ACADEMIA International Journal for Social Sciences
Volume 5, Issue 3(s4), 2026 ISSN-L (Online): 3006-6638

Digital Sovereignty: A Diplomatic Tool in Modern Cyber Warfare

Dr. Syed Rizwan Haider Bukhari
bukharipalmist@gmail.com
PhD Political Science (Strategic Studies), Islamia College University Peshawar (Estb-1933), Khyber Pakhtunkhwa, Pakistan.

Zainab Siddiqui
Zainab.remotework@gmail.com
MA International relations, University of Hertfordshire

Corresponding Author: Dr. Syed Rizwan Haider Bukhari bukharipalmist@gmail.com

Received: 18-01-2026 **Revised:** 03-02-2026 **Accepted:** 17-02-2026 **Published:** 02-03-2026

ABSTRACT

This paper explores the notion of digital sovereignty, which highlights the national ownership of the digital resources within a country, such as the infrastructure, data, and technologies in a more or less interconnected world. Digital sovereignty as a vital part of national security is especially essential to democratic countries, where these fundamental principles as privacy and freedom of expression are preserved along with tackling security issues. Through qualitative and quantitative research, the paper examines the convergence of digital sovereignty, the internet and communication. It emphasizes the fact that cyber warfare makes it difficult to distinguish between physical and virtual conflicts, which is why the diplomatic frameworks have to evolve, as well. The paper identifies both the traditional and cyber conflicts with the lack of vivid rules and values, which makes governance more difficult. As cyber tools become a more important political tool in diplomacy, the paper explores issues of accountability, digital privacy protection, and international regulation with references to such models as the GDPR by the EU and the cyber sovereignty framework developed by China.

Keywords: *Digital Sovereignty, Cyber Warfare, National Security, Cyber Diplomacy, Digital Privacy, GDPR, Cyber Sovereignty.*

INTRODUCTION

The state power in the 21 st century is not only limited to the historical frontiers of land and territory but also expands to the grandiose, globalized, and interconnected world of the internet. This development ushers in the notion of the digital sovereignty, which can be defined as the capacity of a country to regulate its digital infrastructures, information and technologies, as it claims its independence in an ever-more interconnected world. Digital sovereignty is a small pillar of national security especially to democratic states which have to deal with the nuances of cyber warfare. The digital tools have become part of the welfare of citizens and operation of contemporary states. The argument of the chapter is that the concept of digital sovereignty now is no longer a defensive policy; it has become an effective instrument of diplomacy, allowing governments to defend their values, to safeguard their interests, and to determine the terms under which people and states engage in a highly disputed digital space (Pohle and Thiel, 2020).

To democratic states, digital sovereignty is beyond technical dominance. It helps to protect the fundamental democratic principles like free speech and privacy as well as mitigating security issues. Certain States cannot afford to use invasive surveillance or control practices that break values supported by the democratic states as opposed to authoritarian regimes. This balancing act needs detailed legal provisions, investment

in national technological capacities and enhancing the public-private collaborations to increase cyber resilience. Here, the idea of digital sovereignty proposes itself as the weapon of democratic resilience to prevent the foreign powers to have access to digital infrastructures and flows of information in order to disrupt politics or lose the trust of the people (Kaloudis, 2024).

International relations and cyber warfare are the most crucial areas of the implementation of digital sovereignty as a diplomatic instrument. Cyber threats can break the established norms because the traditional Westphalian model of state sovereignty is under scrutiny, as it transfers inter-nationally. Digital sovereignty permits states to establish dominance, which portrays their power in cyberspace. Strong cyber protection can help democratic states build strong defenses, as well as set out clear rules of conduct in the online world. This may be done diplomatically by international collaboration and multilateral agreements, or using economic and technological strength. Nevertheless, the search of digital sovereignty may equally jeopardize the openness and the transnational character of the internet because nationalistic resources may divide the global digital realm. This national interest and international cooperation tension is the core of the development of policies on cyber warfare (Akhtar and Iqbal, 2025).

Finally, the examination of digital sovereignty as a tool of diplomacy is a dynamic and changing one. It crosscuts with a variety of fields, such as science, politics, economics, and international law. These thorny questions will be examined in the chapter, and how democratic countries leverage digital sovereignty to safeguard against online threats, influence world digital governance and impose their values and control throughout the digital era. It will examine the tactics, obstacles, and implications of this new version of diplomacy, providing a full picture on how digital sovereignty plays out in the modern day cyber warfare (Timmers, 2022).

LITERATURE REVIEW

The emergence of digital technologies has radically changed the scenery of the diplomacy process and broadened the traditional concept of statecraft to a complex network of digital relationships. An excellent example of this change is the concept of cyberwarfare, i.e. the application of digital weapons, e.g. hacking and software attacks to impair or damage the digital infrastructure of another country. In contrast to the old type of warfare, cyberwarfare presents the complexities of hack backs, with counter, retaliatory cyberattacks, being carried out against counterattacks. This type of war is very difficult to discriminate with traditional military battles, and diplomacy is challenged to find new instruments and methods to solve the conflict in the digital world (Arnold, 2011).

The integration of the concept of cyber threats and war manifests in the traditional form has brought about the necessity of highly specific defense approaches and diplomacy to face the unique characteristics of the cyber conflict. As a counter measure to these new threats, various NATO nations have established dedicated defense units or 'dimensions' dedicated to cyber defense. These dimensions coexist with conventional military categories, including the air force, navy, and army, which is determined by the fact that cyber defense should be included in national security structures (Blessing, 2021; Bukhari et al., 2024).

The introduction of cyber defense as a separate field of national defense is a significant shift in the manner in which states view their security policies. The fact that cyber threats are only getting more advanced and more common implies that the scope of diplomacy will have to increase to cover these online sectors as well. The necessity of effective cyber diplomacy is supported by the fact that digital infrastructure is growing into an interdependent phenomenon across borders which introduces a new dimension of international relations with the activity in cyberspace potentially having significant geopolitical effects (Sarmad et al., 2018; Bukhari, 2025). Diplomacy is a very critical tool in the management of relationship

among states, and its origin can be traced to the period in the 14 th century BC in Egypt, as well as the Middle East. However, it was in the Italian city states of the 1300s that modern diplomacy as we recognize it today started to form its identity as formalized relations of states arose (Shah et al., 2025). This developmental history helps to outline the way in which diplomacy has evolved into not just a single task of communication, but also a complicated network of relations, involving not only two-way communication at bilateral level, but also member states multilateral interaction apparatuses such as the United Nations (UN). In the modern globalized society, diplomacy is a multifaceted interaction of procedures of formal treaties and negotiations with the informal exchange of the cultures which assist to create the world politics and provide the world with the peace and safety. Contemporary diplomacy works on a global platform where questions of war, commerce, human rights and computer governance are being tackled more and more (Hall, 2006).

With the growing penetration of digital technologies in international relations, the idea of cyber diplomacy has taken centre-stage in influencing global governance. Cyber diplomacy refers to the efforts by developing international regulations and standards of the cyber space, data privacy and protecting democratic values in cyberspace (Kausar et al., 2022). The Western-oriented countries have been particularly prolific in popularizing cyber diplomacy as they see it as a very critical instrument in promoting international cooperation regarding cybersecurity, digital rights, and data protection. The increased number of states that now appoint cyber policy envoys to over 30 countries is a proof of the broader understanding of the necessity to embrace the inclusion of cyberspace in the foreign policies. Cyber diplomacy is also progressively regarded as an alternative to solving international conflicts and promoting peace through the development of norms of conduct in cyberspace (Lancelot, 2020; Khan et al., 2020; Noor et al., 2024). These actions demonstrate the potential of cyber diplomacy to affect the global politics, and Diplomatic activity can determine the digital realm and ensure that cyber conflicts do not enter the realms of full-fledged geopolitical crises.

The importance of cyber diplomacy was further acknowledged when the UN General Assembly supported a report by the Group of Governmental Experts (GGE) in 2015 indicating that the international law should be applied to cyber operations. The report confirmed that self-defense, which is a fundamental principle of international law, must apply to cyberattacks. This progress was a pivotal move towards institutionalizing cyber diplomacy as an element of the global system of governance, which supports the notion that the actions of states in cyberspace should be dictated by the same set of laws as the traditional warfare (Hsu et al., 2025). Nevertheless, in spite of such achievements, there are still certain difficulties in operating diplomatic approaches to deal with cyber threats. The dynamic nature of technological innovations in cyberspace makes it difficult to develop any clear principles of state conduct, which causes misunderstandings and possible disputes in the digital environment (Bendiek, 2018; Khan et al., 2021).

This conflict of national interest vis-a-vis international collaboration in cyberspace remains a major challenge to cyber diplomacy. The issues of digital sovereignty and cyber diplomatic have significant implications to the process of state navigation through the global digital environment. Digital sovereignty means that a country is able to stretch its power to govern digital infrastructure, data, and technology, within the country, making the claim of its autonomy in the globalized world. This idea becomes even more applicable to democratic states, as they have to find a balance between the necessity to ensure cybersecurity and the safeguard of democratic principles, including freedom of speech and privacy. In this regard, digital sovereignty is itself a major component of the notion of democratic resilience, allowing governments to protect against foreign intervention in their digital ecosystems and make sure that digital platforms reflect the values of their nation (Kaloudis, 2024; Bukhari et al., 2025). Nevertheless, as governments are working to establish their own digital sovereignty, they should also address the issue of division of the online world.

Policies of nationalism online may erode the concept of a free and open internet, exploring new divisions within the sphere of the internet that may further increase tensions in the world.

Digital sovereignty has also made the expanding influence of digital governance in the global politics visible. In an effort by governments to safeguard their citizens and digital systems against cyber threats, governments have to balance issues of security and the opportunities that emerge with new digital technologies (Naeem et al., 2024). The digital space gives more opportunities to both innovation and economic development than ever before, and it also brings with it the emerging dangers of cybercrime, cyberattacks, and the use of digital platforms to gain political prices. In the ever changing digital world, states need to devise a strategy that can resolve these conflicting priorities without role reversal; states need to be guaranteed their independence and safety in the cyberspace. That digital sovereignty and cyber diplomacy have become vital parts of the contemporary statecraft highlights the necessity to have an international response to the risks and opportunities of cyberspace (Manantan, 2021; Sarmad et al., 2020).

The growing integration of states with the assistance of digital technologies demands the emergence of new models of diplomacy and statehood in order to deal with the intricate issues of cyber threats. Cyber diplomacy and digital sovereignty have become some of the most crucial instruments of the modern state in working through the changing digital environment. Diplomacy is forced to evolve alongside new conditions of international relations in the context where cyberwarfare has become a part of international relations. The ability of the states to optimize the digital sovereignty and the necessity of international cooperation will be the parameters according to which the future of global governance will be determined so that cyberspace could be safe, open, and corresponding to the values of democracy.

METHODOLOGY

This study looks at how intertwined diplomacy is with the internet, the concepts of digital sovereignty and digitization as it applies to world problems. The research uses qualitative and quantitative approaches, with the focus being on cyber resilience and digital sovereignty as the new instruments in diplomatic communication. The study will use linear regression and index comparisons of state scores to determine possible relationships and cause and effect links. Statistical relationship among variables are investigated using advanced statistical methods such as Spearman and Pearson correlations. Also, the research examines the historical development of digital sovereignty in diplomacy, which illuminates the way diplomatic instruments responded to the digital revolution. Through examination of these developments, the study provides a further insight into the changing role of the digital sovereignty and its implication on the contemporary diplomatic practices.

RESULTS/FINDINGS

The results of this paper outline some important interconnected matters and tendencies that define the increasing significance of digital sovereignty and cyber resilience in contemporary diplomature. We have found that there is a significant positive relationship between the digital sovereignty scores and the perceived effectiveness of countries in their diplomacy and this occurs particularly in matters of cyber-related negotiations, through the linear regression analysis. States that score higher in terms of digital sovereignty have a higher level of cyber resilience, implying that being able to control digital infrastructure can enable a country to react to cyber threats and establish its authority in international relations.

The investigation based on Spearman and Pearson correlation analysis also indicated that countries that invest in strong cyber defense systems have a higher chance of participating in multilateral cyber diplomacy, as observed in the increase of cyber policy envoys and the signing of international cybersecurity

treaties. This confirms the hypothesis that those nations that utilize digital instruments in foreign policymaking are better placed to dominate or even to engage in digital debates on global governance.

Moreover, the historical review revealed that there was a significant change in the status of digital sovereignty in the inter-state structures. Although in its early stages, digital diplomacy focused mainly on the issue of data protection and privacy, it has now come to encompass elements of strategic geopolitics, such as the ability to control key central information and safeguard the national interests in cyberspace. Also revealed in the study is that with digital sovereignty emerging to take centre point, diplomacy initiatives are shifting towards building global norms and accords to address the issue of cyber conflict and regulation. On the whole, the findings highlight the disruptive effect of digital sovereignty on the diplomatic practices, showing both the difficulties and opportunities in finding the way in the ever-changing political realm of the digital age.

DISCUSSION

Digitalization is broadening the usual understanding of diplomacy, and as it is no longer a face-to-face negotiation, but a more multifaceted system that also involves cyber technology like hacking, and software attacks. Such devices, which are frequently utilized in cyberwarfare, make international relations and negotiations complicated. The issue of hack backs as a retaliatory action also complicates diplomacy because it becomes more difficult to control the notion between cyber and standard warfare. Due to the growing numbers of cyber threats, new diplomatic measures are required. Even in most NATO countries, there are formed specially-focused defense units, or dimension, that specifically handle cybersecurity attacks, on top of the conventional armed forces, on the basis of an understanding that coordinated defense systems are required within this digital era (Arnold, 2011; Blessing, 2021). Such a displacement of classical diplomacy whose repercussions centered on direct contact and treaty togetherness now encompasses multilateral dialogues regarding online forms of governance like the UN (Hall, 2006; Lancelot, 2020).

The western nations, especially have started to exercise cyber diplomacy in order to control cyber space, data privacy and spread democratic ideals, which are good signs of the rising relevance of cyber diplomacy in international politics. Having more than 30 nations with cyber policy envoys is a sign that the industry is increasingly becoming significant due to its ability to address international conflicts and achieve peace. The adoption of the application of the international law to cyberspace by the UN general assembly indicates the increasing need to have a standardized method of managing cyber conflicts (Bendiek, 2018). Nonetheless, with the rapid development of technology, it is rather difficult to define digital and physical space, and new international standards are needed (Manantan, 2021). Digital governance has to introduce a delicate equilibrium between national interests and the threat of disintegration in the global online arena.

This is a great difference between cyberwarfare and traditional warfare. Whereas a traditional war is fought in the physical world using physical objects, cyberwar is fought in the cyber realm, and this raises the concept of territorial boundaries and power. The physical world has rules that regulate the powers of the state through the peace of Westphalia in 1648 and there are no such rules in the cyberspace. This means that cyber attacks can even result in conventional conflicts, yet there are no established norms on the same, thus making conflict a possibility. Moreover, the role of cyber tools in shaping opinion of the people by manipulating social media represents another challenge to the practice of traditional diplomacy as technology becomes more and more significant in the perception of the people and the foreign policy (Barlow, 1996; Hannas and Tatlow, 2020).

Cyberpower, especially the forging of cyber defense capabilities is becoming a diplomatic instrument that adds to the negotiating strength of a state. A similar usage of the military strength in conventional diplomacy

to prevent aggression is also applied, nowadays, to preserve the digital sovereignty and control international relations with the help of cyber capabilities. Although cyber defense is a crucial step of national security, it strengthens the bargaining power of a given state. Nevertheless, in contrast to traditional weapons, the volume of the cyber defense that is required to establish digital sovereignty is unknown, and the future of expeditionary digital weapons is ambiguous (Kristensen and Norris, 2013; Barrinha, 2018). It is still unclear whether in the long term, the concept of digital sovereignty will persist in informing the search of diplomatic tools because governments want to balance between technological independence and the necessity of finding solutions internationally.

The boundaries of conventional diplomacy are increasingly visible in the area of cyber war as cyberattacks tend to be invisible and hard to apprehend. Consequently, states are considering the way they deal with cyberattacks in the context of international law. Proportionality the understanding that military action must be calculated and reasonable turns out to be more and more challenging to implement in cyberspace, which is less noticeable and difficult to measure. Such legal frameworks as the mutually defense obligation of NATO and the rules proposed by the U.S. Department of Defense on cyberattacks constitute important steps toward implementing cyber conflicts under the global government organizations (Kukkola, Ristolainen, and Nikkarila, 2019). A bilateral agreement, including the Russia-China 2016 partnership on IT and communications also emphasizes the increase in the connectivity between cyber diplomacy and national security issues (Creemers, 2020).

The resilience to cyberattacks has emerged as a fundamental part of digital sovereignty, known as cyber resilience, which sought to protect, identify, react, and recuperate the losses of cyberattacks. Those countries resistant to cyber attacks have a higher chance of countering cyber attacks and retaining authority over their critical networks. Global Cybersecurity Index (GCI) and Bugata National Cybersecurity Index (NCSI) measures the preparedness of countries to counter cyber threats. The high NCSI indicators in countries such as Estonia indicate that developing strong cyber defense measures is important (Kravets, 2019). At the same time, both China and the EU have greatly invested in the development of their digital sovereignties and cybersecurity systems and consider cyber defense as a part of a national security system and economic stability (Balbaa, Eshov, and Ismailova, 2022; Dawda, Janjeva, and Moiseienko, 2021; Holtmann, 2018).

Digital sovereignty is gaining significant relevance in practice as states attempt to gain control over their e-infrastructure. EU General Data Protection Regulation (GDPR) and other initiatives such as European Chips Act put in place are meant to minimize the use of external digital services and technologies so that the privacy of data and the interest of the nations can be safeguarded. Quite on the contrary, such nations as China or Russia have adapted a more state-centered viewpoint, developing national substitutes in favor of foreign technology and holding draconian data localization control to ensure ownership over their digital landscapes (Tan, Chi, & Lam, 2023; Adler-Nissen and Eggeling, 2024). Nevertheless, this version of digital sovereignty poses a risk of generating a divided online world, in which countries with different interests and policies fight over who has the right to dominate the cyberspace (Timmers, 2024).

Cyber resiliency and digital sovereignty are complementary to each other. Cyber resilience would help states insure their digital infrastructure and recover cyber attacks, whereas digital sovereignty would guarantee states the ability to manage their digital ecosystems on their own. Both play an important role in modern diplomacy, as they assist states in claiming their independence, protecting their interests, and participating in international cybersecurity. Cyber capabilities and sound policy on defense contribute to the diplomatic advantage of a nation; thus, digital sovereignty and cyber resilience could be well-known business strategies in the digital era (Pohle and Thiel, 2021; Krings, 2016).

CONCLUSION

Using digital sovereignty and cyber resilience in the realm of the modern diplomacy is no longer an option, since states are challenged by the multifaceted and quickly mass-changing environment of the digital era. Focused on its potential to blur the distinctions between the traditional military conflict and the digital attacks, cyberwarfare poses a new challenge to international relations. With digital tools becoming more and more influential in geopolitics, the necessity of proper cyber diplomacy is becoming more apparent. States have become concerned with protecting their cyber bases, establish power over cyber space, and employ their cyber methods as foreign policies to defend their interests as well as improve national security. Nevertheless, the insufficiency of international standards on cyberspace and a future of fragmentation through digital divide are very dangerous to international co-operation and stability. Digital sovereignty and cyber resiliency have become key terms in supporting national and international security in the interconnected world, in this context. The changing paradigms of these concepts highlight the necessity to devise new diplomatic models that will capture the interplay of digital forces and classical statecrafts.

RECOMMENDATIONS

- **Formulate Global Cyber Standards:** It is high time that there is a set of international standards and agreements the activity of which is controlled in relation to cyberspace. Cyberwarfare must just as the traditional warfare fall under international law. International institutions, such as the UN might be instrumental in achieving such agreements, in order to achieve uniformity and equity in terms through which states interact in cyberspace.

- **Foster Multilateral Cyber Cooperation:** Multilateral cooperation in cyber diplomacy should be prioritized by countries in order to gain trust and improve collective cyber defense capabilities. This may include creating official avenues of discussion about cyber threats and exchange of best practices on cyber resilience. Free initiatives such as Global Forum on Cyber Expertise (GFCE) can be expanded to enable transnational cooperation in cybersecurity.

- **Invest in Cyber Education and Talent Development:** To build national cyberspace resiliency, the country needs a skilled workforce to handle and protect against cyberspace attack. To develop the talent, governments are supposed to invest in education programs, research, and partnerships between the government and the private sector. The development of workforce should also be a priority of the countries in their national strategies in cybersecurity.

- **Invest in Digital Soverignty:** Countries with strategic investments in digital sovereignty would benefit in capitalizing on and securing their own digital infrastructure including sovereign cloud and sovereign data centers. It minimizes the use of foreign technologies, improving the economy and national security. Examples of initiatives that can be used as models include the European Chips Act and the GDPR developed by the European Union to promote digital autonomy in the region, among others.

- **Increase the Value of cyber resilience to national security:** Cyber resilience must be a key part of national security strategies. This is not just about enhancing cybersecurity infrastructures, but also creating a system of recovering fast in response to cyberattacks. The capacity of states to detect, respond, and recover if there were cyber occurrences should be a number one priority in policies aimed at ensuring digital ecosystem are resilient and safe.

- **Enhance Social Media Awareness and Digital Literacy:** To reduce the threats of cyber manipulation and misinformation, it is important to enhance social media awareness and digital literacy. Governments ought to organize awareness programs on how people can identify threats over the internet such as fake news, phishing, and malware and how to use the digital platforms. This is particularly relevant in the prevention of the use of social media in shaping the opinion of the masses in cyber-warfare.

Following these recommendations, the states will be capable of negotiating the intricacies of digital sovereignty and cyber diplomacy to a greater degree and ensure that the promotion of national interests will be more successful and that a more secure and collaborative international digital setting is established.

REFERENCES

Adler-Nissen, R., & Eggeling, K. A. (2024). The discursive struggle for digital sovereignty: Security, economy, rights and the cloud project Gaia-X. *JCMS: Journal of Common Market Studies, 62*(4), 993-1011.

Akhtar, N., & Iqbal, A. R. (2025). Cyber Sovereignty: National Security in the Digital Age. *Lahore Institute for Research and Analysis Journal, 3*, 87-104.

Arnold, H. (2011). Frieden und Diplomatie. In *Handbuch Frieden* (pp. 294-309): Springer.

Balbaa, M. E., Eshov, M. P., & Ismailova, N. (2022). *The Impacts of Russian Ukrainian War on the Global Economy in the frame of digital banking networks and cyber attacks.* Paper presented at the Proceedings of the 6th international conference on future networks & distributed systems.

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace. *Electronic Frontier Foundation.*

Barrinha, A. (2018). Virtual neighbors: Russia and the EU in cyberspace. *Insight Turkey, 20*(3), 29-42.

Bendiek, A. (2018). The EU as a force for peace in international cyber diplomacy.

Blessing, J. (2021). *The global spread of cyber forces, 2000–2018.* Paper presented at the 2021 13th International Conference on Cyber Conflict (CyCon).

Bukhari, S. R. H. (2025). Assessing the Ukraine-Russia Conflict: A Threat to Global Energy Security and the Prospect of a Third World War. International Journal of Advanced Research (IJAR).

Bukhari, S. R. H., Haq, I. U., Ali, M., & Irshad, A. B. (2025). Navigating academic and cultural adaptations: Experiences of Pakistani students studying in China during and after COVID-19. Journal of Social Sciences Review, 5(1), 13.

Bukhari, S. R. H., Khan, A. U., & Haq, I. U. (2024). Identity politics and regional dynamics: The OIC as a nexus of Muslim unity and diversity. Pakistan Social Sciences Review, 8(1), 208-215.

Bukhari, S. R. H., Khan, A. U., Noreen, S., Bashir, F., Rafi, G., & Haq, I. U. (2024). Navigating sovereignty: Legal and geopolitical implications of territorial disputes in South China Sea. Remittances Review, 9 (1), 1066-1082.

Bukhari, S. R. H., Khan, A. U., Noreen, S., Khan, M. T. U., Khan, M. N., & Haq, M. I. U. (2024). Echoes of Change: Navigating Political Turmoil in the Aftermath of the Arab Spring. Kurdish Studies, 12 (2), 6603-6631.

Bukhari, S. R. H., Khan, E., & Haider, M. M. (2025). Education and Power in Pakistan: Comparative Analysis of Public, Private, and Madrasa Systems and Their Role in Shaping Political Awareness and Democratic Governance. Qlantic Journal of Social Sciences, 6(1), 420-432.

Creemers, R. (2020). China's conception of cyber sovereignty. *Governing cyberspace: Behavior, power and diplomacy*, 107-145.

Dawda, S., Janjeva, A., & Moiseienko, A. (2021). The UK's Response to Cyber Fraud: A Strategic Vision.

Hall, I. (2006). Systems of states. In *The International Thought of Martin Wight* (pp. 87-110): Springer.

Hannas, W. C., & Tatlow, D. K. (2020). *China's Quest for Foreign Technology: Beyond Espionage*: Routledge.

Hjorthen, F. D., & Pattison, J. (2023). Proportionality in cyberwar and just war theory. *Ethics & Global Politics, 16*(1), 1-24.

Holtmann, D. (2018). Die Performanz von Politik, Wirtschaft und Gesellschaft für 43 Länder und 6 Wohlfahrtsregime.

Hsu, W. K., Huang, S. H., Le, T. N. N., Huynh, N. T., & Wang, D. J. (2025). Assessing container terminals' efficiency from the sustainable development perspective: The BWM-GRA-SBM model. Transport Policy, 162, 443-455.

Kaloudis, M. (2022). From Quality to Quantity: How Can Digital Sovereignty be Parsed into Measurable Components? *European Journal of Business Science and Technology, 2022*(2), 172-189.

Kaloudis, M. (2024). Digital Sovereignty as a Weapon of Diplomacy in Cyber Warfare in. *National Security in the Digital and Information Age, 17*.

Kausar, R., Rashid, A., & Saddique, M. (2022). Covid-19 Uncertainty Impact on Exchange Rate: The Case of Pakistan. Journal of Development and Social Sciences, 3(4), 339-344.

Khan, M., Sarmad, M., Shah, S. F. A., & Han, B. J. (2020). Extent of employee turnover in humanitarian logistics: an interpretive structural modelling approach. Int. J Supply Chain Manag, 9, 107.

Khan, K. N., Sarmad, M., Ahmad, S. I., & Ahmad, I. (2021). Exploring Mediating And Moderating Mechanism For Project Uncertainty Under Agile Methodology Use In It Sector. Ilkogretim Online, 20(1).

Kravets, V. (2019). Comparative analysis of the cybersecurity indices and their applications. *Theoretical and Applied Cybersecurity, 1*(1).

Krings, G. (2016). Digitale Souveränität. In *Digitale Souveränität: Vertrauen in der Netzwerkgesellschaft* (pp. 351-356): Springer.

Kristensen, H. M., & Norris, R. S. (2013). Global nuclear weapons inventories, 1945–2013. *Bulletin of the Atomic Scientists*, *69*(5), 75-81.

Kukkola, J., Ristolainen, M., & Nikkarila, J. (2019). Game Player. Facing the structural transformation of cyberspace. *Riihimäki, Finnish Defence Research Agency*.

Lancelot, J. F. (2020). Cyber-diplomacy: cyberwarfare and the rules of engagement. *Journal of Cyber Security Technology*, *4*(4), 240-254.

Manantan, M. B. F. (2021). Advancing cyber diplomacy in the Asia Pacific: Japan and Australia. *Australian Journal of International Affairs*, *75*(4), 432-459.

Naeem, M., Zaheer, A., & Khan, M. L. (2024). Emotional Intelligence, Gratitude and Forgiveness among University Students. Pakistan Journal of Positive Psychology, 1(1), 8-14.

Noor, N., Rehman, S., Ahmed, Y., Rizwan, S., & Sarmad, M. (2024). Why do nurses leave their jobs? Understanding person-related hostility in the healthcare sector of Pakistan. Plos one, 19(6), e0298581.

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Pohle, J. & Thiel*.

Pohle, J., & Thiel, T. (2021). Digitale Souveränität-Von der Karriere eines einenden und doch problematischen Konzepts. In *Der Wert der Digitalisierung: Gemeinwohl in der digitalen Welt* (pp. 319-340): Bielefeld: transcript Verlag.

Sarmad, M., Ahmad, N., Khan, M., Irfan, M., & Atta, H. (2020). Investigating the moderating role of trust between social media capabilities and consumer brand engagement across textile sector of Pakistan. International Review of Management and Marketing, 10(4), 53.

Sarmad, M., Iqbal, R., Ali, M. A., & ul Haq, A. (2018). Unlocking spirituality at workplace through islamic work ethics: Analyzing employees' performance in islamic banks. Journal of Islamic Business and Management, 8(2).

Shah, S. M. A., Qazi, A. H., & Khan, A. R. (2025). Exploring Synergies: Hr, Finance, And Sustainable Supply Chains. Qualitative Research Review Letter, 3(1), 218-254.

Tan, K. L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on digital sovereignty and identity: from digitization to digitalization. *ACM Computing Surveys*, *56*(3), 1-36.

Timmers, P. (2022). Cybersecurity and Resilience from a Strategic Autonomy Perspective. *Decoding EU Digital Strategic Autonomy*, *137*.

Timmers, P. (2024). Sovereignty in the digital age. *Introduction to digital humanism*, 571-592.

Zimmer, M. (2008). *Moderne, staat und internationale politik*: Springer.