Sarcouncil Journal of Public Administration and Management

ISSN(Online): 2945-3712

Volume- 02| Issue- 04| 2023

Research Article **Received:** 21-06-2023 | **Accepted:** 11-07-2023 | **Published:** 08-08-2023

Analysis of the Impact of Cyber-Diplomacy on International Relations

Toye Manuwa
(PhD) Institute of Health Humanities and Entrepreneurship, Ondo, Ondo State

Abstract: Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities and achieve foreign policy objectives. It has emerged as a new and influential dimension of international relations in the 21st century, as more states and non-state actors adopt cyber tools to pursue their interests and values. This paper examines the impact of cyber-diplomacy on international relations, focusing on three main aspects: the evolution of diplomatic norms and practices, the challenges and opportunities for multilateral cooperation, and the implications for global security and stability. The paper argues that cyber-diplomacy has both positive and negative effects on international relations, depending on how it is used and regulated by the actors involved. The paper also provides some recommendations for enhancing the effectiveness and legitimacy of cyber-diplomacy, as well as for mitigating its potential risks and harms.

Keywords: Cyber, Diplomacy, International relations, foreign policy and global security.

INTRODUCTION

Cyber diplomacy is the use of digital tools and platforms to advance diplomatic objectives and interests. It involves engaging with various actors, such as governments, civil society, private sector, and international organizations, on issues related to cyberspace, such as cyber-security, internet governance, digital rights, and cybercrime.

Cyber diplomacy can take different forms, such as bilateral or multilateral dialogues, negotiations, consultations, capacity building, information sharing, and public diplomacy. Cyber diplomacy can also complement traditional diplomacy by enhancing communication, collaboration, and trust among stakeholders. Cyber diplomacy is becoming increasingly important in the 21st century, as cyberspace is a domain of opportunities and challenges for global peace, security, development, and human rights. Cyber diplomacy can help promote a free, open, secure, and resilient cyberspace that benefits all people and respects international law and norms.

Some examples of cyber diplomacy are:

- The UN Group of Governmental Experts (GGE) and the Open-Ended Working Group (OEWG) on developments in the field of information and telecommunications in the context of international security, which aim to develop a common understanding of responsible state behavior in cyberspace (Riodan, 2019).

The UN GGE is an abbreviation for the United Nations Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace in the Context of International Security. It is one of the main forums for discussing cyber issues at the UN level. It was established in 2004 and has convened six times so far. The UN GGE consists of 25 Member States that are appointed by the UN Secretary-General for each session. The UN GGE operates by consensus and produces reports that contain recommendations for enhancing cyber stability and security.

The UN GGE has made significant contributions to the development of norms and rules for responsible state behavior in cyberspace. In 2013, it affirmed that international law applies to cyberspace and that states have the inherent right to self-defense as recognized in the UN Charter. In 2015, it proposed a set of voluntary norms for states to refrain from malicious cyber activities against each other's critical infrastructure, computer emergency response teams (CERTs), or the use of proxies for cyber-attacks. In 2021, it reaffirmed these norms and provided further guidance on how to implement them in practice. It also recognized the importance of confidence-building measures (CBMs), capacity building, and cooperation among all stakeholders in cyberspace (Riodan, 2019).

The UN GGE is not a permanent body and its mandate has to be renewed by the UN General Assembly every two years. The current session of the UN GGE will end in 2021 and its future is uncertain. Some challenges that the UN GGE faces include the lack of representation of developing countries, civil society, and other stakeholders; the difficulty of reaching consensus among diverse views and interests; and the gap between its recommendations and their actual implementation by states

***Corresponding Author:** Toye Manuwa

DOI- https://doi.org/10.5281/zenodo.8224179

- The Global Forum on Cyber Expertise (GFCE), which is a platform for sharing best practices and building capacity on cyber issues among various stakeholders (Tsalikis, *et al.*, 2018).

The Global Forum on Cyber Expertise (GFCE) is a platform for international collaboration on cyber capacity building. It aims to strengthen cyber resilience and security in all regions of the world by connecting needs, resources and expertise. The GFCE also supports cyber diplomacy by facilitating high-level discussions and policy recommendations on how to respond to emerging challenges in cyberspace.

The GFCE contributes to cyber diplomacy by providing a multi-stakeholder forum for dialogue and coordination on cyber capacity building. The GFCE members and partners include governments, international organizations, civil society, private sector, academia and technical community from all regions of the world. They work together in thematic working groups and practical initiatives to share knowledge, best practices and lessons learned on cyber capacity building. The GFCE also develops a global agenda for cyber capacity building based on the Delhi Communiqué, which prioritizes five themes and 11 topics for action.

By strengthening cyber capacity and expertise globally, the GFCE helps create a more secure, open and peaceful digital world. The GFCE also supports the implementation of the UN resolutions and processes on cyber issues, such as the UN Group of Governmental Experts (UN GGE) and the Open-Ended Working Group (OEWG). The GFCE is committed to enhancing cyber diplomacy through international collaboration and cooperation (Tsalikis, *et al.*, 2018).

- The Freedom Online Coalition (FOC), which is a group of governments that work together to support internet freedom and human rights online (Dutton & Dubois, 2017).

The Freedom Online Coalition (FOC) is a group of countries that share a common vision of an Internet that is free, open, secure, and interoperable. The FOC was established in 2011 as a response to the growing threats to human rights and fundamental freedoms online. The FOC aims to promote and protect these rights through diplomatic coordination, shaping global norms, and multi-stakeholder collaboration.

The FOC uses cyber diplomacy to advocate for its principles and values in various international forums and platforms, such as the United Nations, the Internet Governance Forum, and the Global Conference on Cyberspace. The FOC also uses cyber diplomacy to coordinate joint statements and actions in response to emerging threats or violations of human rights online, such as Internet shutdowns, surveillance technologies, or digital authoritarianism. The FOC works closely with civil society and the private sector to ensure that their perspectives and expertise are included in its cyber diplomacy efforts. The FOC believes that cyber diplomacy can help create a more peaceful, prosperous, and inclusive digital world, where everyone can enjoy their rights and freedoms online. The FOC invites other countries that share this vision to join its efforts and become members of the Coalition (Dutton & Dubois, 2017).

- The Paris Call for Trust and Security in Cyberspace, which is a multi-stakeholder declaration that calls for cooperation and adherence to principles and norms for a stable and secure cyberspace (Jovanović & Kerr, 2019).

The Paris Call for Trust and Security in Cyberspace is a declaration that was launched on 12 November 2018 at the Paris Peace Forum by the President of France, Emmanuel Macron. It is a non-binding initiative that calls for states, the private sector, and civil society organizations to work together to promote security in cyberspace, counter disinformation, and address new threats endangering citizens and infrastructure. It is based on nine common principles to secure cyberspace, which provide areas for discussion and action. The Paris Call invites all cyberspace actors to work together and encourage states to cooperate with private sector partners, academia, and civil society. The supporters of the Paris Call commit to working together to adopt responsible behavior and implement within cyberspace the fundamental principles which apply in the physical world.

The Paris Call is a significant example of cyber diplomacy because it is a multi-stakeholder framework that involves different actors from different sectors and regions. It is also a flexible and inclusive platform that allows for dialogue and cooperation on various topics related to cyberspace. The Paris Call aims to complement and reinforce existing international processes and norms on cybersecurity, such as the United Nations Group of Governmental Experts

Publisher: SARC Publisher

(UNGGE) and the Open-Ended Working Group (OEWG). The Paris Call also seeks to foster confidence-building measures, capacity-building initiatives, and best practices among its supporters (Barrinha & Renard, 2020).

As of November 2021, the Paris Call has more than 1200 supporters, including 80 states, 700+ companies, and 380+ civil society organizations. Some of the notable supporters are Canada, the European Union, Microsoft, Google, Facebook, Amnesty International, and Human Rights Watch. The United States also joined the Paris Call in November 2021 under the Biden administration, after snubbing it under the Trump administration.

International relations is the study of how states and other actors interact in the global arena. It examines the causes and consequences of cooperation and conflict, as well as the norms and institutions that shape world politics. International relations is a multidisciplinary field that draws on history, economics, sociology, psychology, law, and other disciplines to understand and explain complex phenomena. The study of international relations is important for several reasons. First, it helps us to understand the world we live in and the challenges we face as global citizens. Second, it provides us with analytical tools and frameworks to evaluate different policies and strategies for addressing global issues. Third, it enables us to develop critical thinking and communication skills that are essential for academic and professional success.

Cyber-diplomacy is a subset of international relations that focuses on the use of digital technologies and platforms to conduct diplomacy and influence foreign policy outcomes. Cyber-diplomacy can involve both state and non-state actors, such as hackers, activists, corporations, and civil society groups. Cyber-diplomacy has become increasingly important in the 21st century, as the world faces complex and interconnected challenges that require global collaboration and coordination.

One of the positive impacts of cyber-diplomacy is that it can enhance communication and engagement between states and non-state actors, such as civil society, media, academia, and private sector. Cyber-diplomacy can enable more inclusive, diverse, and transparent dialogue on global issues, as well as foster mutual understanding and trust. For example, the United Nations has launched several online platforms to facilitate multilateral consultations and participation, such as the UN75 initiative, the UN Digital Cooperation Roadmap, and the UN Cybersecurity Tech Accord.

Another positive impact of cyber-diplomacy is that it can facilitate cooperation and coordination on common challenges and opportunities, such as climate change, health, trade, human rights, and development. Cyber-diplomacy can help to bridge gaps and build consensus among different stakeholders, as well as mobilize resources and expertise. For example, the World Health Organization has used digital platforms to coordinate the global response to the COVID-19 pandemic, such as the COVID-19 Solidarity Response Fund, the Access to COVID-19 Tools Accelerator, and the COVID-19 Technology Access Pool.

However, cyber-diplomacy also has some negative impacts on international relations. One of them is that it can increase the risks of cyber-conflict and cyber-warfare, as states and non-state actors use cyberspace to pursue their interests and agendas, sometimes at the expense of others. Cyber-diplomacy can also create new sources of tension and mistrust, as states and non-state actors engage in cyber-attacks, cyber-espionage, cyber-disinformation, and cyber-manipulation. For example, the recent SolarWinds hack, attributed to Russia, compromised the security and integrity of several US government agencies and private companies.

Meanwhile, Cyber-diplomacy should not be seen as a zero-sum game or a tool for confrontation or domination. Rather, it should be seen as an opportunity for collaboration or innovation. For example, the Global Partnership on Artificial Intelligence (GPAI) is an initiative that brings together experts from government (Barrinha & Renard, 2020), because it aims to promote a peaceful, secure, open, and cooperative cyberspace that respects human rights and the rule of law. This paper therefore seeks to explore the impact of cyber-diplomacy on international relations.

Statement of the Problem

Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities and achieve foreign policy objectives. It has become an increasingly important tool for states to communicate, negotiate, cooperate and influence other actors in the international arena. However, cyber-diplomacy also poses significant challenges

Publisher: SARC Publisher

and risks for the traditional norms and practices of diplomacy, such as sovereignty, non-interference, confidentiality and reciprocity (Nye, 2017). Significance of Cyber-diplomacy on international relations cannot be over-emphasized. It enables states to reach out to a wider and more diverse audience, including non-state actors, civil society, media and public opinion. This can enhance the legitimacy, transparency and accountability of diplomatic actions, as well as foster dialogue and mutual understanding among different stakeholders (Hocking, *et al.*, 2012). It also allows states to access and share information more easily and rapidly, which can improve the quality and efficiency of decision-making and coordination. It can also facilitate the exchange of best practices, knowledge and expertise among diplomats and experts from different countries and regions.

There has been dearth of research on cyber-diplomacy, because of the fact that it is new on the international platform and not all states have adopted it coupled with the fact that some world leaders find difficulty in how to balance the opportunities and challenges of cyber-diplomacy for international relations; how to adapt the existing norms and rules of diplomacy to the new realities and demands of cyber-diplomacy as well as how to enhance the capacity and skills of diplomats to effectively use cyber-diplomacy tools and platforms with a secured and resilient cyber-diplomacy infrastructure and networks. It is against this background that this paper examines the impact of cyber-diplomacy on international relations.

PURPOSE OF THE STUDY

The main purpose of the paper is to examine the impact of cyber-diplomacy on international relations.

Specifically, the study seeks to:

- explore how cyber-diplomacy affect the norms, rules, and practices of traditional diplomacy;
- investigate the opportunities and challenges of cyber-diplomacy for enhancing cooperation and resolving conflicts among states and other stakeholders;
- examine how cyber-diplomacy influence the power dynamics and the balance of power in the international system and
- assess the ethical and legal implications of cyber-diplomacy for human rights, democracy, and global justice.

RESEARCH QUESTIONS

The following questions guided the study:

1. How does cyber-diplomacy affect the norms, rules, and practices of traditional diplomacy?
2. What are the opportunities and challenges of cyber-diplomacy for enhancing cooperation and resolving conflicts among states and other stakeholders?
3. How does cyber-diplomacy influence the power dynamics and the balance of power in the international system?
4. What are the ethical and legal implications of cyber-diplomacy for human rights, democracy, and global justice?

LITERATURE REVIEW-OVERVIEW OF CYBER-DIPLOMACY

Cyber-diplomacy is the use of digital tools and platforms to advance diplomatic objectives and engage with various stakeholders in the cyberspace. Cyber-diplomacy can be seen as a subset of public diplomacy, which aims to influence public opinion and shape the image of a country or an organization in the international arena. Cyber-diplomacy can also be used to address specific issues or challenges related to cyber-security, cyber-governance, cyber-development, cyber-human rights, and cyber-conflict prevention and resolution (Barrinha & Renard, 2020).

The origin of cyber-diplomacy can be traced back to the year 2007, when Estonia faced a massive cyber-attack that disrupted its critical infrastructure and public services. This incident highlighted the need for international cooperation and dialogue on cyber issues, as well as the challenges posed by different norms and values in cyberspace. Since then, many countries have developed cyber strategies and appointed cyber diplomats to pursue their interests and values in cyberspace, while engaging with other actors through various institutions and platforms. Cyber-diplomacy is thus an attempt to construct a cyber-international society, bridging the national interests of states with the global dynamics of cyberspace (Barrinha & Renard, 2017; Kurbalija, 2016 and Nye, 2010).

According to Hocking & Melissen (2015), in their book, the origin of cyber-diplomacy can be traced back to the early 2000s, when some countries started to recognize the need for international cooperation and dialogue on cyber issues. One of the first examples of cyber-diplomacy was the US International Strategy for Cyberspace, published in 2011, which outlined the US vision and objectives

Publisher: SARC Publisher

for cyberspace and appointed designated diplomats to pursue them. Another milestone was the establishment of the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications in the Context of International Security, which produced several consensus reports on norms and principles for responsible state behavior in cyberspace.

However, cyber-diplomacy has also faced many challenges and difficulties, as different actors have diverging interests, values, and visions for the future of cyberspace. Some countries, such as China and Russia, have advocated for more state control and sovereignty over cyberspace, while others, such as the US and the EU, have defended a more open and multi-stakeholder approach. These tensions have been reflected in various initiatives and proposals that aim to reshape the governance and regulation of cyberspace, such as the New IP protocol suggested by a Huawei-led group in 2019 (Forbes Report, 2020).

Cyber-diplomacy is therefore an emerging and evolving practice that attempts to construct a cyber-international society, bridging the national interests of states with the global dynamics of cyberspace. Cyber-diplomacy requires not only technical expertise, but also political acumen, cultural sensitivity, and ethical awareness. As cyberspace becomes more interconnected and interdependent with other domains of human activity, cyber-diplomacy will play an increasingly important role in ensuring peace, security, and cooperation in the digital age.

How Does Cyber-Diplomacy Affect the Norms, Rules, and Practices of Traditional Diplomacy?

Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities and achieve foreign policy goals. It can involve various actors, such as governments, international organizations, civil society, and private sector. Cyber-diplomacy can have significant impacts on the norms, rules, and practices of traditional diplomacy, as it introduces new opportunities and challenges for diplomatic actors.

One of the impacts of cyber-diplomacy is that it can enhance the accessibility and inclusiveness of diplomatic processes. By using online tools and platforms, such as social media, video conferencing, and e-participation, diplomatic actors can reach out to a wider range of stakeholders, such as non-state actors, marginalized groups, and public opinion. This can increase the transparency and accountability of diplomatic activities, as well as foster dialogue and cooperation among different actors (Pamment & Wilkins, 2020).

Another impact of cyber-diplomacy is that it can increase the complexity and uncertainty of diplomatic environments. By operating in cyberspace, diplomatic actors are exposed to various risks and threats, such as cyber-attacks, disinformation, espionage, and interference. These can undermine the security and credibility of diplomatic communications and negotiations, as well as affect the sovereignty and interests of states. Moreover, cyberspace is a dynamic and contested domain, where different actors have different views and interests on how it should be governed and regulated (Council on Foreign Relations Report, 2021).

Therefore, cyber-diplomacy can affect the norms, rules, and practices of traditional diplomacy in both positive and negative ways. It can enable more effective and inclusive diplomatic engagement, but also create more challenging and uncertain diplomatic scenarios. Diplomatic actors need to adapt to these changes and develop new skills and strategies to cope with the opportunities and challenges of cyber-diplomacy.

What are the Opportunities and Challenges of Cyber-Diplomacy for Enhancing Cooperation and Resolving Conflicts among States and Other Stakeholders?

Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities and achieve foreign policy goals. It can involve various actors, such as states, international organizations, civil society, private sector, and individuals. Cyber-diplomacy can offer many opportunities and challenges for enhancing cooperation and resolving conflicts among these stakeholders.

Some of the opportunities of cyber-diplomacy are:

- It can facilitate communication, dialogue, and negotiation among different parties, especially in times of crisis or tension.
- It can enable the participation and inclusion of diverse voices and perspectives, especially from marginalized or underrepresented groups.
- It can foster mutual understanding, trust, and confidence-building among different actors, through the exchange of information, culture, and values.
- It can promote transparency, accountability, and legitimacy of diplomatic actions and

Publisher: SARC Publisher

outcomes, through the use of open data, social media, and online platforms.
- It can support the implementation and monitoring of international agreements and norms, through the use of digital tools and mechanisms.

Some of the challenges of cyber-diplomacy are:
- It can increase the complexity and uncertainty of diplomatic interactions, due to the multiplicity of actors, platforms, and issues involved.
- It can create or exacerbate power asymmetries and inequalities among different actors, due to the digital divide, cyber-attacks, misinformation, and propaganda.
- It can undermine the security and sovereignty of states and other stakeholders, due to the vulnerability of cyberspace to interference, espionage, sabotage, and coercion.
- It can erode the credibility and authority of diplomatic actors and institutions, due to the lack of regulation, verification, and accountability of online activities and content.
- It can generate or escalate conflicts and tensions among different actors, due to the miscommunication, misunderstanding, or manipulation of online information and behaviour.

Therefore, cyber-diplomacy requires a careful balance between the opportunities and challenges that it presents. It also requires a collaborative and multi-stakeholder approach that respects the principles and norms of international law and diplomacy. Cyber-diplomacy can be a powerful tool for enhancing cooperation and resolving conflicts among states and other stakeholders if it is used responsibly and effectively.

How Does Cyber-Diplomacy Influence the Power Dynamics and the Balance Of Power In the International System?

Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities, such as communication, negotiation, cooperation, and public diplomacy. Cyber-diplomacy can be seen as a tool to enhance the efficiency, transparency, and inclusiveness of traditional diplomacy, but also as a challenge to its norms, practices, and institutions.

Cyber-diplomacy has a significant impact on the power dynamics and the balance of power in the international system. On one hand, cyber-diplomacy can empower smaller and weaker actors, such as developing countries, civil society organizations, and individuals, by giving them access to information, resources, and networks that can increase their influence and participation in global affairs. On the other hand, cyber-diplomacy can also create new vulnerabilities and threats for actors, such as cyber-attacks, disinformation, and espionage, that can undermine their security and sovereignty (Bjola & Holmes, 2015).

Cyber-diplomacy also affects the balance of power between the major powers in the international system. The rise of China as a global cyber power poses a challenge to the dominance of the United States and its allies in cyberspace. China has been pursuing a strategy of cyber sovereignty, which asserts its right to control its own cyberspace and to shape the global governance of cyberspace according to its interests and values. The United States and its allies have been advocating for a free and open cyberspace, which promotes human rights, democracy, and multilateralism. The competition between these two visions of cyberspace has implications for the stability and order of the international system (Nye, 2017). Cyber-diplomacy is therefore a complex and dynamic phenomenon that requires constant adaptation and innovation from actors in the international 0system. Cyber-diplomacy can be a source of cooperation or conflict, depending on how actors use it and how they respond to it. Cyber-diplomacy can also create new opportunities or challenges for achieving global goals, such as peace, security, development, and justice.

What are the Ethical and Legal Implications of Cyber-Diplomacy for Human Rights, Democracy, and Global Justice?

Cyber-diplomacy can offer many benefits for advancing human rights, such as increasing access, transparency, participation, and accountability. Cyber-diplomacy can offer many benefits for democracy, such as increasing transparency, accountability, participation, and inclusion. However, cyber-diplomacy also poses some ethical and legal challenges that need to be addressed.

One of the ethical challenges is how to balance the right to privacy and the need for security in cyberspace. Cyber-diplomacy involves the collection, processing, and sharing of large amounts of data, which may contain sensitive or personal information (Dutton & Dubois, 2017). How can diplomats protect the privacy of their

Publisher: SARC Publisher

interlocutors and their own? How can they prevent unauthorized access, misuse, or manipulation of data? How can they ensure that data is used for legitimate purposes and in accordance with ethical principles?

Another ethical challenge is how to deal with the risks of misinformation, disinformation, and propaganda in cyberspace. Cyber-diplomacy can be used as a tool for spreading false or misleading information, influencing public opinion, undermining trust, and destabilizing democratic institutions. How can diplomats verify the accuracy and credibility of information? How can they counter the negative effects of misinformation, disinformation, and propaganda? How can they promote a culture of critical thinking and media literacy among citizens?

A legal challenge is how to define and regulate the jurisdiction and responsibility of cyber-diplomats. Cyber-diplomacy transcends national borders and involves multiple actors, such as states, international organizations, civil society, private sector, and individuals. How can cyber-diplomats respect the sovereignty and laws of other countries? How can they comply with international norms and agreements on cyberspace? How can they be held accountable for their actions and decisions in cyberspace?

These are some of the ethical and legal implications of cyber-diplomacy for democracy that need to be explored and addressed. Cyber-diplomacy has the potential to enhance democracy, but it also requires ethical and legal frameworks that ensure its responsible and effective use. Cyber-diplomacy can have many benefits, such as enhancing communication, transparency, participation, and cooperation among different stakeholders. However, it can also pose significant challenges and risks, such as cyber-attacks, misinformation, espionage, and interference in domestic affairs (Pamment & Wilkins, 2020).

Some of the ethical and legal implications of cyber-diplomacy for global justice. Global justice is a normative concept that refers to the fair and equitable distribution of rights, opportunities, and resources among all people in the world. It also entails respect for human dignity, diversity, and democracy. Global justice can be affected by various factors, such as globalization, development, human rights, security, and environment.

One of the ethical implications of cyber-diplomacy for global justice is the potential for digital divide and inequality. Digital divide refers to the gap between those who have access to and benefit from digital technologies and those who do not. This gap can be influenced by various factors, such as income, education, gender, age, location, and culture. Digital divide can affect the ability of different actors to participate in and influence cyber-diplomacy processes and outcomes. For example, some countries may have more resources and capabilities to engage in cyber-diplomacy than others. Some groups may have more voice and representation in cyber-diplomacy platforms than others. Some individuals may have more access to and awareness of cyber-diplomacy issues than others (Council on Foreign Relations Report, 2021).

Another ethical implication of cyber-diplomacy for global justice is the potential for cyber-harm and violation of human rights. Cyber-harm refers to any negative impact or damage caused by cyber activities or incidents on individuals, groups, or states. Cyber-harm can include physical harm, psychological harm, economic harm, social harm, or political harm. Cyber-harm can violate various human rights, such as privacy, freedom of expression, freedom of association, freedom of information, and freedom from discrimination. For example, some cyber-attacks may target critical infrastructure or services that affect people's health, safety, or livelihoods. Some misinformation campaigns may spread false or misleading information that affect people's opinions or behaviors. Some espionage operations may collect or leak sensitive or personal data that affect people's privacy or security.

One of the legal implications of cyber-diplomacy for global justice is the lack of clear and consistent rules and norms for cyberspace. Cyberspace is a complex and dynamic domain that transcends national borders and jurisdictions. It involves multiple actors with diverse interests and values. It challenges traditional concepts and principles of international law and diplomacy. For example, some cyber activities or incidents may be difficult to attribute or verify due to anonymity or encryption. Some cyber activities or incidents may be ambiguous or controversial in terms of legality or legitimacy due to different interpretations or perspectives. Some cyber activities or incidents may be disproportionate or excessive in terms of response or retaliation due to lack of proportionality or necessity.

Publisher: SARC Publisher

Cyber-diplomacy has significant ethical and legal implications for global justice. It can offer many advantages but also pose many challenges and risks for different actors and stakeholders in cyberspace. It requires careful consideration and evaluation of its potential benefits and costs for global justice. It also demands collective action and collaboration among different actors and stakeholders to ensure that cyberspace is a safe, secure, open, and inclusive domain that respects human rights and promotes global justice.

SUMMARY

Cyber-diplomacy is the use of digital technologies and platforms to conduct diplomatic activities and achieve foreign policy goals. It has a significant impact on international relations, as it enables new forms of communication, cooperation, and conflict among states and non-state actors. This paper examines the main features, benefits, and challenges of cyber-diplomacy, as well as the implications for the future of global governance and security.

CONCLUSION

This paper explores the impact of cyber-diplomacy on international relations, focusing on three main aspects: communication, cooperation and conflict. The researcher argues how cyber-diplomacy can facilitate dialogue and exchange of information among different actors, foster collaboration and trust on common issues and challenges, and also generate tensions and disputes in the cyberspace. The paper also discussed some of the opportunities and risks that cyber-diplomacy poses for the future of global governance and security. Cyber-diplomacy is not a substitute for traditional diplomacy, but rather a complementary and innovative tool that can enhance the effectiveness and legitimacy of diplomatic action. Cyber-diplomacy is a dynamic and evolving phenomenon that requires constant adaptation and learning from both practitioners and scholars.

RECOMMENDATIONS

The following are the recommendations made by the researcher based on the argument of the study:

1. There is a need to develop a comprehensive and coherent cyber strategy that aligns with national interests and values.
2. Strengthening of cyber resilience and security by investing in infrastructure, capacity building and awareness raising is imperative.
3. There is need to promote cyber norms and rules that foster a peaceful, stable and open cyberspace.
4. Engage in multilateral and bilateral dialogues and partnerships on cyber issues with relevant stakeholders.
5. Support digital inclusion and innovation by bridging the digital gap and fostering a vibrant digital economy and society.

REFERENCES

1. Barrinha, A. & Renard, T. “Cyber-diplomacy: the making of an international society in the digital age.” *Global Affairs* 3.4-5 (2017): 353-364.
2. Barrinha, A. & Renard, T. “Power and Diplomacy in the Post-Liberal Cyberspace.” *The Washington Quarterly* 43.2 (2020): 7-25.
3. Bjola, C. & Holmes, M. (eds.). “Digital Diplomacy: Theory and Practice.” *Routledge* (2015).
4. Council on Foreign Relations Report. The Emergence of Cyber Diplomacy in an Increasingly Post-Liberal Cyberspace: https://www.cfr.org/blog/emergence-cyber-diplomacy-increasingly-post-liberal-cyberspace (2021)
5. Dutton, W. H. & Dubois, E. “The Fifth Estate: A Rising Force of Pluralistic Accountability.” *In W. H. Dutton (Ed.), Politics and the Internet in Comparative Context: Views from the Cloud, Routledge* (2017). 3–18).
6. Forbes Report. “New IP: Huawei's Plan To Replace The Internet – Forbes.” https://www.forbes.com/sites/zakdoffman/2020/03/29/huawei-has-a-plan-to-replace-the-internet-and-its-too-late-to-stop-them/
7. Hocking, B. & Melissen, J, eds. “Diplomacy in the Digital Age.” *Clingendael Institute* (2015).
8. Hocking, B. & Melissen, J. “Diplomacy in the Digital Age.” *Clingendael Report* (2015).
9. Hocking, B., Melissen, J., Riordan, S. & Sharp, P. “Futures for Diplomacy: Integrative Diplomacy in the 21st Century.” *Netherlands Institute of International Relations ‘Clingendael’* (2012).
10. Jovanović, J. & Kerr, P, eds. “Multistakeholder Diplomacy: Challenges and Opportunities.” DiploFoundation.
11. Kurbalija, J. “Introduction to Digital Diplomacy.” *DiploFoundation* (2016).
12. Kurbalija, J. “Introduction to Internet Governance (7th ed.).” *DiploFoundation* (2016).

Publisher: SARC Publisher

13. Kurbalija, J. "The emergence of cyber diplomacy: from idea to practice." *DiploFoundation* (2016).
14. Nye Jr, J. S. "Cyber power." *Harvard University, Belfer Center for Science and International Affairs* (2010).
15. Nye Jr, J. S. "Cyber Power." *In D. Held & P. Maffettone (Eds.), Global Political Theory, Polity Press* (2017): 175–187.
16. Pamment, J. & Wilkins, K. G. "The Handbook of Public Diplomacy." *Routledge* (2020).
17. Riordan, S. "Cyberdiplomacy: Managing Security and Governance Online." *Polity Press* (2019).
18. Tsalikis, A., Kurbalija J. & Radunović V. (eds.) "Introduction to Cybersecurity for Diplomats: A Diplo Reader." *DiploFoundation* (2018).

Source of support: Nil; **Conflict of interest:** Nil.

Cite this article as:
Manuwa, T. "Analysis of the Impact of Cyber-Diplomacy on International Relations." *Sarcouncil Journal of Public Administration and Management* 2.4 (2023): pp 1-9.

Publisher: SARC Publisher