

CYBER DIPLOMACY ON THE AXIS OF DIGITAL TRANSFORMATION

Sarvinoz Muhiddinova

Teacher of Chirchik State Pedagogical University

E-mail: sarvinozmuhiddinova365@gmail.com

Abstract

The article analyzes the increasing role of digital technologies and the Internet in the foreign policy of states in the context of globalization. The activity of actors of international relations in cyberspace is investigated.

Keywords: Cyberspace, diplomacy, digital world, cybersecurity, cyberattacks, globalization, international organizations.

Introduction

RAQAMLI TRANSFORMATSIYA O'QIDA KIBER DIPLOMATIYA

Sarvinoz Muhiddinova

Chirchiq davlat pedagogika universiteti o'qituvchisi

E-mail: sarvinozmuhiddinova365@gmail.com

Annotatsiya:

Maqolada globallashuv sharoitida davlatlarning tashqi siyosatida raqamli texnologiyalar va internetning ortib borayotgan roli tahlil qilinadi. Xalqaro munosabatlar subyektlarining kibermakondagi faoliyati o'rganiladi. Global kiberoxavfsizlikning dolzarb masalalari ko'rib chiqiladi.

Kalit so'zlar: kibermakon, diplomatiya, raqamli dunyo, kiberoxavfsizlik, kiberhujumlar, globallashuv, xalqaro tashkilotlar.

КИБЕРДИПЛОМАТИЯ НА ОСИ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Сарвиноз Мухиддинова

Преподаватель Чирчикского государственного педагогического университета

E-mail: sarvinozmuhiddinova365@gmail.com

Аннотация:

В статье анализируется возрастающая роль цифровых технологий и интернета, во внешней политике государств в условиях глобализации. Исследуется деятельность субъектов международных отношений в киберпространстве. Рассмотрены актуальные вопросы глобальной кибербезопасности

Ключевые слова: киберпространство, дипломатия, цифровой мир, кибербезопасность, кибератаки, глобализация, международные организации.



Introduction

Important events in history have not only led to rapid changes in the world order, but also laid the foundation for a change in the content of diplomacy. Today, information and communication technologies, which have become an important part of international relations, are increasing their influence every day and at the same time demonstrating their competence in cyberspace. Information and communication technologies, which facilitate the exchange of information, create important infrastructure services for citizens and enable their daily interactions, have quickly become an important tool based on international relations. In this context, "cyber diplomacy", which has emerged as a new concept with the effect of digitalization, embodies the power of information and technology in politics.

MAIN PART

If we consider cyber diplomacy as a concept, it is defined as an active part of cyberspace, within the framework of diplomatic tools and ideas, focused on solving problems in cyberspace. In this context, diplomacy has emerged as a new revolutionary method, and subsequently its content has also changed. In this era of digitalization, the growth of internet users and the transparent dissemination of their information and thoughts on this platform has become an indicator of the transition to a new community-oriented model [1].

Usually, governments and international organizations use the internet and social media to easily achieve strategic goals in foreign policy. Thus, resolving diplomatic issues through the internet and using technical means of communication and decision-making in this area is a result of digitalization. The ability to interact through the internet and information systems also facilitates international diplomatic activities. Many governments around the world actively use important social media tools and form their foreign policy programs based on them.

The technological revolution brought about by globalization has made diplomacy a part of the changes and has managed to adapt diplomats to this area. Today, diplomats must follow the media and events on a daily basis due to their duties. At this stage, diplomats can easily assess events from all sides thanks to the internet, which facilitates their work [2]. For this reason, the rapid development of internet technologies, which are the building blocks of change, has forced diplomats to increase their competence in the digital platform.

Social media has the potential to change the context of international relations. For this reason, the use of social media in diplomatic relations helps diplomats perform a variety of activities, from international negotiations to crisis management. All this forms a roadmap for understanding global security and diplomacy in the 21st century. Thus, governments that dominate the digital world will gain an advantage in cyberspace compared to inactive governments.

The insecurity of cyber platforms day by day reveals the concept of cyber diplomacy. Although digital diplomacy and cyber diplomacy are related to each other, they are conceptually different. Digital diplomacy is the transfer of all diplomatic activities to a digital platform. In this context, digital diplomacy aims to enhance the reputation of a country and realize its foreign policy goals by communicating with citizens. The way to achieve this goal is to connect



to digital tools. Cyber diplomacy, on the other hand, aims to develop diplomatic strategies proportionate to the threats in the cyber world.

If we take an example of all these events, we can put Israel at the forefront in this field. Because Israel is one of the countries that uses cyber diplomacy most actively and effectively. The University of Haifa in Israel has launched a program to train “citizen diplomats.” The program includes training in commenting on online newspapers, entering and updating information on Wikipedia pages, forums, and using Facebook and Twitter. Thus, the program aims to make citizen diplomats dominant in the virtual environment.

Another country, Australia, appointed an “ambassador for cyberspace” in 2016 to create a safe and transparent online environment for its international partners. His goal here is to represent the country in international cyberspace [3].

The concept of “cyberspace” was first used by Louis Couffignal in 1958, and in 1984 the term was used by William Gibson in his novel *Neuromancer*, and the author became a pioneer in the general dissemination of this concept [4]. Cybersecurity has attracted attention from the perspective of security, which is one of the working areas of international relations and also has a place in the discussions of international law.

On December 25, 2015, US President Barack Obama and Chinese President Xi Jinping reached a mutual agreement that both sides “will not conduct cyber-attacks involving copyright infringement and online theft, and will not support individuals or organizations that knowingly conduct cyber-attacks.”

Although some viewed this agreement as an important step, many analysts assessed it as an agreement that will remain on paper. Considering that cyberspace has its own nature of uncertainty and anarchy, it is a question of whether an agreement that will remain on paper can be included in a more realistic framework. China is considered to be one of the most aggressive players in cyberspace. Likewise, this is one of the main reasons behind the US-China agreement. According to a report presented to the US House of Representatives in 2013, it was claimed that China's intelligence activities targeted US military and economic infrastructure, stole the economy, technological innovations and copyrights, and at the same time gained access to military secrets. The report stated that 50,000 attacks were carried out against the US Department of Defense each year and that China was the leading country of attack [5].

The advances in science and technology in our century have also affected the dimensions of security. Conventional elements of security have given way to asymmetric elements and have generated debates in the perception of security. The biggest advantage of the cyber world is that cyber weapons are cheaper than conventional weapons, the perpetrator is not easy to detect, and actions in cyberspace can have devastating consequences in the real world. The United Nations (UN) has been working on cybersecurity since 1980. Research on cybersecurity is conducted mainly based on UN General Assembly resolutions through the UN agency, ITU (International Telecommunication Union). The UN also hosts the Intergovernmental Group of Experts on Cybercrime, and there are estimates that this initiative will be more comprehensive and pave the way for international norms for the peaceful use of cyberspace in the future [6].

The Role of Social Media Platforms in Digital Diplomacy



The foundation of digital media is undoubtedly formed around the axis of social media. "Social media" is a term commonly used for online tools and websites that create interaction by allowing users to share information, thoughts, interests and knowledge. Various websites and applications (twitter, facebook, instagram, youtube, etc.) have made the digital environment attractive. Social media has become an integral part of life wherever there is access to the Internet.

In terms of diplomacy, in the new era, information is collected through social media, microblogs and search engines. Nowadays, the Internet is considered by states as a unique diplomatic tool; thus, states have the opportunity to promote not only their position on various issues but also their ideas around the world through the targeted use of the Internet. However, social media comes with many risks for states. Social media gives people the opportunity to unite for a specific purpose from different parts of the world and this has made the policies of states much more visible than before. Thus, a local event can easily have a global impact.

In the context of diplomatic relations, Twitter has taken an important place in social media. So much so that Twitter has recently come to be seen as an effective public relations tool. Through Twitter, governments or institutions interact with their followers individually. Twitter enables interaction between states and citizens and paves the way for the formation of Twitter diplomacy, making a major contribution to the political participation of citizens [7].

From the perspective of official institutions, Twitter, which came to the fore in social movements such as the Arab Spring and the Gezi events, has brought a new dimension to the relationship with citizens. The thoughts of citizens or public organizations can be instantly measured through this channel and appropriate actions can be taken.

Diplomatic threats and attacks in cyberspace

The successive technological developments in the information age have also changed the size and methods of wars. Thus, states have begun to become even stronger in the international arena in order to avoid cyber attacks or to minimize these attacks. However, countries that frequently use cyber activity do not look very moderately at the formation of global cyber security. In this context, the threat of cyber warfare in the digital world manifests itself in the international arena. States can use tactical elements in strategic cyber wars in different ways. On the other hand, the attacked entity can differentiate the scale of the conflict by mutual escalation. In this case, the question of the limits of cyber warfare becomes very important. Consideration of attack methods as a second strike opportunity in cyber warfare is an important issue for the near future. It should be clearly defined administratively whether diplomatic preferences will be used by both parties or steps will be taken within the framework of crisis management [8].

In light of all this information, the main topic becomes the need for secure and global cooperation between states, as countries use their balance of power as a trump card against each other on the cyber platform. Increasing the number of legal norms and cyber security institutions are important for creating a global cyber security zone to maintain an environment of mutual trust, peace and minimize threats in cyberspace.

CONCLUSION



The development of digital diplomacy has revealed the need for cyber diplomacy. Digital diplomacy plays an important role in transferring diplomatic activities to the digital platform. For example: Diplomatic negotiations are conducted via the Zoom platform, agreements are concluded electronically, etc. States actively use many different platforms and applications.

However, using diplomacy on digital platforms can cause problems. Because digital platforms can be accessed by anyone. Thus, digital platforms become insecure as they are exposed to serious risks day by day. This situation shows the importance of cyber diplomacy.

Cyber diplomacy is the ability of states to conduct their diplomatic activities and relations securely on a cyber platform, clearing digital platforms of all possible dangers. This requires states to come together in cooperation. The importance of this cooperation is quite obvious in today's world, where digitalization is accelerating. States need to take decisive steps in this area to prevent possible cyber threats and attacks.

Cyberspace is a phenomenon that goes beyond national borders and shows how important international organizations, interstate solidarity and cooperation within a limited area are. In this context, cyber diplomacy will require states to unite in order to ensure security in cyberspace.

The reason why cyber security and cyberspace are so closely intertwined with international relations can be seen as an opportunity for "security studies" and "military capacity development". The People's Republic of China was included in the space competition between the United States and Russia during the Cold War. After all, it is obvious that it is difficult or even utopian for states to reach a consensus in the field of cyberspace. However, a point of view that can be put forward for the establishment of peace is the creation of cyber problem platforms on a global scale. Thus, it is possible that international organizations and actors playing leading roles in cyberspace can meet on common ground.

REFERENCES

1. Bjola, C., M. Holmes (2015). *Digital Diplomacy: Theory and Practice*, Newyork: Routledge. pg. 25-28
2. Tuncer, H. (2006). *Küresel diplomasi*, Ankara: Ümit Yayıncılık. s.13
3. Sandre, A. (2015). *Digital diplomacy: Conversations on İnnovation in Foreign Policy*, Digital Diplomacy: Theory and Practice, Newyork: Routledgepg. 105
4. KORHAN Sevda, *Siber Uzayda Uluslararası İlişkilerin Değişen Parametreleri*, Yüksek Lisans Tezi, Konya: Selçuk Üniversitesi, 2018. s.17.
5. AKYEŞİLMEN, Nezir, *Disiplinlerarası Bir Yaklaşımla Siber Politika & Siber Güvenlik*, Ankara: Orion Kitapevi, 2018.s.15.
6. ÇELİK, Soner, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", *Academic Review Of Humanities And Social Sciences*, Vol:1, Issue:2, 2018.s.3.
7. Fletcher, T. (2011). *Twiplomacy –Riding the Digital Tiger*. <https://www.gov.uk/government/news/twiplomacy-riding-the-digital-tiger>. pg. 8
8. Melissen, J. (2005). *The New Public Diplomacy, Soft Power in International Relations*. New York: Palgrave MacMillan. pg. 13



9. Muhiddinova Sarvinoz. (2024, December 10). AQSHNING MARKAZIY OSIYODAGI MANFAATLARINI QAYTA KO'RIB CHIQISH: YANGI STRATEGIYA ZARURATI. Google Scholar.

https://scholar.google.com/citations?view_op=view_citation&hl=ru&user=GTMrfTMAAAAJ&citation_for_view=GTMrfTMAAAAJ:9yKSN-GCB0IC

