JOURNAL OF JURISPRUDENCE, INTERNATIONAL LAW AND CONTEMPORARY LEGAL ISSUES
Rivers State University, Faculty of Law *ISSN: 1115 5167 Vol.21 Issue.2, 2026*

AN ASSESSMENT OF THE 1961 VIENNA CONVENTION ON DIPLOMATIC RELATIONS AS A LEGAL FRAMEWORK FOR DIGITAL DIPLOMACY AND ITS CONSEQUENCES FOR GLOBAL DIPLOMATIC STABILITY

Desmond O.N. Agwor, Ph.D & Raphael Bappaluk Tokma***

Abstract
For over six decades, the 1961 Vienna Convention on Diplomatic Relations (VCDR) has endured as the indispensable juridical bedrock of interstate intercourse, codifying with remarkable durability the immunities, privileges, and functional prerogatives upon which the entire edifice of modern statecraft repose. Yet this venerable instrument, conceived within a pre-digital epistemology of physical presence and paper-based correspondence, now confronts an unprecedented normative crisis occasioned by the ascendancy of information and communication technologies it was never conceived to accommodate. This article undertakes a rigorous doctrinal assessment of the VCDR's continued efficacy as the legal cornerstone of statecraft, illuminating the significant "legal vacuum" that digital technologies have precipitated within the architecture of diplomatic law. Employing a critical analytical methodology, the study interrogates how digital diplomacy and e-diplomacy have reconfigured the modalities of interstate communication through virtual platforms, engendering negotiation processes that are simultaneously more inclusive and yet impoverished by the absence of non-verbal cues indispensable to high-stakes discourse. The inquiry further scrutinises the contested legal status of virtual embassies, which unsettle the territorial premises upon which the Convention's definitional architecture rests and complicate, in equal measure, the identification of a cognisable "receiving state". In this connection, the article advances a case for a "transformative interpretation" of Article 22, urging that the principle of inviolability be extended to a mission's official digital infrastructure, inclusive of websites and social media assets, as a digital extension of physical premises. The research also probes, with particular attention to doctrinal nuance, the complexities attending diplomatic immunity in relation to cybercrimes, alongside the formidable evidentiary and technical hurdles that beset the legal attribution of state-sponsored cyberattacks. It evaluates, moreover, the transformative implications of Artificial Intelligence and regional regulatory frameworks, notably the European Union's AI Act, for the evolution of global standards of ethical state conduct, while drawing upon the national blueprints of Estonia and Romania as instructive paradigms for the integration of technological expertise into diplomatic institutional structures. Arising from this comprehensive analysis of the hurdles attending the attribution of state-sponsored cyber espionage and the far-reaching implications of Artificial Intelligence for global diplomatic standards, the paper proffers six critical recommendations calculated to secure long-term global diplomatic stability within an increasingly borderless digital order.

Keywords: *Diplomatic Relations, Digital Diplomacy and Global Diplomatic Stability*

1. Introduction

The 1961 Vienna Convention on Diplomatic Relations (VCDR) has, for well over six decades, subsisted as the indispensable juridical cornerstone of international relations, furnishing the

essential normative architecture for interstate communication, the establishment and functioning of diplomatic missions, and the codification of immunities and privileges that undergird the entire edifice of modern statecraft. It remains, in this regard, one of the most successfully ratified and universally observed instruments of public international law, a testament to the enduring wisdom of its drafters. However, the framers of the Convention laboured within a pre-digital epistemological horizon characterised by traditional physical presence, personal envoyship, and paper-based correspondence, a circumstance that renders it increasingly arduous to accommodate the contemporary reality wherein information and communication technologies (ICT) enable states to prosecute foreign policy objectives remotely through an expanding constellation of virtual platforms.[1] In the twenty-first century, the exponential evolution of these technologies has far outpaced the incremental development of universal norms of international law, precipitating a significant "legal vacuum", or, at best, a fragmented regulatory environment in which traditional rules are applied only mutatis mutandis, and often imperfectly, to digital interactions. This regulatory lacuna assumes particular gravity as digital diplomacy consolidates its status as an increasingly autonomous modality of foreign policy communication; the absence of explicit conventional provisions governing virtual embassies, or fixing liability for state-sponsored cyber attacks upon diplomatic resources, threatens materially to erode the very edifice of global stability that the VCDR was designed in perpetuity to preserve. Consequently, this article is impelled by the conviction that, while the VCDR endures as the foundational bedrock of diplomatic law, its long-term efficacy within a borderless cyberspace is contingent upon either a transformative interpretation of its core principles or the adoption of a special protocol, so as to ensure that digital statecraft remains an instrument of peaceful cooperation rather than a vector of unregulated global conflict. It is to a systematic exposition of these doctrinal and normative challenges, and to the formulation of appropriately calibrated legal responses, that the ensuing discussion is addressed.[2]

2. Conceptual Analysis

To advance the discussion, it is pertinent to elucidate key concepts such as digital diplomacy, e-diplomacy, cyber diplomacy, digital statecraft and digital embassy.

i. Digital Diplomacy

Digital diplomacy is comprehensively defined as the systematic and regulated use of modern information and communication technologies by authorized state bodies to strengthen foreign

* Ph.D, LL.M, LL.B (RSU, Port Harcourt), BL (Abuja), DIP (RIVCAS, Port Harcourt), MCIArb; Lecturer at Law, Department of Jurisprudence and International Law, Faculty of Law, Rivers State University, Nkpolu-Oroworukwo, P.M.B. 5080, Port Harcourt, Nigeria.
Tel: +2348035425341, E-mail: desmond.agwor3@ust.edu.ng; desmondnoa@gmail.com
** L.B (Unijos), BL (NLS, Abuja). Tel: +2347037509920 E-mail: raphaeltokma345@gmail.com
[1] I Britchenko, Digital Diplomacy as a Tool of International Legal Communication: Challenges and Prospects. *Journal of International Legal Communication*, (2025) (1) 16, 30-39.
[2] *Ibid*

policy interaction, public communication, and effective international legal coordination within the digital environment. Unlike traditional diplomacy, which for centuries was based almost exclusively on personal meetings, private delegations, and permanent physical missions, digital diplomacy combines these classical principles with the rapid capabilities of the virtual world, allowing for real-time response and a wider scope for public engagement beyond elite circles.[3] In contemporary scientific discourse, this phenomenon is often viewed through a multidimensional lens, categorized into four distinct academic approaches: the instrumental approach, focusing on technical tools; the network approach, emphasizing multilateral information exchange; the reputational approach, concentrating on national image-building; and the legal approach, which addresses norm development and information security.[4] This transformation has enabled states to present their foreign policy agendas to a wider audience, especially for small states that can utilize social media campaigns to punch above their weight in global affairs. However, digital diplomacy also introduces risks of interference in internal affairs through digital technologies, as disinformation and cyberattacks can now be conducted remotely, necessitating a clear legal understanding of how these activities fit within the existing rules of diplomatic law.

ii. E-Diplomacy

The concept of e-diplomacy, which emerged primarily in the early 2000s within the United States Foreign Service, refers specifically to the use of the internet and social networking tools to achieve traditional diplomatic objectives. It was initially viewed as a supplement to classical diplomatic tools, helping to bridge the gap between the government and the people, people to people, and the people to the government in an era increasingly dominated by public diplomacy.[5] E-diplomacy involves the use of blogs, social networks, and other digital communication aids to reshape the complex world of high-level communication, often making it more inclusive by involving a larger number of actors in the dialogue.[6] This modern way of communication has forced a re-evaluation of the 1961 Vienna Convention's applicability, as customs in international law have continued to evolve since the codification of customary law in 1961 due to these technological advances.[7] While e-diplomacy provides convenience and speed, it also introduces significant security risks, particularly when sensitive diplomatic negotiations rely on commercial platforms like WhatsApp or Signal that are vulnerable to hacking and data breaches.

[3] S N Voicu, Digital Diplomacy, A New MicroSphere of Public Communication. *Postmodern Openings*, (2020) 11(3), 160-176. https://doi.org/10.18662/po/11.3/205
[4] M A Ali, and B J Abdul Jabbar, The application of rules of diplomatic law to digital diplomacy. *Al-Iraqia University Journal*, (2024) (2) 1-22.
[5] A Ross, Digital Diplomacy and US Foreign Policy. *The Hague Journal of Diplomacy*, (2011) 6(3-4), 451–455.
[6] J Kurbalija, *E-diplomacy and Diplomatic Law in the Internet Era*, (DiploFoundation/NATO CCD COE 2013).
[7] M O Nedelea, The Transformation of Diplomacy in the Digital Age: The Legal Framework, Security Challenges, and the Estonian Model. *European Journal of Law and Public Administration*, (2025) 12(2), 63–77.

iii. Cyber Diplomacy

Cyber diplomacy is a specialized field that focuses specifically on the "what" of diplomacy, dealing with the negotiation of norms, rules, and standards for state behavior in cyberspace. Unlike digital diplomacy, which uses digital tools to conduct general foreign policy, cyber diplomacy addresses the policy and legal aspects of the digital realm itself, including issues such as internet governance, data privacy, and the application of international law to state-sponsored cyber operations. It is primarily concerned with establishing principles for responsible state behavior in cyberspace to ensure a global, open, free, stable, and secure digital environment.[8] Cyber diplomats often play a key role in the fight against international cybercrime, the protection of critical information systems, and the promotion of a humanistic perspective on digital transformation. States such as Estonia have established dedicated cyber diplomacy departments to secure their cyberspace and contribute to international law and norms. This field is becoming increasingly vital as digital platforms become the primary arena for competing for influence and shaping a nation's image, while simultaneously hosting threats like cyber espionage and disinformation that can undermine international security.[9]

iv. Digital Statecraft

Digital statecraft is the most encompassing term in this field, referring to the use of all instruments of national power diplomatic, economic, military, and informational to pursue a state's interests in the digital domain. It represents the full integration of digital considerations into a state's foreign and security policy, going beyond traditional diplomacy to include intelligence gathering, cyber operations, and the promotion of a country's technological model on the world stage.[10] Digital statecraft recognizes that the geopolitical balance of power is increasingly shifted by investments in research and development of new technologies, which are often used in the "grey area" between war and peace.[11] Countries like Denmark have pioneered this approach by appointing "tech-ambassadors" who liaise directly with the global IT industry to strengthen ties and encourage investment, effectively creating a new era of "Tech Plomacy". This strategy involves not only representing government interests to tech giants but also collecting knowledge on global technological trends to inform domestic public debate and policy development.[12] Digital statecraft is thus the art of using digital means to achieve strategic objectives, requiring a robust and coherent legal framework to ensure the effectiveness and legitimacy of these expansive actions.

v. Virtual Embassy

A virtual embassy is a diplomatic mission that exists only on an electronic network, such as the metaverse or platforms like Second Life, and has no physical basis on the ground in the receiving

[8] M Schmitt, *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. (Cambridge University Press, 2017) 23.
[9] *Ibid*
[10] K Burkadze, Legal aspects of digital diplomacy. *Law and World Journal*, (2023) 9(25), 70–76.
[11] *Ibid*
[12] https://journalresearchstream.ijarms.org/index.php/rs/article/view/69

state. Pioneered by the Maldives in 2007 and followed by nations like Barbados, Sweden, and South Korea, these digital posts are designed to provide administrative and consular services while allowing small countries to participate more meaningfully in international relations.[13] Virtual embassies enable states to establish a presence and expand relations with many more countries than they could afford physically, acting as a low-cost tool for establishing allies and providing services worldwide. They often reflect traditional national architecture in their digital design and are intended as a forum for interaction in business, tourism, and cultural industries.[14] However, virtual embassies disrupt traditional interpretations of VCDR Articles 2 and 41[15], which require the establishment of permanent missions on the basis of mutual agreement and the conduct of official business through physical ministries. They challenge the territorial definition of "premises of the mission" under VCDR Article 1(i), leading to legal uncertainty regarding their protected status and immunities.

3. Transformation of Core Diplomatic Functions Under Article 3

Article 3[16] defines the primary functions of a diplomatic mission as including the representation of the sending state and negotiation with the government of the receiving state. Modern technology has radically reconfigured the method of representation, as heads of state and senior officials are now capable of communicating continuously through digital platforms, often establishing direct public interactions that bypass the traditional mediation of the permanent resident mission.[17] This shift allows for the implementation of foreign policy goals and the projection of national influence without a constant physical presence in every part of the world, though it simultaneously risks diminishing the historical symbolic role and situational authority of the resident diplomat.[18] ICTs play a pivotal role in facilitating interactive relationships for missions with both official stakeholders and the broader public in the host country, transforming representation into a dynamic, real-time activity. In the field of negotiation, Article 3(c)[19] is challenged by the rise of online talks and digital conferencing platforms, which have become a mainstay of international relations, particularly accelerated during the global health crisis. Digital tools have made international negotiations significantly more inclusive by facilitating the participation of a larger number of actors, including civil society and business representatives, as evidenced by the World Summit on the Information Society (WSIS).[20] Also, the internet allows negotiators to access vast amounts of

[13] A Gupta, Metaverse: Challenges and Opportunities for Diplomacy and International Relations. *International Law and Politics*, (2023) 55(1), 1–15.
[14] *Ibid*
[15] VCDR 1961, Art 2 & 4
[16] VCDR 1961, Art 3
[17] S Ahmed, and A Paliwal, Cyber Espionage and the Limits of State Responsibility. *Proceedings of the ICLT* 2025, (2025) 16-26.
[18] *Ibid*
[19] VCDR 1961, Art 3(c)
[20] A Gupta, Metaverse: Challenges and Opportunities for Diplomacy and International Relations. *International Law and Politics*, (2023) 55(1), 1-15.

statistical, economic, and cultural data in real-time, enabling a more practical and informed drafting of negotiating texts and facilitating immediate decision-making during high-stakes talk. This digital efficiency allows diplomats to send strong signals or messages that reach the largest possible audience both internally and externally within seconds, making digital signals essential for modern diplomacy. Despite these clear efficiencies, online negotiation environments frequently suffer from the profound loss of "human elements," such as body language, eye contact, and other non-verbal cues that are essential for high-level communication. This lack of physical proximity can significantly reduce trust between parties and make it difficult for negotiators to recognize the credibility or seriousness of their counterparts, which may paradoxically slow down the process of reaching an effective, lasting agreement. Furthermore, communicating online for negotiation reduces the ability to accurately interpret situational developments, potentially leading to misunderstandings between sides. Additionally, the pervasive risk of identity manipulation, deep fakes, and fraud in online environments poses a continuous threat to the integrity and confidentiality of sensitive diplomatic exchanges, as verifying the identity of parties involved in online talks remains difficult. Technology has also enabled the specialized practice of "shuttle diplomacy" through the creation of secure and non-confrontational channels for dialogue between warring groups or parties in conflict. Digital platforms serve as a vital key to conflict resolution, reconciliation, and preventive diplomacy by allowing for rapid information sharing and the receipt of immediate feedback on peace initiatives.[21] ICTs across mainstream media and new media platforms play a large role in supporting diplomats by creating awareness for new initiatives and policies designed to address key public issues. However, to maintain the necessary decorum and professionalism, digital diplomacy must adopt strict procedural standards to ensure that even informal exchanges on platforms like WhatsApp or Signal adhere to the time-honored principles of discretion, confidentiality, and mutual respect.

4. The Legal Status of Virtual Embassies and the "Receiving State" Dilemma

The establishment of virtual embassies pioneered by the Maldives in 2007 and followed by nations such as Barbados and Sweden presents a direct challenge to the territorial definitions inherent in the VCDR. Article 1(i)[22] of the Convention defines "premises of the mission" specifically as physical buildings and ancillary land utilized for the purposes of the mission, a description that does not explicitly encapsulate 3D immersive spaces established in the metaverse.[23] This creates a significant legal hurdle, as it remains unclear whether these digital posts enjoy the full protections, such as inviolability and tax exemptions, granted to traditional missions under existing treaty standards. The unique nature of the metaverse, which combines VR and AR, only adds to the complexity of regulating these developments under a convention drafted in the 1960s. A major legal and political dilemma arises in identifying the "receiving state" for virtual diplomatic posts,

[21] Gupta (n 13).
[22] VCDR 1961, Art 1(i)
[23] Gupta (n 13)

as the borderless environment of the metaverse does not align with traditional notions of jurisdiction. Both the VCDR and the Vienna Convention on Consular Relations (VCCR) impose specific, continuous obligations on a "receiving state" within whose territory the mission must be established to be legally valid.[24] Without a clearly defined receiving state, it becomes impossible to enforce host-state obligations, such as the facilitation of premises under Article 21 or the provision of security and inviolability under Article 22, which are essential for the mission to function legally.[25] This mandate of being in the receiving state is present in numerous provisions, making the identification of a host state a prerequisite for the application of diplomatic law. One proposed solution for this dilemma is to identify the receiving state as the nation whose national visits or interacts with the virtual embassy. This is based on the rationale that the treatment and safety of the nation is of concern to the state involved. However, this approach is deemed impractical because diplomatic obligations like immunity and inviolability are continuous in nature and cannot be based on the sporadic, individual visits of nationals from different states. Such an interpretation could lead to the incoherent scenario where a national of the sending state visits the virtual office, effectively making the sending state its own receiving state, which is a legal impossibility under the framework of the VCDR and VCCR. Consequently, subsequent visits by other nationals cannot remedy the fundamental lack of a host state at the time of the mission's creation. An alternative interpretation suggests that the state hosting the physical servers for the metaverse platform should be designated as the receiving state.[26] Servers are physical data centers that store all content shared over a platform, and their location could theoretically provide a territorial link for legal jurisdiction. This is legally problematic because a vast majority of the world's physical data centers are concentrated in a few Western nations, such as the United States and Ireland. Adopting this server-based method would grant these host nations a disproportionate level of authority over the digital missions of other states, potentially subjecting sensitive foreign missions to the internal laws and regulations of the Western host nation. As a result, the international community currently lacks a foolproof method for determining a receiving state in a digital context, leaving virtual embassies in a state of legal uncertainty.

5. Expanding the Principle of Inviolability to Digital Infrastructure

Article 22[27] mandates the absolute inviolability of mission premises, obligating the host state to take all appropriate measures to protect against intrusion, damage, or any disturbance of the peace. In the modern digital age, legal experts argue for a "transformative interpretation" of this article, where a mission's official website, social media accounts, and digital assets are treated as a "digital extension" of its physical facilities.[28] This conceptual expansion is necessary because the

[24]I Britchenko, Digital Diplomacy as a Tool of International Legal Communication: Challenges and Prospects. *Journal of International Legal Communication*, (2025) (1) 16, 30-39.
[25]*Ibid*
[26]Gupta (n 13)
[27] VCDR 1961, Art 22.
[28] Burkadze (n 10).

compromise of a mission's digital infrastructure can be just as damaging to diplomatic prestige and national security as a physical breach of an embassy building.[29] The 2007 cyber attacks on Estonia served as a stark wake-up call in this regard, demonstrating that the vulnerability of digital infrastructure can escalate into a major diplomatic crisis. Under this modernized framework, host states would have an international obligation to provide advanced security measures to protect these digital spaces from cyber attacks, just as they provide physical security guards for embassy gates.

This duty includes the use of encryption, intrusion detection systems, and other sophisticated cyber security measures that ensure the safety of sensitive data[30]. Some scholars even suggest that a crippling cyber attack could be interpreted as a "disaster" requiring immediate intervention, similar to the emergency exceptions for fire or natural disasters found in consular law under Article 31 of the VCCR. This proactive approach would require the host state to intervene to stop attacks that disrupt the essential work of the diplomatic mission, thereby maintaining the "peace" of the mission in the virtual domain. The tension between traditional territorial sovereignty and the borderless nature of cyberspace is acutely highlighted when a mission's digital infrastructure is allegedly used to commit a cybercrime, such as producing malware or attacking host-country networks. Even if host-state intelligence services detect malicious activity originating from an embassy's computer, the authorities cannot enter the physical premises to investigate or seize hardware without the express approval of the head of the mission. This creates a digital shield that protects diplomats, ensuring that the principle of inviolability remains paramount even when it potentially conflicts with the host state's domestic criminal laws. In consular contexts, the host state might have slightly more options, such as entering non-consular parts of a building, but diplomatic premises remain strictly off-limits without consent.[31] Historical case law, most notably the Tehran Hostages case, affirms that a host state has a flagrant obligation to protect the premises and correspondence of a mission from attack. In the contemporary context, this duty must logically extend to safeguarding the official online platforms of embassies against state-sponsored surveillance, data exfiltration, or hijacking.[32] The UN General Assembly's resolution on "The Right to Privacy in the Digital Age" reinforces this by affirming that the same rights individuals enjoy offline, such as the privacy of correspondence, must be rigorously protected online.[33] Undoubtedly, this resolution applies to diplomats as private individuals entitled to privacy in their correspondence, and any host-state censorship of these digital communications is contrary to the spirit of both the UN resolution and the VCDR.

[29] *Ibid*
[30] I Britchenko, Digital Diplomacy as a Tool of International Legal Communication: Challenges and Prospects. *Journal of International Legal Communication*, (2025) 16(1), 30-39.
[31] S N Voicu, Digital Diplomacy. A New MicroSphere of Public Communication. *Postmodern Openings*, (2020) 11 (3), 160-176.
[32] *Ibid*
[33] *Ibid*

6. Diplomatic Immunity and the Complexities of Cyber Espionage

Diplomatic immunity, governed by Article 31 of the VCDR[34], exempts envoys from the criminal, civil, and administrative jurisdiction of the receiving state. This broad immunity logically extends to cybercrimes and civil offenses committed via digital platforms, such as online defamation, slander, or unauthorized data access. While such protections are essential to prevent host-state harassment of diplomats, they create significant challenges for a receiving state attempting to hold actors accountable for modern digital wrongdoings[35]. In the event of human rights violations committed through digital means, the ICJ has noted that the only real remedy available to a host state is declaring the perpetrator *persona non grata* under Article 9. Cyber espionage represents the most significant and unresolved challenge to this legal framework, as it is a clandestine activity that utilizes digital tools to exfiltrate sensitive information from governments or corporations. While cyber espionage is not explicitly prohibited under peacetime international law, it raises serious legal concerns regarding the violation of state sovereignty and the principle of non-intervention. The Lotus Case establishes that states are free to act unless explicitly prohibited, a principle that continues to shape the permissive view of espionage in the international arena.[36] Some academic perspectives even suggest an affirmative "right to spy" for national defense purposes, further complicating the development of a binding prohibition against such activities in cyberspace.

A primary hurdle in establishing state responsibility for cyber espionage is the profound technical and legal difficulty of "attribution". Attackers frequently employ sophisticated anonymizing tools, proxy servers, and fake digital identities to hide their true origin, allowing perpetrating states to maintain "plausible deniability". For instance, during the 2009 "GhostNet" operation that targeted diplomatic information in over 100 countries, technical indicators pointed toward Chinese servers, but no conclusive legal evidence could definitively link the activity to the state. Because high-confidence intelligence often falls short of the evidentiary threshold required by international courts, linking an attack to a specific state actor remains elusive. Cyber espionage often leaves no visible or physical damage, which complicates the legal requirement to show "legally cognizable damage" or injury. Traditional international law typically seeks evidence of tangible harm to persons or property, whereas digital surveillance results in the exfiltration of intangible data.[37] However, emerging legal arguments contend that the loss of confidentiality, national security, or strategic advantage should be recognized as a legitimate injury, especially when it targets critical state functions. Without a universal regulatory instrument, the mechanisms for holding states

[34]VCDR 1961, Art 31.
[35]S Ahmed, and A Paliwal, Cyber Espionage and the Limits of State Responsibility, *Proceedings of the ICLT 2025*, (2025) 16-26.
[36]Ahmed (n 35)
[37]*Ibid*

responsible for digital intrusions remain uncoordinated and highly fragmented, often resulting in public "naming and shaming" rather than formal legal accountability.

7. Integrating AI Aad Regional Regulatory Models for Stability

Artificial Intelligence (AI) is rapidly transforming the practice of diplomacy by enabling big data analysis, predictive modeling for strategic decision-making, and the automation of routine administrative tasks. States use AI to respond more effectively to complex geopolitical challenges, yet its use introduces significant risks related to ethical transparency, algorithmic bias, and the potential for deep fakes to disrupt international relations. Panellists at the "Diplomacy in the Digital Age" dialogue emphasized that trust in AI depends on its ability to provide clear, understandable justifications for decisions, a challenge known as "explainability". Robust international collaboration and ethical oversight are required to ensure that AI serves to enhance diplomatic capacity rather than becoming a vector for destabilization.[38] The European Union has established itself as a global "digital normative power" through the adoption of the world's first comprehensive legislation on AI, the AI Act. This innovative, risk-based framework prohibits unacceptable practices like social scoring and imposes strict transparency and safety obligations on high-risk systems. For digital diplomacy, the AI Act sets a global standard, the "Brussels effect" influencing how AI is developed and used by other countries and ensuring it respects fundamental rights and human-centric values.[39] The EU's digital diplomacy is further supported by the Digital Services Act (DSA), which provides legal tools to combat disinformation and information manipulation that threaten national security. National models, particularly those of Estonia and Romania, provide successful blueprints for integrating digital considerations into national statecraft. Estonia's "X-Road" secure data exchange and its unique "e-Residency" program demonstrate how a small state can project significant international influence by promoting its model of e-governance and hosting centers of excellence like the NATO CCDCOE. Similarly, Romania's Law 58/2023 represents a pioneering effort to explicitly regulate "cyber diplomacy" as the promote of national foreign policy interests within cyber security negotiations. These models show that technological expertise can be a valuable diplomatic asset, allowing states to adapt to the requirements of the digital environment and actively shape international standards. Despite the success of these models, states face ongoing challenges related to technological dependence and the rivalry between competing models of digital governance. The Estonian experience highlights that even the most advanced digital societies remain vulnerable to paralyzing cyber attacks, and the reliance on technologies developed by multinational companies can limit a state's decision-making autonomy.[40] To maintain long-term stability, the international community should follow the "United Europe" model, jointly protecting strategic interests through regional partnerships and alliances. By consolidating these bilateral and

[38] S Roy, The Role of Artificial Intelligence in Shaping Global Diplomacy. *Research Stream* (2026) (1) 3, 44-48.
[39] *Ibid*
[40] A Gupta, Metaverse: Challenges and Opportunities for Diplomacy and International Relations. *Journal of International Law and Politics,* (2023) (1), 1-15.

regional digital dialogues, states can promote a stable, predictable digital space based on the rule of law and mutual respect for fundamental rights.[41]

8. Conclusion

Digital diplomacy has permanently and irreversibly altered the landscape of international relations, yet the rapid pace of technological innovation continues to outstrip the development of universal legal norms, creating a dangerous fragmentation in the global order. While the VCDR remains a remarkably resilient framework for traditional interactions, the current "legal gap" regarding virtual missions, cyber espionage, and AI governance threatens to undermine the very stability it was designed to preserve by allowing state actors to operate in a gray zone of accountability. This article concludes that the most effective and necessary path forward is the urgent development of a special protocol or specific amendments to the VCDR that define the status of virtual institutions and establish secure, harmonized standards for digital communication. Ultimately, the future of global diplomatic stability depends on a concerted international effort to bridge these legal gaps through collaboration, ensuring that the digital arena remains a space for peaceful cooperation, transparency, and the protection of fundamental human rights for all nations.

9. Recommendations

Flowing from the hurdles of attributing state-sponsored cyber espionage and evaluated Artificial Intelligence's impact on global diplomatic standards, the study recommends as follows:

i. Adoption of a special protocol or specific amendments to the VCDR to define the legal status of virtual institutions and establish universal norms for digital statecraft.
ii. Implementation of a "transformative interpretation" of Article 22 to extend the principle of absolute inviolability to a mission's official digital infrastructure and sensitive data assets.
iii. Establishment of harmonized international standards and strict procedural rules for digital communication to mitigate risks of hacking, data breaches, and identity manipulation.
iv. Utilization of successful national and regional models, such as the "United Europe" approach, to build collective cyber-defense and ethical AI oversight frameworks.
v. Establishment of a specialised international attribution mechanism, comprising technical and legal experts, to develop harmonised evidentiary standards for adjudicating claims of state-sponsored cyber espionage and to lower the threshold of "plausible deniability" presently enjoyed by perpetrating states.
vi. Institution of mandatory capacity-building and continuing legal education programmes within foreign ministries and diplomatic academies, to equip envoys with the technical literacy and ethical grounding necessary for the responsible deployment of Artificial Intelligence and other emerging technologies in the conduct of statecraft.

[41] *Ibid*