization (SCO). *The NATO Cooperative Cyber Defence Centre of Excellence.* Available at: https://ccdcoe.org/organisations/sco/

Tiirmaa-Klaar, H. (2013). Cyber diplomacy: Agenda, challenges and mission. *Peacetime Regime for State Activities in Cyberspace*, 509-531.

Timur, F. G. C. (2017). The Rise of Cyber Diplomacy ASEAN's Perspective in Cyber Security. *KnE Social Sciences*, 244-250.

Van der Meer, S. (2015). Enhancing international cyber security: A key role for diplomacy. *Security and Human Rights*, *26*(2-4), 193-205.

Weber, R. H. (2010). *Shaping Internet governance: regulatory challenges* (Vol. 46). Springer Science & Business Media.