P-ISSN 2708-6453	Pakistan Languages and Humanities Review	May-June 2026, Vol. 10, No. 3
O-ISSN 2708-6461	https://doi.org/10.47205/plhr.2026(10-III)05	[45-56]

Pakistan Languages and Humanities Review
www.plhr.org.pk

RESEARCH PAPER

Digital Diplomacy: Navigating the Cyber War in International Affairs

[1]Aleeza Arshad, [2]Laiba Nadeem and [3]Mobeen Waqar

1. MS Scholar, Department of Politics & International Relations, GC Women University Sialkot, Punjab, Pakistan.
2. MS Scholar, Department of Politics & International Relations, GC Women University Sialkot, Punjab, Pakistan.
3. MS Scholar, Department of Politics & International Relations, GC Women University Sialkot, Punjab, Pakistan

Corresponding Author alizehchaudhary2@gmail.com

ABSTRACT

Cyberspace is rapidly changing the face of international relations, creating new forms of conflicts, competitions and diplomacy of which states are still only now gaining a full understanding of and control over. In this study, the term digital sovereignty is discussed in the context of the present cyber warfare and is analyzed based on several recent literatures and sources from academia that present it as a new method of state diplomacy to attempt at the solution to ever increasing cyber-warfare threat to the States. The research is qualitative and descriptive and based on secondary sources only, it focuses on some of the main themes in cyber diplomacy, namely the development of cyber diplomacy, salient cyber incidents, international frameworks for cyber governance and attribution and regulation in cyberspace. Security is found to be an integral part of twenty-first century foreign policy and that digital sovereignty combined with strong cyber diplomacy is an adequate measure to counter cyber threats as military deterrence or technical defense have proven themselves to be insufficient measures.

Keywords: Cyber-War, Digitalization, International Relations, Diplomacy

Introduction

International relations have seen a dramatic loss of many of their classical traits in the last few decades, accompanied by the rapid development of digital technologies. Nowhere is this truer than with Cyber space, which has become a new arena in which countries are competing, cooperating and conflictual rather unthinkingly a generation ago. In recent years, digitisation has become a central feature of our society and is the building block of all sector-oriented activities, including digital security, which is crucial in today's world where the digitalization of economic activity or even military actions has become indispensable. The research project "Digital Diplomacy: Navigating the Cyber War in International Affairs" aims to challenge the role of digital diplomacy in responding to cyber threats as well as the implications for international security. This work aims to better understand the capabilities that countries can pursue in their foreign policies and how these capabilities can be managed through diplomacy with consideration to the dangers that may arise.

As cyber-attacks are becoming increasingly common and sophisticated worldwide, this study has become more and more pertinent. Digital incidents can disrupt and wreak chaos globally on any agency, business or critical infrastructure. The examples of the WannaCry ransomware attack in 2017 affecting more than 150 countries,

and the SolarWinds breach in 2020, demonstrate just how susceptible the connected world is. This concept for a project, being the fusion of technology and international relations, a topic which is still in its early stages of development and needs further research, compelled me to choose it. From my perspective as a student of international affairs, it is important to understand that one must evolve the traditional principles of diplomatic relationship in order to deal with the new threats of the Cyber World.

The rationale for this research is the importance of finding effective diplomatic response to cyber conflicts as an integral aspect of modern diplomacy. So for now the international community doesn't have a set of comprehensive norms and mechanisms to govern states' activities in their cybertronic domain, and that causes uncertainty and potential escalation. The study's significance lies in its contribution to the ongoing discussion on the role of digital diplomacy in promoting cooperation and averting conflicts between states. This work seeks to provide the policy-maker, and the academic, with useful insights gained from examining how the various countries deal with these cyber tensions. Cyber warfare, therefore, is an important subject for anyone involving themselves in international relations now and in the future: The modern world is a cyber one, and with greater than ever opportunities comes the dangers.

Literature Review

Aldrich and Karatzogianni focus their discussion on the evolving linkage between cyber power and cyber diplomacy and how the international system is changing in the digital era. One aspect they raise is whether cyber power is an extension of traditional soft power concepts attributed to them or if it is a new type of power that requires fresh thinking. The authors investigate how Power itself has been changed through the use of digital technologies and hearken a unique focus on the role of big tech firms and how they either boost or undercut national power. One preoccupation in their efforts is making sure that diplomats are not simply resuming traditional practice involving things like persuading, propagating and espionage, but that something truly new, even more flexible, is being developed as a new form of internet governance diplomacy. They also call attention to a conscious dichotomy of the field between younger scholars who study the arms races through the lens of the cybersphere and older scholars who are interested in diplomacy and normative control. A new development within the international landscape of relations is the emergence of specialized diplomats specializing in the sphere of AI, cyber security and big data. The chapter should take the discussion of cyber power one step further and to remove the military perspective, noting that cyber diplomacy is now a significant and integral component of managing global affairs today.

However, for this kind of diplomacy to remain stable, as states are becoming more and more eager to use offensive cyber means for military operations and espionage, the actors should also build up the capacity to do effective cyber diplomacy, as Tiirmaa-Klaar (2025) noted. She acknowledges the conflicts between offensive cyber and diplomatic activities, with this being a prime management challenge for government. She says Cyber diplomacy can be used to prevent conflicts, foster trust, increase transparency and prevent misunderstandings that could escalate into crises. The chapter also underscores the insufficiently recognised part that plays in security-by-design – making digital products secure from the ground up – played by those who don't wear a uniform and wear a hat. Therefore, Tiirmaa-Klaar considers such regulation as complementary to diplomacy, as it will increase overall cyber resilience. In addition, she reviews the various conceptions of cyber conflict held by different states and the cyber espionage as a phenomenon, as well as the current international frameworks for holding

someone accountable in cyberspace. She believes cyber warfare and cyber diplomacy are closely linked and that a mixture of diplomatic and good regulation is key to a peaceful and secure cyber world.

A very influential early conceptualization of cyber-diplomacy as a field and not just a further tool of traditional diplomacy can be seen in Barrinha and Renard (2018). They maintain that a fundamental shift in the significance of cyberspace in IR has caused the incorporation of cyber matters into foreign policy and the creation of new diplomatic positions. They believe increasing the relevance of cyberspace in IR has compelled states to devote attention to cyber issues in foreign policy and formed sub-commission positions: diplomatic scores. Informed by the English School of International Relations, they conceptualise cyber-diplomacy as a new type of international practice that helps shape the establishment of a "cyber-international society" characterised by common norms, rules and expectations about the behaviour of states online. In the authors' view, cyber-diplomacy is situated between the interests of the country and social or wider global dynamics, demonstrating the unique nature of cyberspace. They found it paramount to establish international cooperation and governance in the digital space while also identifying its challenges, hence providing a theoretical grounding in the study of diplomacy in this new era of digitalization (Barrinha & Renard, 2018).

Kasper, Osula and Molnár discuss the very gradual shift of the European Union's attitude towards cybersecurity and cyber diplomacy from data security policies specific to a few sectors of the economy to the protection of critical infrastructure, technological sovereignty, countering cybercrime and responsible state activity in cyberspace. They emphasize the fact that cyber diplomacy is a relatively new but growing field of EU policy, which is still not completely defined. Cyber diplomacy, seen as "public diplomacy 2.0," is sometimes considered to be a public diplomacy in the digital realm because of the lack of boundaries in the cyber space and the proliferation of civilian-military and domestic-foreign policy interactions. An important aspect of the article is its focus on EU cyber diplomacy instruments and capacities: it gives insight in how these are being used in practice. The authors also investigate if cyber diplomacy is becoming a new policy field, or staying a part of the general cyber-security policy. They consider that despite the considerable advances made, it is important to redefine the institutional and conceptual framework of cyber diplomacy at a higher level yet (Kasper, Osula & Molnár, 2021). Hallams (2010) contend that the internet is redefining the landscape of government communication and engagement with audiences worldwide, and that diplomatic communication online is an increasingly powerful tool in the foreign policy tool-kit. In this study, in which the author concentrates on the U.S. example, she explores how the Obama administration reacted to Al-Qaeda's success in using the internet to propagandize and use “Public Diplomacy 2.0” to reach foreign publics, in particular Muslim youth. Based on soft power theory, Hallams believes that the power of disseminating credible messages online through a campaigning approach is as relevant as military action in combating extremist narratives. Digital technologies extend the diplomat's outreach; but, as she notes, it's not about the technology, but about what's said and how well and persuasively it is said. She ends up saying digital diplomacy has become an integral part of modern foreign policy—and a central battleground in the all-world contest of ideas.

Barrinha and Renard's apparent work to elaborate a criterion for cyber-diplomacy is one of the most considered and placed early attempts to establish cyber-diplomacy as a discipline of its own at the same time attempting to produce an accurate picture of the field. They start with the fact that the world of cyberspace has become a

very much focal point of international relations and most major powers are directly dealing with cyber issues in their foreign policies, and creating special envoys to do so! They highlight how and why cyber-diplomacy has emerged, and leave readers with a deep understanding that the concept of cyber-diplomacy is a middle-ground issue that combines the national interests of specific nation states with the global dynamics of world society, where cyberspace itself has evolved over the last few decades. Cyber diplomacy is actively attempting to develop a 'shared set of norms, rules and expectations [which] could appropriate state behaviour online, analogous to traditional diplomacy that governs behaviours in the real world. Put simply, their analysis offers a solid theoretical starting point for exploring the question of why the emergence of shared-governance formats for cyberspace continues to strain relationships, even as the phenomenon of digital diplomacy is becoming more prominent and necessitating a conceptual reevaluation of diplomacy in the digital realm (Barrinha & Renard, 2018).

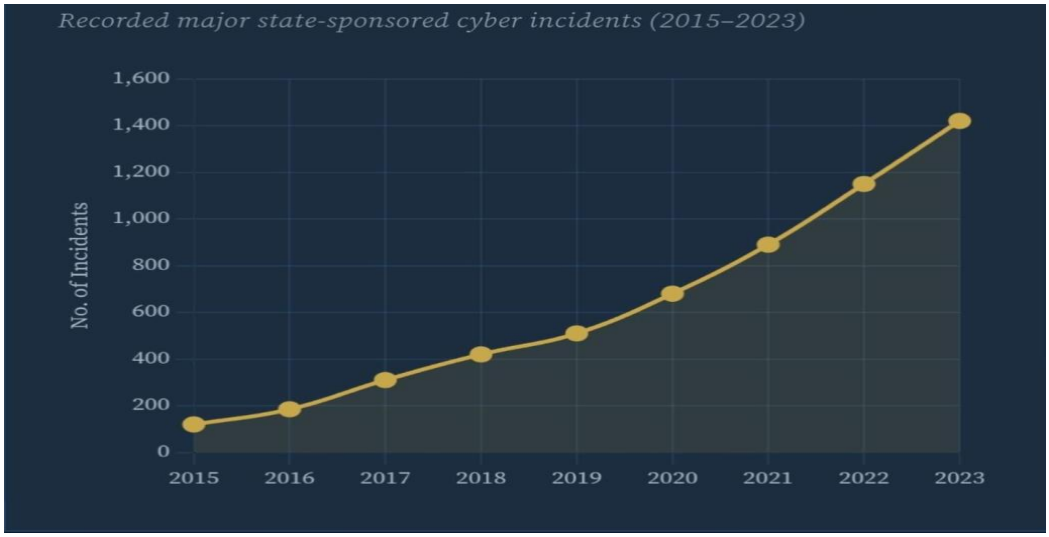

Figure 1: Global Cyber-attacks annual growth

Bukhari and Siddiqui (2026) claim that establishing digital sovereignty has emerged beyond mere technical domain as a tool for cyber warfare and leverage for the powers of the state. It gives states the means to gain control of digital infrastructure, defend national interests and have a stronger hand to play in cyberspace. The authors connect sovereignty over data, systems and technology with geopolitical leverage, and demonstrate that with respect to technology and data, the world is becoming more sophisticated, with capabilities now increasingly restricted to certain countries. To directly influence international relations. They also highlight that cyber warfare has become a new dimension of the conflict, for which a comprehensive approach is necessary, in which cyber operations are linked with diplomatic activities. At this level, the concept of digital sovereignty acts as a means of dissuading cyber risks and contributes to establishing an environment of trust and establishing responsible state practices. It is also important for developing countries as it provides them with a power to countervail the influence of leading technological nations and help them gain a status in the international community. The report emphasizes that cyber conflicts are becoming more intricate between state and non-state actors as well as between States and private business entities. As a whole, they say that digital sovereignty is key to modern power politics, as well as cyber security and diplomacy.

In a new legal and political study, Buchkovska (2025) analyzes cyber diplomacy from the perspective of its importance in modern geopolitics and explains how it has

emerged as a major tool for states to ensure their digital future amid escalating cyber challenges and disputes. Cyber diplomacy is heralded as an integral part of foreign policy, important for ensuring relations, resolving disputes and creating shared norms on-line. Important legal issues are underlined, including the uncertainty of how to transpose the current law into the cyberspace context, in which the problems of attribution, indistinct boundaries and enormous technological evolution render the application of the international law problematic. It also highlights the ongoing struggle between state sovereignty and the globalized and borderless digital world, making consensus building tougher. Buchkovska also examines the contribution made by multilateral approaches and institutions to bridging some of the legal voids that have not yet been completely plugged, and how present multilateral agreements rely on traditional law in many instances.Although these multilateral approaches and institutions remain irregular and weak, Buchkovska also addresses the gaps they fill in relation to traditional law; in some respects, they will depend upon it. She also discusses the increasing role played by private technology companies in cyber diplomacy, which may be problematic for accountability and oversight. In her overall conclusion, she argues for greater legal cooperation, trust and coordinated international governance to make cyber diplomacy a more effective process.

Barrinha and Renard (2018) regard cyber-diplomacy as an institution of international society and not just an extension of traditional diplomacy. According to them, states can be seen as intent on fostering a "cyber-international society", established through partnerships of norms and governance in the cyber sphere, through the prism of the English School approach. These demonstrate that cyber space is now an essential environment for international relations and that there is a growing tendency of States to make cyber a focus of foreign policy and to create formal career-level foreign affairs positions for cyber. Their analysis of the conflict between the state interests and a decentralized, transnational space of cyberspace underlines the need and the complexity of norm-building. They question if it is possible to establish a stable global governance in cyberspace, in the face of developing geopolitical competition today. Overall, they offer a solid basis to know cyber diplomacy as a nascent international institution (Barrinha & Renard, 2018). The author of this book, Alethawy (2022), explores the concept of digital diplomacy as a contemporary foreign policy instrument, influenced by the fast-paced changes of technology especially in the context of social media and online platforms. He says these tools help states to reach any audience in the world in a faster and simpler way than traditional diplomatic means. According to Ulema, digital diplomacy is a type of public diplomacy that utilizes digital technologies to engage foreign publics and a state's agenda. The article highlights the fact that 'Digital diplomacy' is not the replacement for the traditional form of diplomacy but is a complement to it and must be used in a formal diplomacy process. It also includes a discussion of some of the main tools used by social media, virtual embassies and online diplomatic training. Meanwhile, Alethawy warns of cybersecurity threats, which are rooted in the new digital tools that are vulnerable to creating state consistency issues when dealing with their diplomatic affairs. In general, he highlights that there is a strong similarity between digital diplomacy and cybersecurity in modern foreign policy (Alethawy, 2022).

Material and Methods

In this study, the secondary sources like peer-reviewed journal article and academic book chapters that are relevant to digital diplomacy, cyber sovereignty and cyber security were used. To use descriptive approach to explain the concept and the

development and to use analytical approach to critically explore the scholarly arguments and pattern across the literature. Study is conceptual, no primary data or fieldwork done. This blend of description and analysis offers a comprehensive and sophisticated grasp of digital sovereignty's use as a diplomatic instrument in cyber operations today.

Results and Discussion

Modern International Relations Cyber Threat.

Types of Cyber Threats

Some of the elements of cyber threats today range from ransomware and phishing, denial of service attacks, espionage and disinformation campaigns. They target various parts of the functioning of the state and society, including disruption of energy infrastructure, stealing of valuable government data, and manipulation of public opinion.

Major Cyber Incidents

The seriousness of Cybercrime has become non neglection in real life. In the 2017 WannaCry attack, its ransomware was able to penetrate 150 countries in mere hours and paralyze hospitals, banks and government systems around the world, leaving a trail of business disruption.The WannaCry attack of 2017 spread to 150 countries and stopped hospitals, banks and government systems within a matter of hours, leaving a path of business disruption. Worse, the SolarWinds incident of 2020 installed a malicious update on trusted software used by people working at numerous US government agencies, making it clear that even the most secure institutions are vulnerable to such breaches.

State-Sponsored Cyber Attacks

One of the emerging topics in world affairs is the role played in the world by governments in their cyber operations. Cyber campaigns to steal intelligence, disrupt democratic processes, and undermine opposing economies have been documented in states such as Russia, China, and North Korea against countries that are not currently engaging in "full spectrum" conventional warfare.

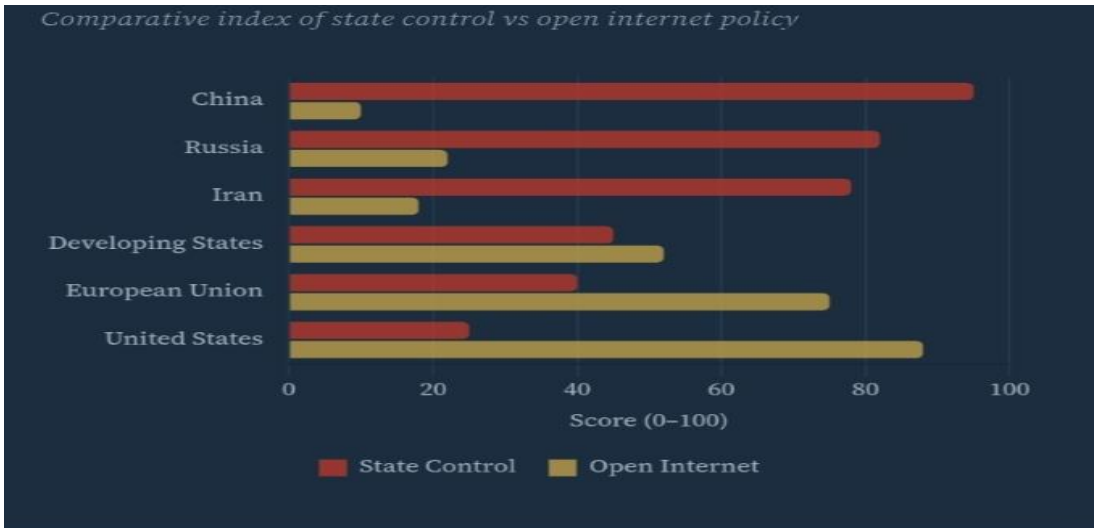

Figure 2: Digital Sovereignty approach by region

Without holding Artificial Intelligence, the Internet of Things, blockchain or even quantum computing lightly, modern cyber diplomacy can hardly be envisioned without acknowledging the influence of these new technologies, each of which is transforming the way that states approach one another and protection in cyberspace. The fact that AI can serve as an instrument for enforcement: "At the same time, AI provides better capabilities to governments to detect and deter malicious actors; it also enables bad actors to make more sophisticated attacks, so it is more important than ever that there are consensual agreements on responsible use of AI in diplomacy. Cautiously optimistic, blockchain recognizes the ability to help safeguard global treaties and records, but with a word of warning: its security is very much in a vector suitable for AI attack. Most urgently, quantum computing, as a serious long-term threat to existing encryption systems, with the ability to break the existing security infrastructure making international consensus on norms a far underdiscussed one of the challenges in today's diplomatic agendas (Radanliev, 2025).

Digital Diplomacy as an answer.

These are the traditional diplomatic tools that must be adapted for use in Cyberspace.

Governments have started to refashion traditional diplomatic tools to deal with cyber challenges. Both sides' discussions, written protocols and the appointment of specific cyber security ambassadors underscore states' renewed attention to cyberspace as a theater for concerted diplomatic efforts.

European and international frameworks and norms on education and learning

The UN Group of Governmental Experts has been tasked with setting some initial principles of responsible state conduct online. The purpose of these is to minimise the risk of conflict and thus establish a common ground rule on appropriate/inaappropriate behaviour in cyberspace.

International Organizations

NATO has taken cyber defense on-board as part of its collective security obligations and considers cyber attacks of serious magnitude to meet the criteria that would trigger NATO's mutual defense commitments. The UN remains the main multi-lateral forum for discussing cyber governance, but action is slow due to conflicting national interests.

Cautious word of praise for blockchain. Radanliev believes AI can be used effectively to improve the transparency and verifiability of international accords, but also cautions against the potential new global threat from AI-based attacks on blockchain systems, which most policy makers have not paid enough attention to. Near future security risk capable to whack diplomatic communications, military networks and financial systems—quantum computing. A window is open and rapidly closing for the creation of international norms with regard to quantum security (Radanliev, 2025).

Ways to walk the talk, they say. Walls Have Eyes

Attribution Difficulties

The greatest hurdle in cyber diplomacy is just that of determining who perpetrated an attack. Sophistication and the ability to disguise one's identity, route

attacks to pass through third countries, and utilize civilian infrastructure, commonly allow sophisticated actors to make it difficult to definitively identify an attack and attribute it politically and technically. The international regulations might not be in place. International regulations may not exist. Conventional wars are bound by well-known international laws and cyberspace is not completely regulated at the International level. While there is no single clear legal definition of a cyber act of war, nor of proportionate legal responses, there are no universally agreed guidelines or codes of conduct.

Cyberspace Sovereignty issues

The concept of sovereignty online is very different in various states. Some want state regulation of national Internet and others want free-flowing, globally interconnected Internet. The conflicting visions have significant fissures and can make consensus building on cyber norms very challenging.

Opportunities for Cooperation

Confidence-Building Measures

Miscommunication and unintended escalation between governments can be minimised by various practical measures, such as creating direct contact hotlines and exchanging threat information and joint cyber drills.

Proposed Diplomatic Solutions

There are several scholars and policy makers who suggest that the treaties and accords of multilateral cyber law need to be strengthened, the international cyber courts need to be established, and international cyber organizations such as OSCE build their mandate to bridge cyber disputes. The inclusion of private technology companies in these dialogues is being seen as important as well as.

Future of Digital Diplomacy

In the future, digital diplomacy should be further institutionalized with the establishment of permanent diplomatic missions which will focus on digital theme. The existing diplomatic architecture will need to be continued and evolve, reflecting the changing nature of threat in the age of AI and quantum.

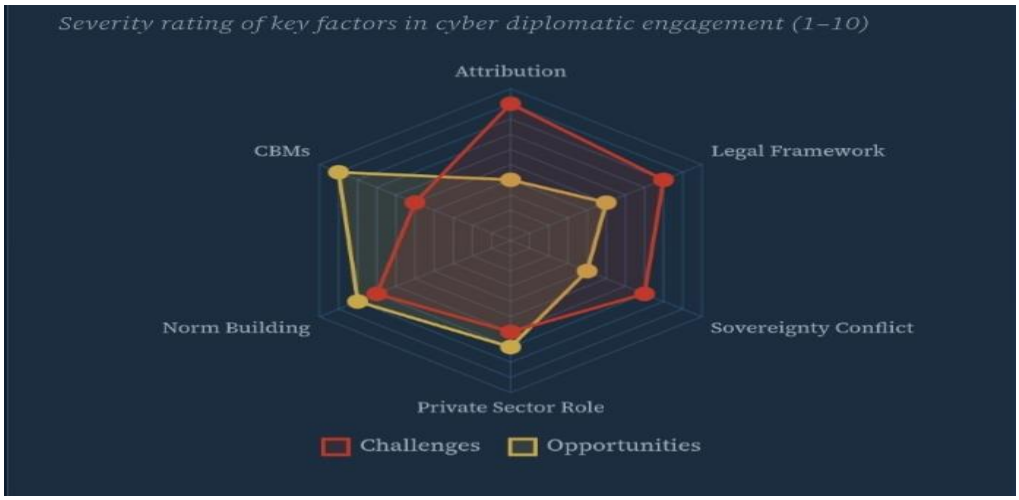

Figure 3: Cyber Diplomacy- Challenges vs Opportunities

Conclusion

In this study, the development trend of digital sovereignty, cyber warfare and cyber diplomacy in the field of international relations in today's world has been studied. The conclusions are clear: Cyberspace has become one of the most contested, and significant fields of national strategy, and states are increasingly using digital tools to exercise their influence and to safeguard their national interest, as well as to advance diplomacy, forge alliances and agree norms for responsible online engagement. Indeed, the global security environment is changing, bilaterals are becoming strained, international sanctions have been enforced and these major cyber incidents are now well-established political events with diplomatic repercussions as much as technical challenges.

It has also become evident in the study that digital sovereignty by now has shifted its original geopolitical meaning of technical governance and is now a substantive tool of foreign policy available to States to express their independence, transcend technological reliance on 'dominating actors' and boost their negotiating power in global international arenas. The growth of cyber diplomacy as a field of practice has been paralleled by the research's findings that cyber diplomacy is not yet well formed as an institutional infrastructure, legal frameworks or shared normative foundations. One of the issues that frustrates efforts to develop a stable and cooperative international internet order is the conflict between states which champion open and globally interwoven internet and those which want to have strict control over their digital infrastructure. Contrary to popular belief that technological defense is enough to safeguard against all forms of cyber threats, this study, in general, indicates that a technological approach alone is not sufficient and that diplomacy be at the core of any strategy worth considering to manage conflicts and achieve stability in the digital age.

International relations, diplomacy and war have forever changed and cannot be altered from their digital presence. It had started out as a means of communication and of commerce; now it is a theatre of ideas, interests and power in a war each State wages daily for influence, security, strategical advantages. The consequences are potentially far-reaching. Real physical harm to real people can be done through Cyber attacks to Critical Infrastructure. Disinformation can erode the 'context and trust' of the society and create a sense of disintegration in democracies. The consequences of state sponsored espionage can be years in coming and can have national security implications that are not immediately recognized and overcome. Under these conditions, digital sovereignty and cyber diplomacy are no luxury for a country but a condition and requirement for any one that seeks to ensure the security of its citizens, maintain countries' independence and actively participate in the development and maintenance of the international order.

All the scholars and policymakers whose work has been summarized in this study have created a rich body of knowledge and that knowledge must be given flesh to become real diplomatic action, institutions that are more powerful, and a global governance that is more representative. Effective international peace and security – and much of this hinges on technological and digital management challenges and opportunities – starts with the subject of cyber diplomacy, as a subject, a practice and a priority.

Recommendations

The results of this study offer some key recommendations to the national and international policy makers.

Governments must consider cyber diplomacy as not only a foreign policy issue, but also a primary and fundamental one. This will require setting up dedicated cyber diplomatic units in foreign ministries, designating cyber experts as ambassadorial positions, as well as investing in resources to enable continued participation in multilateral cyber governance fora. U.S., France and Estonia are just a few of the countries that have successfully implemented this approach to cyber diplomacy and have seen valuable outcomes in the form of Cyber alliances, shaping Cyber norms, and deterring hostile Cyber behavior.

Second, the international community also needs to do more and feel more willing to create a comprehensive and legally binding framework for state behavior in cyberspace. Current voluntary regulations created by the UN Group of Governmental Experts are a great starting point, but without any enforcement instruments and not agreed to by everyone. A greater clarity in the law, such as by clearly outlining what would constitute a "Cyber act of aggression" and providing rules for proportionate responses and state accountability for attacks conducted from its territory would be hugely helpful in mitigating this ambiguity which bad actors have exploited so far.

Third, it is necessary to include the attribution problem at the strategic agenda of the policymakers. Given the lack of the ability to reliably and publicly point to state or non-state entities for the purpose of deterrence and accountability, the fight against cyberattacks is less than successful. Governments should make significant investments in technical attribution and implement common international guidelines for transparent and credible technical attribution verification and communication.

Fourth, efforts should be made to help developing and smaller states to strengthen their cyber diplomatic skills. Currently, cyber diplomacy is governed not just by a few giant states with sufficient technical capabilities and institutional resources that are able to play a meaningful role in international negotiations but also by a significantly larger group of so-called "exceptional" states. Not only are there a few giant states that have the technical capabilities and institutional resources to play a meaningful role in negotiations, but there are also a much higher number of so-called "exceptional" states that are engaged in cyber diplomacy in some capacity. This imbalance poses the threat of a world order in cyberspace that is propped up by the powerful at the expense of the weaker. Inclusive multilateral settings, capacity building initiatives and technology transfer best practices are crucial for creating an actual international cyber governance system that provides all states a real voice.

The private sector's function is to be formally engaged and formalised within cyber diplomatic mechanisms - fifth. Major technology firms own and manage critical digital infrastructure, create software/hardware states rely on and have intelligence on cyber threats from which governments are frequently blindsided. They cannot be excluded from diplomatic processes without being counter-productive, that's so impractical. Governments should find appropriate ways to cooperate with the private sector in cyber security and (cyber) diplomacy and have clear regulations on the balancing between public and national security considerations and private interests.

Sixth, there should be further institutionalisation and expansion of agreed steps towards the construction of trust between states. Establishing direct communication hotlines between cyber authorities or regular bilateral and multilateral cyber dialogue sessions and organizing joint incident response exercises can greatly reduce the risk of miscalculation and accidental escalation. These measures are especially vital between major powers with cyber competition that has the greatest potential for serious conflict.

Suggestions for future research

For the purposes of this study, contextual analyses of the trajectory of digital sovereignty and cyber diplomacy have been enlarged, but some aspects of the issues have not yet received sufficient attention and warrant further exploration in subsequent research. The rapid pace of advancements in AI is transforming the nature of cyber threats and prompting a need for developing new diplomatic mechanisms and tools that can operate with AI technology in the cyber domain. Cybersecurity is another new front where quantum computing can play an important role that will impact encryption, intelligence gathering and the evolving power dynamics in the cyber world between states. Finally, the lessons learned from future studies should integrate the unique experiences of developing Nations, as they are underrepresented in current cyber diplomacy literature and are more likely to focus on big powers' cyber diplomacy.

The study of the effectiveness of the current confidence-building measures as well as cyber norms would be helpful in determining whether diplomatic move was successful in mitigating the occurrence and intensity of cyber conflict or merely superficial ones with no real currency when it comes to addressing cyber threats. Lastly, scholars will be able to benefit from seeing greater attention paid to the role played by non-state actors—such as civil society groups, hacktivists and tech companies—in setting the direction of cyber diplomacy, as these actors have an increasing presence in the digital landscape, one that some standard diplomatic structures are not yet prepared to address.

References

Aldrich, R. J., & Karatzogianni, A. (2025). Cyber power and cyber diplomacy. *In The Palgrave handbook on cyber diplomacy(pp. 53–75).* Palgrave Macmillan.

Alethawy, M. (2022). Digital diplomacy and cybersecurity. *Ahi Evran Akademi, 3(1),* 82–90.

Barrinha, A., & Renard, T. (2018). Cyber-diplomacy: The making of an international society in the digital age. *Global Affairs,* 3(4–5), 353–364.

Buchkovska, K. (2025). Cyber diplomacy: Securing the (digital) future. *Journal of Law and Politics, 6(1),* 97–108.

Bukhari, S. R. H., & Siddiqui, Z. (2026). Digital sovereignty: A diplomatic tool in modern cyber warfare. *ACADEMIA International Journal for Social Sciences, 5(3s4),* 17.

Hallams, E. (2010). Digital diplomacy: The internet, the battle for ideas and US foreign policy. *CEU Political Science Journal, 5(4),* 538–574.

Kasper, A., Osula, A.-M., & Molnár, A. (2021). EU cybersecurity and cyber diplomacy. *IDP: Revista de Internet, Derecho y Política,* (34).

Radanliev, P. (2025). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology, 9(1),* 28–78.

Rehman, H. U. (2025). Pakistan and the new frontier of cyber diplomacy. *BTTN Journal*, 4(1).

Tiirmaa Klaar, H. (2025). Seeking balance between cyber diplomacy and cyber warfare. *In The Palgrave handbook on cyber diplomacy (pp. 231–251).* Palgrave Macmillan.