The Bipolar Nature of Digital Diplomacy: Balancing Threats and Security

By Mariam Bregvadze

Abstract

Digital diplomacy, which is gaining traction alongside the development of the Internet, is critical for any state and its diplomatic ties. However, there are questions about how well the privacy of their connection is safeguarded and how breaking this privacy threatens national security.

Diplomacy, as a technique of establishing international connections and effectively implementing them, has changed international relations between states as a result of digital technological advancement. As a result, technical developments have covered all aspects of international interactions, including diplomacy. To avoid more problems, it is in the best interests of any state to secure its state affairs to the greatest extent possible. Today, everything is based on digital broadcasting, which, on the one hand, enables inter-state contact while, on the other, jeopardizes the security of information conveyed via digital tools.

The article will examine the perils of digital diplomacy and whether it is a tool for ensuring security in international relations. Based on a comparative analysis, we examine the activities of various nations and explore the factors that make digital diplomacy a threat to the states unions.

In the end, we will offer the readers recommendations that will avoid the use of digital diplomacy as a possible violator of state or international security.

Keywords**:** Digital diplomacy, States Security, Cyber Security, International Relations.

Introduction

The emergence of digital gadgets, such as the telegraph, computer, and cell phone, all of which contain dimatia between them. With ongoing change, there was a need for faster-acting tools to support a specific state's diplomacy and union. As an alternative, look for those social networks, such as Twitter, Facebook, and so on. For example, when he had network diplomacy, the major focus was on network issues; twiplomay, which emerged from Twitter, shares a connection with the usage of social networks. As a result, digital diplomacy is a multifaceted discipline that incorporates social networks into traditional diplomacy, as well as the study of the efficiency of digital devices in the use of diplomacy and its complexities.

Diplomacy, or the art of carrying out a country's foreign policy, is inextricably linked to global trends. Classical diplomacy, which originated centuries ago, is continuously being updated to reflect current events. Thus, with the introduction of innovations, classical diplomacy underwent a partial transformation and became known to the world as digital diplomacy.

Since the global pandemic Covid-19 outbreak, digital diplomacy has grown in importance. The incident that stop the world also posed issues that altered the path of global politics in relation to the Union. States were forced to connect with one another via digital devices, and state agencies began to frequence use social media to express their messages, among other things. As a result, a new period emerged, beginning in the early 2000s.

Digital diplomacy brings about substantial changes in today's reality. The challenges are numerous. It is about whether digital diplomacy, as a subset of digital broadcasting, is enough protected or not. Following the global expansion of digital devices, a time of developing new security standards begins, during which cyber security and related challenges emerge as a new challenge. Digital diplomacy, as a means of communicating a state's political or other messages, is inextricably linked to cybercrime, including cyber espionage, cyber attacks on diplomatic missions, disinformation campaigns, cyber manipulations during international talks, cyber sabotage, etc. As a result, the question arises in the cyber age, when cyber attacks are one of the weapons of war in the current state of conflict: how safe is digital diplomacy? What reforms are required to ensure that there are no concerns about whether digital diplomacy is safe or dangerous. All of this is unquestionably tied to the security of the state and the confidentiality of its information.

The Evolution of Diplomacy in the Digital Era

Classical diplomacy, which first appeared in ancient Greece and Rome, was constantly modeled. Today's diplomacy is completely different from centuries ago (Ghosh, 2019, 1). If diplomacy was once exclusively responsible for resolving political concerns, it has evolved throughout time, expanding beyond the political framework and, in the age of cyber threats and technology, addressing security and economic-cultural issues. Changes in geopolitics and political events prompted diplomatic maneuvering in a variety of domains. As a result, the methods used to produce it varied.

New means for implementing state policy emerged as a result of historical shifts, geopolitical events, and technical advancement. Since the world has become digital, technology have actively participated in state governance; yet, the dangers that have always accompanied this progress are also being investigating.

The first "digitalization" of classical diplomacy starts from the period when telegraph and radio were actively used for information transmission. In the 1860s, when the telegraph was first used, British Prime Minister Lord Palmerston said "Oh God, this is the end of diplomacy" (Olubukola S. Adesina, 2017). Indeed, it marked the start of the modern period. As a result, radio transmitters, cable phone, cell phones, and fax were more widely used for information transfer. As a result, classical diplomacy began to adapt to the digital era. Specifically, this age begins after the end of the twenty centery, when society begins to actively employ mobile phones. Following this occurrence, diplomats and statesmen were able to communicate more easily. The subsequent period is associated with the invention of the fax machine, which played an important role in the transfer of documents between states (Luis Ritto, 2014). Diplomats began to actively use fax in their diplomatic missions, this fact of course made it even easier to communicate between diplomats and transfer information relatively quickly.

The growth of the Internet began in the 1990s of the twentieth century, as did its integration with the state's governance structure, including diplomacy. States have started to connect with their embassies via the Internet. Although classical diplomacy continues to dominate the topic of state relations (Samantha Bradshaw, 2015), digital connectivity and fiber connections have ushered in a new age in diplomatic history. In 2007, Sweden established the first virtual embassy in Second Life, connecting diplomacy with digitalization (Kevin Jon Heller, 2007). This most recent instance occurred in the 2000s, during a period of fast technological advancement.

Therefore, since this period, the connection between diplomacy and digital devices has been actively started at the level that it is often used to express political messages. The first digital diplomacy event in the 21st century was the "Arab Spring" event in 2010-2012.

This event, which took place in the Central Asia and North Africa region, is considered a turning point in digital diplomacy. In Tunisia, Mohamed Bouaziz, a street vendor, protested police corruption and set himself on fire (Özekin, Akkaş, 2014, 76). The incident quickly spread on social media, sparking outrage.

The anti-government speeches, uprisings, and protests that occurred during this time period were extensively covered on social media platforms such as Facebook and Twitter. The utilization of these platforms has garnered international notice. Citizens used social media to share information about current happenings in the region, bypassing the state-controlled media (QadirMushtaq, Afzal, 2017).

At the same time, it's intriguing to see how the "Arab Spring" and digital diplomacy are intertwined. During this event, not only citizens but also international organizations and governments from other countries participated in the protest. These actors used social media to build their own narratives. For example, the US State Department used Twitter to directly contact with protesters. The United Nations and other non-governmental organizations aggressively used internet channels to monitor the situation on the ground. In fact, the Arab Spring has demonstrated that digital diplomacy can be both a control mechanism and a means for residents of a state to freely express themselves. As regimes in the region adapted to digital broadcasting, they used cyber tactics to suppress opposition opinion.

Consequently, the "Arab Spring" turned out to be an event that reminded the world that digital diplomacy is constantly being questioned as a threat or security provider.

Cybersecurity Challenges in the International Relations

At the end of the 20th century, when the personal computer was invented, criminal offenses began with it. After the computer, soon the Internet is born, which gives rise to new types of crimes (Schjolberg, 2008, 1).

Cyberspace, which began to develop in the 1970s and reached the 1990s, presents new and unexplored crimes and challenges to states.

After cyberspace posed a lot of security challenges to states, they began to construct regulatory structures. Prior to the development of international regulatory systems, the United States and the United Kingdom implemented domestic legislation to deter cybercrime.

The introduction of cybercrime regulatory agreements began in the early 2000s, with one of the most prominent being the Council of Europe Convention on Cybercrime (2001). It was the first international convention that controls permanent contact between signatory governments in emergency situations and ensures the sharing of experiences in order to prevent potential internet threats (Convention on Cybercrime, 2001).Since 2001, international agreements have been adopted between states, the main idea of which is to regulate possible crimes based on cyberspace. It should be noted that the United Nations is currently working on a convention, the purpose of which will be to prevent crimes committed in cyberspace, which pose a threat not only to individuals and legal entities, but also to subjects of international law (United Nations: Member States finalize a new cybercrime convention, 2024).

As we mentioned above, cyberspace is often used for such crimes, the purpose of which is to harm the state, hinder its effective work, etc. Cyberspace is also actively used in digital diplomacy, which is manifested in the fact that we are facing such types of cybercrimes that are directly directed against the diplomatic corps, against the diplomat of the state or others.

Consider each of these.

The most common cybercrime linked to digital diplomacy is disinformation on social media. One of the key reasons why disinformation poses a threat to digital diplomacy is that it affects trust in numerous international institutions and non-state actors. For example, in 2017, the Swedish Institute of International Relations accused the Russian Federation of spreading disinformation in order to influence Swedish society and thwart Sweden's NATO membership (Topor, Tabachnik, 2021). This is not the first time the Russian Federation has attempted to impose political influence through the use of disinformation. For example, during the 2014 Russia-Ukraine crisis, material was broadcast in the Russian language on TV stations along the border, resulting in a shift in public sentiment and Russification (Todd C. Helmus, 2018, 10).

These acts are directly linked to its diplomatic relations with other countries. In many situations, the propagation of misinformation harmed the relationship between the two countries, causing difficulties.Furthermore, an attack on a diplomatic mission is one of the most well-known ways in which various entities use cyberspace to undermine international relations.

An attack is an attack on the digital infrastructure of embassies or diplomatic missions, with the goal of launching a malicious program, virus, or other into their server that will damage the server, disrupt information delivery, or even cause the diplomatic mission to be temporarily closed, which will, of course, have a negative impact on the diplomatic mission's relationships.

The secure aspect of digital diplomacy is significantly impacted by cyber sabotage. This fact may disrupt diplomatic communication, erode diplomatic credibility, expose sensitive or confidential state information, or even aggravate international tensions. For example, in 2010, the Wikileaks incident occurred in the United States. WikiLeaks is a media group and website that collects sensitive and confidential material. In 2010, Wikileaks released a number of documents pertaining to the continuing hostilities in Iraq and Afghanistan. Despite the fact that the majority of the disclosed information was public, then-US President Barack Obama saw this as a threat to US national security (Ray, 2024). This event clearly shows that the leakage of information that is important for the state causes strain in diplomatic relations and international embarrassment.

In addition, another major threat to the secure nature of digital diplomacy is cyber manipulation in international relations. This type of cybercrime in relation to digital diplomacy presents the greatest danger of straining diplomatic relations between states and negatively changing the state's situation in the international arena. Cyber manipulation can lead to diplomatic confrontations between states, for example in 2015, in Germany, Russian-hired hackers launched a cyber attack on the Bundestag, causing damage to the accounts of members of parliament, including those of Angela Merkel. Also, a large amount of material has disappeared (The State of IT Security in Germany 2015).

This event strained diplomatic relations between the Russian Federation and Germany. Moreover, in 2020, the European Union imposed sanctions on the Russian Federation in response to a 2015 cyber attack. (Malicious cyber-attacks: EU sanctions two individuals and one body over 2015 Bundestag hack, 2020).

All of the aforementioned cybercrimes have a significant influence on diplomatic ties between states. As previously stated, the aforementioned crimes can severely strain relations between governments, particularly during diplomatic missions and on a global scale. As a result, cyberspace continues to pose the most significant obstacle to digital diplomacy. There are no effective systems in place to govern cyberspace use. Because cyberspace is so vast and limitless, it is difficult to adhere to legal frameworks; as a result, we are dealing with not just crimes against individuals and legal entities, but also crimes against states.

All of this poses massive challenges on a global basis. Today, when the social space is developing at a fast pace, states are actively using it, the information that the state provides to its diplomat is almost insecure. The balance between digital diplomacy and security is disturbed.

Digital Diplomacy as a Tool for Security

At the end of the 20th century, along with the formation of the Internet, the cyberspace was born. Its development and active involvement in state governance will lead to the establishment of cyber diplomacy as a new type of diplomacy and a new form of international relations.

The definition of cyber diplomacy is as follows, it describes diplomatic techniques and negotiations in international relations that deal with issues related to cyberspace (Radanliev, 2024, 1).

Cyber diplomacy is very important for the security of the state, because without its use, the adversary can create social engineering tactics, such as phishing, baiting, thereby endangering the national security of the state (Radanliev, 2024, 2). In cyber diplomacy, international collaboration is required to ensure that various states are prepared to prevent impediments and threats in cyberspace. Cyber-diplomacy is a strategy for resolving conflicts and disagreements that aims to avoid cyberspace conflicts from escalating into geopolitical catastrophes. One of the goals of cyber diplomacy is to achieve a balance between individual rights and national security in cyberspace. (Radanliev, 2024, 3).

Therefore, for all of this, as we mentioned above, it is necessary to exchange information between states, educational trainings and so on, because cyber diplomacy and cyber challenges are still a new field in international relations, and therefore effective international mechanisms for its regulation do not yet exist.

Although there is no explicit international legal system for potential cyber threats, significant governments have implemented conventions to help de-escalate cyber-conflicts in cyberspace. For example, the United States and the Russian Federation met in 2013 and 2021 to discuss guidelines for dealing with cyber risks to state security. (The White House Office of the Press Secretary, 2013) (World economic forum, 2021). In addition, the United States signed an agreement with China in 2015 to prevent attacks on American companies and federal agencies from China, aimed at reducing economic cyber-espionage and state involvement in the matter.

…….

As a result, with the help of cyber diplomacy, such cases from China's side have been drastically reduced. All this once again underlines, in the present period, within the framework of realpolitik, how important cyber diplomacy is in matters of state security (Rollins, 2015).

The Tallinn Manual 2.0 (2017) Cyber Diplomacy Review is a crucial resource for cyber diplomacy practitioners. Unlike the 2013 evaluation, this part focuses on cyberspace developments that endanger a state's security and play an important role in ensuring its sovereignty (Michael N. Schmitt, 2017).

The Tallinn Manual 2.0 (2017)'s drawback is that it is not a legal document; rather, it is a guide that cannot be influenced; hence, whether or not the advice contained in the guide are implemented is up to the state's decision.

As a result of the above incidents, we may conclude that cyber diplomacy, as a subset of digital diplomacy, is critical for regulating cyberspace threats to state security.

Conclusion

Overall, digital diplomacy, with its dual nature (threatening/safe), plays the most important role in state security. As we discussed in the preceding paper, digital devices are an essential component of today's world.

As a result, it is critical to operate these gadgets in a manner that does not endanger the state or any legal or physical person, but rather ensures a safe environment for them. Unfortunately, in today's environment, digital broadcasts, together with digital technology security, pose the greatest risk of the publication of personal or state information, violation of privacy, and so on.

Because the article focuses on state security, we can conclude that digital diplomacy is critical in the realm of international relations. It is via it that states and other actors interact. Because so much information passes via touch, states should have the ability to secure the information that is most relevant to them. The current legislative framework is insufficient, calling the activity of digital diplomacy into question in terms of security. Although states are actively attempting to develop a legal framework for the secure flow of information in the digital world, this is insufficient.

Because, by analyzing the cases presented above, we are convinced that the states often hire hackers, because in an unfair way, through digital devices, to obtain information that will help to weaken the adversary. In this case, we are dealing not with the question of the safe or dangerous nature of digital diplomacy, but with the question of the integrity of the nations.

Today, it is difficult to determine if digital diplomacy is risky or safe because the international community lacks a clear regulatory mechanism. With the advancement of technology, the issue of security gets even more complex, since it has downsides. States must develop a powerful lever to decrease the activation of hazardous issues that jeopardize their security.

Digital diplomacy, as a new type of diplomacy and a new form of international relations, is still in the process of development and construction, which means that the issues associated with its bilateral character are developing. The states should ensure by creating clear and binding documents to regulate the situation, conflicts and disagreements in the cyber space, so that it does not become unmanageable in the future and does not turn into a military conflict.

References:

Adesina, Olubukola S. "Foreign Policy in an Era of Digital Diplomacy." *Cogent Social Sciences*, August 31, 2017. https://www.tandfonline.com/doi/epdf/10.1080/23311886.2017.1297175?needAccess=true

Bradshaw, Samantha. "Digital Diplomacy - #NotDiplomacy." *Centre for International Governance Innovation*, April 7, 2015. https://www.cigionline.org/articles/digital-diplomacy-notdiplomacy/

Council of Europe. Convention on Cybercrime. Budapest, November 23, 2001. European Treaty Series - No. 185. https://rm.coe.int/16800cce5b

European Council. "Malicious Cyber-Attacks: EU Sanctions Two Individuals and One Body over 2015 Bundestag Hack." October 22, 2020. https://www.consilium.europa.eu/en/press/press-releases/2020/10/22/malicious-cyber-attacks-eu-sanctions-two-individuals-and-one-body-over-2015-bundestag-hack/

Federal Office for Information Security (BSI). *The State of IT Security in Germany 2015*. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Publications/Securitysituation/IT-Security-Situation-in-Germany-2015.pdf?__blob=publicationFile&v=2

Ghosh, Kathakali Abhijit. "The Evolution of Diplomacy: From Classical to Modern." *Millennial Asia*, 2019.

Heller, Kevin Jon. "Sweden Opens Second Life Embassy." *Opinio Juris*, January 30, 2007. https://opiniojuris.org/2007/01/30/sweden-opens-second-life-embassy/

Mushtaq, Abdul Qadir, and Muhammad Afzal. "Arab Spring: Its Causes and Consequences." *Journal of the Punjab University Historical Society* 30, no. 1 (January - June 2017). https://tehqeeqat.com/downloadpdf/25342

Özekin, Muhammed Kürşad, and Hasan Hüseyin Akkaş. "An Empirical Look to the Arab Spring: Causes and Consequences." *Alternatives: Turkish Journal of International Relations 13, no. 1-2 (Spring-Summer 2014).* https://ciaotest.cc.columbia.edu/journals/tjir/v13i1/f_0033740_27513.pdf

Radanliev, Petar. "Cyber Diplomacy: Defining the Opportunities for Cybersecurity and Risks from Artificial Intelligence, IoT, Blockchains, and Quantum Computing." *Journal of Cyber Policy*, 2024. https://www.tandfonline.com/doi/full/10.1080/23742917.2024.2312671

Ray, Michel. "WikiLeaks, a Media Organization and Website." 2024

Ritto, Luis. "Diplomacy and Its Practice vs Digital Diplomacy." *Diplomat Magazine*, September 7, 2014. https://diplomatmagazine.eu/2014/10/18/diplomacy-practice-vs-digital-diplomacy-2/

Rollins, John W. "U.S.–China Cyber Agreement." October 16, 2015. https://sgp.fas.org/crs/row/IN10376.pdf

Schjolberg, Stein. "The History of Global Harmonization on Cybercrime Legislation: The Road to Geneva." December 2008. https://www.cybercrimelaw.net/documents/cybercrime_history.pdf

Schmitt, Michael N. Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. 2017. https://www.onlinelibrary.iihl.org/wp-content/uploads/2021/05/2017-Tallinn-Manual-2.0.pdf

The White House Office of the Press Secretary. "FACT SHEET: U.S.-Russian Cooperation on Information and Communications Technology Security." June 17, 2013. https://obamawhitehouse.archives.gov/the-press-office/2013/06/17/fact-sheet-us-russian-cooperation-information-and-communications-technol

Topor, Lev, and Alexander Tabachnik. "Russian Cyber Information Warfare: International Distribution and Domestic Control." *Journal of Advanced Military Studies* 12, no. 1 (2021). https://www.usmcu.edu/Outreach/Marine-Corps-University-Press/MCU-Journal/JAMS-vol-12-no-1/Russian-Cyber-Information-Warfare/

United Nations. "Member States Finalize a New Cybercrime Convention." *United Nations Office on Drugs and Crime*, August 9, 2024. https://www.unodc.org/unodc/frontpage/2024/August/united-nations_-member-states-finalize-a-new-cybercrime-convention.html

World Economic Forum. "What the Biden-Putin Summit Reveals about Future of Cyber Attacks - and How to Increase Cybersecurity." June 17, 2021. https://www.weforum.org/agenda/2021/06/joe-biden-vladimir-putin-summit-cybersecurity/