Indus Journal of Social Sciences
Online ISSN: 2960-219X
Print ISSN: 2960-2203
Volume 3, Number 4, 2025, Pages 397 – 407
Journal Home Page
https://induspublishers.com/IJSS/about

Sovereignty and Cyber Security: Re-Thinking State Power in the 21st Century

Nawazish Ali[1], Afzaal Ahmad[2] & Iqra Zafar[3]

[1]*Student of Department of Political Science, University of Sargodha, Sargodha, Email: nawazishalimarth@gmail.com*
[2]*Visiting Lecturer, University of Sargodha, Sargodha, Email: afzaal786ahmad55@gmail.com*
[3]*Visiting Lecturer, University of Sargodha, Sargodha, Email: Usmaniqra644@gmail.com*

ARTICLE INFO

Article History:

Received:	*September*	*07, 2025*
Revised:	*October*	*05, 2025*
Accepted:	*October*	*13, 2025*
Available Online:	*November*	*02, 2025*

Keywords:

Sovereignty, cyberspace, cyber security, state power, digital sovereignty, cyber threats

Corresponding Author:
Nawazish Ali
Email:
nawazishalimarth@gmail.com

ABSTRACT

The relationship between cyber security and state sovereignty has become a very important aspect of international politics in the 21 st century. The borderlessness of cyberspace is slowly eroding traditional ideas of territorial control and political authority as threats like these can now be made through cyberspace. Because cyber-attacks, web-based spying, and manipulation of information are beyond national borders. This paper discusses how states are re-examining the exercise of power in the digital age and balancing the requirements of the security, rule and civil liberties. It examines the changing paradigms of cyber sovereignty, how cyber capabilities can be strategically used in offence and defence and impact international law and diplomacy. The paper argues that cybersecurity is not simply a technical concern, but a central element of state power that requires innovative policy approaches and multilateral cooperation to safeguard national interests in an increasingly interconnected world.

Introduction

The 21st century is a new form of power to the countries in cyberspace. Cyberspace is digital networks without natural boundaries unlike land, sea, and air. It is not only risky but also provides opportunities. Governments are using digital technology to operate the state, communicate with the population, and manage money but remain vulnerable to cyber-attacks, which may be disseminated across borders in a short time. According to Topor (2024), the sovereignty of a country today has to encompass the right of managing and securing its digital territory and its physical frontiers.

The antique concept of Westphalia sovereignty is being doubted. The notion that a state owns all things within its boundaries is no longer applicable in cyberspace. Hackers, cybercriminals or even foreign governments can launch attacks at a very distant distance of location without necessarily

leaving a finger print. These attribution problems undermine the capacity of the states to adopt normal diplomatic or military means in response (Rid, 2013). Even the loss of a war can be very tragic to a small nation, like it was demonstrated in the 2007 Estonian cyberattacks (Deibert, 2013). These incidents pose critical issues on the way in which a nation retains its sovereignty.

The cyberspace is owned and controlled by a number of private firms, further complicating the situation. Governments are frequently outcompeted by cloud solutions, software developers, and internet service providers as the ones with more power over digital traffic. According to Goldsmith and Wu (2006), governments continue to be relevant, and there is no complete borderless internet. Rather, governments, businesses and individuals have a divided control. This begs the question of the extent to which sovereignty a state can exercise when the most important infrastructure of that state is not entirely controlled by it.

The governments find different responses to this Issue. Authoritarian regimes such as China and Russia advocate the so-called cyber sovereignty, i.e. the intense government control over their online space. Democracies tend to encourage openness and international connections, yet they establish the regulations on the digital safety, espionage, and data protection (MacKinnon, 2012; Mueller, 2017). According to Nye (2010), cyber power is not only about tech, but it is also related to the way governments engage in rule-making, standards and the ways they regulate the digital space.

The factors render cyber security and sovereignty significant In the world politics. This paper examines the need to reconsider the state power in the 21 st century owing to the development of cyberspace. It relies on selected works to demonstrate the importance of sovereignty in cyberspace to global order, rather than being a technical challenge.

We cannot put aside the larger concept of power in the context of re-thinking the concept of sovereignty in the digital era. The classic understanding of power is economic, military and territorial might. However, cyberspace provides a fresh dimension through which these powers are practiced differently. According to Nye (2010), the cyberspace power implies the utilization of the digital means to attain the objectives of protecting networks, manipulating people, or annoying adversaries. States now must not only defend the cyberspace, but they must also shape global digital regulation, an extension of sovereignty to the global level.

The fact is that cyberspace is difficult to regulate. According to Rid (2013), the consequences of cyber actions though not considered as complete wars, have political and strategic impact. There are attacks that cannot be predicted, there are those that can be prevented, but states cannot always point anybody. So, Uncertainty undermines the ability of sovereignty and minimizes the usefulness of traditional deterrence. Indicatively, in 2007, the country of Estonia had serious cyberattacks, which damaged but remained unidentified by the attackers (Deibert, 2013). Sovereignty of Estonia was undermined by the lack of clarity on shared blame, and it was not in a position to resist it in case any other state had invaded it under the international law.

The digital Infrastructure is very technical and political. As described by Mueller (2017), the key aspect of internet regulations is sovereignty, including the authority to establish data flows or domain names. States attempting to enact legislation on digital networks can run into conflict with world openness policies. Despite the role played by governments via law and enforcement in the internet, Goldsmith and Wu (2006) demonstrated that they do not have absolute power due to the global nature of cyberspace. Governments, businesses and international groups share sovereignty.

Cyber sovereignty is a particularly disputable concept. It is embraced by authoritarian regimes to have a strict control of the internet. An example is China, which emphasizes on localization of

data, filtering and independence in technology whereas most western nations advocate a more open global internet (MacKinnon, 2012; Topor, 2024). These models all indicate that internet sovereignty is not an impartial or definite concept. The discussion of world talks today is aimed at achieving the balance between security, openness and sovereignty.

In this way, cyberspace will have to rethink the idea of a strong state. Sovereignty now encompasses both border control and network protection, information management and digital life standards. According to Deibert (2013), the dark side of the internet, which includes hacking, manipulation, as well as spying, demonstrated that states should do more to protect themselves against traditional as well as cyber threats. This fact has made cyber sovereignty an aspect of international politics, a manner of exercising influence and defence. This article advances that sovereignty in cyberspace is going to determine the future of the state power.

Problem Statement

The emergence of cyberspace in the 21 st century has broken the traditional concept of sovereignty that was historically based on the borders of the territory and exclusive state control. The digital networks cross jurisdictions, providing cyber threats like espionage, sabotage, and disinformation that undermine the state control but does not physically cross boundaries (Rid, 2013). This fact undermines the traditional Westphalian concept of sovereignty and makes states reconsider the principles of their authority.

Available knowledge offers useful information which is still disjointed. Nye (2010) focuses on the emergence of the so-called cyber power, and Mueller (2017) presents the danger of internet fragmentation. Goldsmith and Wu (2006) show that it is possible to control the digital sphere by states, but Topor (2024) points out that cyber sovereignty is a political and security project. However, no apparent agreement exists as to whether cyberspace undermines the sovereignty or it merely transforms it. The main problem, then, is how the concept of sovereignty is being redefined during the digital age, and what does reconfiguration of sovereignty entail to the 21 st century power of the state.

Research Objectives

1. To analyze how the rise of cybersecurity challenges and reshapes the traditional concept of state sovereignty in the 21st century.
2. To examine the evolving strategies through which states assert, defend, and negotiate power in the digital domain.
3. To assess the implications of cyber governance, surveillance, and digital interdependence on global power relations and national autonomy.

Research Questions

1. How has cybersecurity transformed the traditional understanding and exercise of state sovereignty?
2. In what ways do states use digital tools and cyber strategies to maintain or expand their power in international relations?
3. What are the broader implications of cyber interdependence and governance for state authority and global security?

Significance of this study

The importance of this study should be seen in the fact that it contributes to one of the most urgent issues of modern political science and international relations the change in sovereignty in the

digital age. Conventional theories of sovereignty focus on territorial integrity, control of borders and supremacy of state in its jurisdiction. However, due to the new spaces of cyberspace, as Deibert (2013) and Nye (2010) stress, state power is challenged and even undermined. The present paper fills the gap in the classical conception of the concept of sovereignty and the reality of cyber power, presenting a new approach to the analysis of the state power in the twenty-first century.

Academically, the research contributes to the literature on the topic of sovereignty by applying theories of sovereignty to new literature on cyber security. Though, as Rid (2013) argues, the militarization of cyberspace is problematic, Mueller (2017) emphasizes the danger of fragmentation of the internet as the states strive to gain control. Introducing these views into a discussion, this study can add to a more complex perception of the way sovereignty is changing. It also concurs with the current research which underscores the interrelation between power, technology, and governance (Goldsmith and Wu, 2006; MacKinnon, 2012).

Practically, the research is very significant to policymakers, security experts, and world bodies. Cyberattacks are gaining popularity among states and disrupt the fundamental infrastructure, posing a threat to the national security and making the democratic processes difficult. The definition of sovereignty in digital setting will help decision makers to come up with resilience building measures that will not compromise openness. Additionally, the situation in china versus internet freedom in liberal democracies characterizes the opposite course states can choose (Topor, 2024). This paper has been able to identify the policy trade-offs between control and connectivity through the analysis of these rival models and some implications to governments through this analysis.

International governance and law have been other areas that the research has become meaningful. The existing legal systems are ineffective to address the digital threats. The international community has encountered problems of attributing, mass jurisdiction, and conflicting norms which have presented a challenge to the collective response to cyber incidents by the international community. Through the interaction of sovereignty with the governance structures, this study throws some light on how international norms could evolve to enhance cooperation without infringing state autonomy.

Lastly, this study is relevant to the society. The concept of cyber security goes beyond the state power to protect citizens, civil liberties, and democratic institutions. According to MacKinnon (2012), the fight over liberty has been irrevocably linked to the issue of sovereignty because the state influence is still largely common in determining the frontiers of digital rights. The implications of knowing how states exercise sovereignty in the cyberspace is thus of direct concern to the access of information, privacy and security of individuals.

Research Methodology

The research methodology used in this study is qualitative based on literature. The argument is based on a critical analysis of the books, journal articles, as well as policy papers related to the topic of cybersecurity and sovereignty. The study employs thematic and conceptual analysis method to discuss the manner in which the scholars have argued about the state power in the 21 st century and how digital technologies transform sovereignty. Unlike use of numerical data, this is more interpretational, comparative and synthesizing in that it brings a deeper comprehension of the changing theories and perspectives. The qualitative orientation gives room to uncovering the assumptions underlying, influences of ideologies, and alternative accounts in the literature. Through the analysis of how various authors approach the issues of cyber threats, state resilience, and the loss or change of sovereignty, the paper identifies some areas of agreement and

disagreement. In addition, the methodology allows the research to engage the different critically perceptions of other disciplines, including political science, international relations, and security studies in order to have a more detailed image. In such interpretation process, the study will not chart only. The existing knowledge and also expose parallel areas of weaknesses in conceptualization and as well as uncharted areas that will dictate the birth of the new mode of thinking about the applicability of sovereignty in the digital age.

Theoretical Framework

The two key theories used in this study include the Classical Sovereignty Theory and Cyber Power Theory that explain how the emergence of the cyberspace has redefined the concept of state power and the sense of sovereignty in the twenty-first century. The efforts to scrutinize the shifting issues that states encounter in the borderless digital realm is formed by a mixture of the traditional view and a contemporary reinterpretation of the problem, which establishes a balanced prism through which the problem can be viewed.

Classical Sovereignty Theory is the basis of the interpretation of the sovereignty as the most supreme authority of the state in its territory and principle of non-intervention in the domestic affairs. This framework developed out of the Westphalian tradition, which influenced the modern international system which viewed states as autonomous actors with distinct boundaries. Nonetheless, Krasner (1999), describes sovereignty as the act of organized hypocrisy, noting that although the principle is maintained in rhetoric, it has been broken by interventions, economic globalization and outside pressure in most instances. In the domain of cybersecurity, this theory emphasizes the conflict between the concept of territorial dominance and the practice of cyber threats that disregard the existence of physical boundaries and render the states incapable of controlling and securing their online space fully.

Although the Classical Sovereignty Theory can be used to set the historical background, the theory of Cyber Power (Nye, 2010) can be used to comprehend the sovereignty in the digital era. Nye defines cyber power as the capacity to employ digital assets and strengths so as to influence the occurrences in international relations. This consists of defensive as well as offensive operations, but also the greater power over information streams, popular opinion, and global standards. Unlike the conventional power, cyber power is very asymmetric and decentralized: non-state actors, smaller states, and corporations can fight against larger powers using loopholes in digital networks. According to this theory, it is obvious that cyberspace sovereignty concerns not only the ability to control the territory but also the capacity to resist, technological and power in the digital world.

Combined, the two theories form a powerful analysis. Classical sovereignty theory grounds the research on the traditional values of state power, whereas cyber power theory describes the changes caused by the digital technologies. The works of Deibert (2013), Rid (2013), Mueller (2017), Goldsmith and Wu (2006), MacKinnon (2012), Topor (2024), Castells (2009), Choucri (2012), and Kello (2017) are also supportive works that enable the connection of the theory to the real-world discussion of cyber conflict, global governance, and digital sovereignty. The hybrid framework enables the paper to evaluate the question of whether sovereignty is being subdued, transfigured, and redefined in the wake of cybersecurity and technological transformation.

Literature Review

1. *Thomas Rid's Cyber War Will Not Take Place (2013)* is One of the most discussed works in the areas of cybersecurity and foreign relations. Rid confronts the widely held view that cyberspace has brought about a novel type of warfare, rather, he claims that what most

people term as cyber war is more appropriately perceived as three separate actions: sabotage, espionage, and subversion. In his opinion, none of them can be considered a full-fledged war in the Clausewitzian meaning of war as not all of them involve physical violence, political aim, and definite consequences, which are the characteristics of the ordinary war. This point is essential in the re-evaluation of state power in the 21 st century. Rid encourages scholars and policymakers to pay less attention to the rhetoric of war and more to political, legal, and strategic consequences of cyber activities by denying the existence of the so-called cyber war. As an instance, cyber espionage activities like stealing government or corporate secrets may not cause damage to infrastructure, but it destroys sovereignty by disabling state control on information. Equally, cyber subversion, such as propaganda campaigns, has the ability to sabotage democratic institutions without necessarily passing through the gate of open confrontation. The structure of sovereignty in the realm of persistent, ambiguous and frequently deniable threats is challenged in Rid as a way of reflecting on the actions of the state to enforce and protect its sovereignty. Rather than planning against the eventuality of digital Pearl Harbor the way policymakers had been warning, Rid points to the fact that states should be prepared to live in low-level attacks that are persistent and defy the distinction between war, crime, and politics. His work thus redefines the argument on sovereignty by showing how cyber activities undermine state power in ways very subtle and long lasting. Although the book by Rid is a strong critique of the narrative of the cyber war, it is not in itself a detailed theory of the development of sovereignty on the basis of cyber pressure, but is rather aimed at refuting hyperbolic statements (Rid, 2013). There is more research that can be conducted on his analysis about how states redefine the concept of sovereignty as a reaction to long-term realities of sabotage, espionage, and subversion in the digital era.

2. Joseph Nye's *Cyber Power (2010)* is a continuation of his previous writings about soft and hard power to determine the ways in which the digital era is changing international relations. According to Nye (2010), cyber power is the capacity to achieve desired results by exploiting the electronically networked information materials of the cyber space. He distinguishes between two types of cyber power, i.e., offensive facets, including cyberattacks, espionage, and sabotage; and defensive or soft power aspects, i.e., influencing the development of global standards, norms, and narratives of digital governance. The contribution by Nye is significant in that he appreciates that states are not the only ones with cyber power. Contrary to the old civilian methods of military or economic power, the cyberspace enables non-state actors - hacks, corporations, activist groups - to exercise influence without being commensurate by their size. This decentralization complicates the conventional concept of sovereignty where the state was presupposed as the main and most influential player. Nye also highlights the asymmetric characteristic of cyber conflict: weaker states or even small organizations can cause significant damage to the stronger ones by cyberattacks as occurred in the examples of cyber espionage and ransomware attacks. Meanwhile, Nye places cyber power in the context of his general theory of complex interdependence. He emphasizes the fact that cyberspace is highly inter-linked and that collaboration is not less significant than competition. This sense of sovereignty cannot be absolute, but rather mediated by common vulnerabilities and the need to have transnational norms. His model, therefore, provides useful discourses in the conceptualization of how sovereignty can be practiced in a world where boundaries are porous and power is dispersed all over. Although this work is conceptually rich, Nye makes it work mostly theoretical. Instead, he describes the concept of cyber power and its importance without providing the empirical research on how states implement the cyber strategy and the ways

in which they balance sovereignty with interdependence (Nye, 2010). This creates a gap that can be further researched on the practical processes by which states seek their sovereignty in cyberspace.

3. Jack Goldsmith and Tim Wu's *Who Controls the Internet? Illusions of a Borderless World* in it, they critique the early utopian sentiment that the Internet is free of control, and cannot be touched by the hands of the state. They demonstrate that in fact, the Internet is not borderless, but rather, it is a product of a country's politics, culture, and laws. Through case studies, they illustrate government power in controlling the Internet's legal, technical, and regulatory aspects, i.e., the Great Firewall of China, France's regulation of Nazi memorabilia, copyright control in the United States, etc. Goldsmith and Wu (2006) assert that in the case of cyberspace, states are not powerless, but merely adapt their existing regulatory frameworks to exercise dominance over the virtual. Their primary argument is that cyberspace is more territorial than many of its early advocates envisaged, raising new and extreme questions in the scope of control of the state. Goldsmith and Wu, in their study of cyber sovereignty, demonstrate that states can and do regulate cyberspace. Importantly, Goldsmith and Wu show that the perception of the state sovereignty is obsolete in the new digital era and that the authority of the state is disrupted, but, the state is not eliminated. emphasis on the compatibility of sovereignty with cyberspace regulation supports the argument that sovereignty remains relevant, though in an evolving form. Despite its groundbreaking insights, Goldsmith and Wu's book is dated. Written in the early 2000s, it does not address the rise of social media platforms, cloud computing, mobile internet, or artificial intelligence—all of which dramatically reshape state-cyber relations (Goldsmith & Wu, 2006). Moreover, their examples focus mainly on Western democracies, with limited exploration of alternative models of cyber sovereignty in non-Western contexts.

4. *Westcott's Digital Diplomacy and State Authority (2020)* examines how digital technology has revolutionized diplomacy, communication, and sovereignty in the 21 st century. According to him, the more states engage in diplomacy, online platforms the more the old conception of state power is being undermined by the decentralizing aspects of information flows in the digital realm. Online communication causes national borders to become indistinct and controlling communication and information by the state becomes almost impossible to achieve. Westcott(2020) points out that digital diplomacy not only increases the engagement and transparency but also exposes some weaknesses especially in relation to cyber threats and disinformation campaigns. His works show that sovereignty has recently become the capacity to control the integrity of information, secure the critical infrastructure, and develop resilience against cyber manipulation. Westcott successfully connects the issues of diplomacy and digitalization, and his work is based more on the aspects of communications and soft power, instead of structural change of sovereignty. The incorporation of cybersecurity, state power, and sovereignty in the international relations field outside the digital diplomacy frameworks still requires further theoretical integration.

5. *Durojaye & Raji's State-Sponsored Cyber Activities and Global Power* explores the impact that the state and state-sponsored entities have in the cyber environment by both offensive and defensive campaigns. They highlight their analysis through the increasing militarization of cyberspace and how cyberattacks are applied to exert national power even without physical warfare. They stress that the critical infrastructure and data systems are now an extension of a national sovereignty. The states are currently spending a lot on cyber capabilities as a tool of deterrence and influence by establishing an unequal relationship where technologically superior countries take over the digital arena. The article

recommends that there should be more international standards and policies of the world in order to control cyber conduct. Despite the valuable evaluation of the cyber conflicts and power balance by Durojaye and Raji, they pay more attention to the technical and security sides of the relationships without deriving how these relationships transform the state sovereignty as a political notion. Qualitative studies bridging the linkage between technological militarization of the cyberspace and the re-definition of political sovereignty in the digital age are still minimal.

6. *Lev Topor's Cyber Sovereignty: International Security, Mass Communication, and the Future of the Internet* recent book directly relates to the current changing concept of cyber sovereignty in the context of international relations. According to Topor (2024), states are redefining cyber space sovereignty as an element of the overall security and communication policies. He analyzes how governments define cyber sovereignty as a defensive need safeguarding data, networks, and critical infrastructure and a political initiative associated with legitimacy and control over information circulation. He reveals that states not only apply cyber sovereignty to control technology but also narratives and influence popular opinion as well as establish political power both domestically and abroad. It is especially pertinent to this two-fold attention in the times of disinformation campaigns, surveillance technologies, and world discussions on the topic of digital governance. Topor gives useful insights on the contemporary relevance of sovereignty by demonstrating how the traditional IR concepts are digitized. Nevertheless, he is more descriptive. Although he charts the strategies employed by states to frame and sell cyber sovereignty, he never theorizes fully the relationship between classical sovereignty and contemporary cyber power. The book presents some significant trends but does not answer the further analytical questions of how cyber sovereignty rearranges the balance between state power and transnational digital forces (Topor, 2024).

Analysis and Discussion

The contemporary digital realm has transformed the concept of state sovereignty that has existed radically. Conventionally, the power of states was marked and restricted as per the geographical boundaries and control of material resources. However, the cyberspace is a space of no borders where digital infrastructures and data flows and virtual networks often transcend national borders. This change fails to hold the classical concept of Westphalian sovereignty, in which national interest and power on the digital space must be imposed by states using new strategies (Kello, 2013).

One of the most Significant implications of this change can be viewed as the appearance of the notion of cyber sovereignty. Cyber sovereignty may be described as the state assertion to control digital infrastructures, data management and cyber action within and sometimes outside a state. Some countries such as china and Russia that have practiced this in full throttle and put strict measures on internet control, localization of data and tracking cyberspace. Its advocates believe that cyber sovereignty helps states to ensure the security of their critical information infrastructure, protect their nationals against cybercrime, and safeguard national security. Those against it, however, caution that too much state regulation in cyberspace will disrupt international cooperation in digital space, choke innovation, and endanger free exchange of information (Maurer, 2018).

Cyber threats have also become ubiquitous and asymmetric as far as security is concerned. Cyber-attacks can also be mounted remotely by a nation or non-state entity and sometimes with little risk of specified immediate attribution or revenge unlike traditional military threats. The 2016

interference of the U.S. elections as well as the cyber espionage campaigns sponsored by states, are high profile, but they highlight that national infrastructures are vulnerable and that cyber capabilities are strategically important. As a result, states are embarking on encompassing cyber strategies in national security frameworks, raising cyber command structures, and funding defensive and offensive cyber operations. This change indicates a wider realization that cyber security cannot be separated with the capability of states and sovereignty (Libicki, 2007).

In addition, the Internet security issues also demand the reconsideration of the conventional diplomacy and international law. The inexistence of universally recognised norms and enforceable regulations in cyberspace makes it difficult to put in place accountability and response. States have to maintain a complicated balance between the need to declare their national interests and the obligation to follow the development of international frames. Multilateral initiatives, including the UN Group of Governmental Experts (GGE) on Developments in the Field of Information and Telecommunications, are aimed at coming up with norms of responsible state conduct in cyberspace. Nevertheless, diverse national interests and the variety of ideas concerning cyber sovereignty tend to conflict with agreement. This conflict highlights the paradox of digital sovereignty in that, on the one hand, states want to have a dominant role in the cyber industry, on the other hand, cyberspace is global and, therefore, requires collaboration and joint regulation (Cornish and Edwards, 2009).

Cyber sovereignty has a socio political aspect, which is also important. Cyber security cannot be considered only a technical or a military problem; it has social, economic, or political aspects. Governments have to find a balance between security needs and safeguarding civil liberties, privacy rights and freedom of expressing themselves. As an example, a policy that puts a heavy emphasis on national security by spying on or censoring most people can result in people losing trust and developing internal opposition. Consequently, cyberspace should be governed through delicate approaches that combine technology, policy, and human rights issues (Deibert, 2013).

Overall, the discussion shows that digital age requires re-conceptualization of state power. The concept of cyber security has become part of the core of sovereignty by defining the way of how states distribute the power, safeguard their national interests, and communicate and cooperate on the international level. Although cyber sovereignty provides a model of control assertion, it comes with the challenges of governance, collaboration and legitimacy. States need to implement multi-dimensional approaches, the integration of technological potential, legal frameworks, and diplomatic interactions, to cope in the complex and changing cyberspace. Lastly, the nexus of cyber security and sovereignty justifies the original condition of state power in the 21 st century, not according to its physical delimitation but according to the possibility to regulate the invisible yet important sphere of cyberspace.

Implications

The consequences of this study go far beyond the theoretical discussions, since it involves the way we conceptualize sovereignty, the way governments address the issues of cyber threat, and the ways of societies to reconcile the issues of security and freedom in the cyberspace age. This research illuminates academic, policy, and practical implications that go hand-in-hand by reconsidering state power in the 21st century.

Academically, the paper helps advance the changing body of literature concerning sovereignty by refuting the conventional belief that defined state power basically in terms of borders and military power. The emergence of cyberspace proves that power cannot be perceived solely in physical sense anymore, but has to reflect on the digital networks that the states, corporations and non-state

actors have operated in. Reading Nye (2010), Rid (2013), Mueller (2017), and Topor (2024), this study invites scholars to embrace the interdisciplinary methods which utilize the political science, international law, and technology studies. Concurrently, it points to an apparent gap: the literature on this subject gives significant attention to the views of digitally advanced states, leaving us with no answers concerning how weaker states negotiate the sovereignty of the cyber-space. By pointing out this gap, the research opens possibilities of further opportunities to broaden the range of dominant narratives and more diverse voices can be represented.

On the policy level, the study clarifies that the conventional policy approaches to protecting the sovereignty are becoming inefficient. Cyberattacks recognize no boundaries and can be perpetrated by an actor that is even hard to identify, including state-sponsored gangs, or individuals. In the case of governments, defending sovereignty requires not solely the territorial protection but also the digital one. Statecraft development often takes the form of legal frameworks, cyber defense and investment in digital literacy. Nevertheless, none of the states can address these issues independently. It is imperative to communicate with the rest of the states in terms of sharing information, norm-building, and capacity development. This is especially significant to the nations of the Global South that in many cases do not have the capacities to develop effective cyber security on their own. The divide between the digitally strong and digitally weak states will continue to grow without the aspect of inclusive cooperation, negatively affecting the sovereignty of the nation and the stability of the world.

To governments, the results highlight the problem of the importance of investing in infrastructure, skilled workers, and quick response mechanisms to protect sovereign cyberspace. The international organizations should be on the forefront to create inclusive platforms of governance in which the smaller states too have a say in determining the norms of the cyber conduct. In the case of civil society, the study draws attention to the necessity to make certain that any attempt to enhance cybersecurity will not harm democracy, privacy, and human rights. The sovereignty of the digital age cannot be narrowed down to control; it has to safeguard the freedoms that provide the legitimacy to the power of states.

Combined, the findings of this paper highlight the reality that sovereignty in the 21 st century no longer exists within territorial boundaries but rather is delimited by the ability of states to control and safeguard their digital realm. Putting state power back on its feet in this manner is not merely an exercise in theory: it is a pressing need among policymakers, academics, and civilizations engaged in the reality of a non-national world.

Conclusion

The conclusion of the paper is that digital era is changing the concept of sovereignty not basing on territory and physical power but ability to exercise control and control in the cyberspace. The existing literature on the subject indicates multiple aspects of this change, yet does not unify, which can be discussed as one of the indicators of rapid technological shifts. The paper concludes that the issue of sovereignty in cyberspace cannot be maintained only by the states, but they have to cooperate, share common norms and international rules, but the imbalanced powers of states pose problems related to fairness and legitimacy. The element of cybersecurity is also connected with the protection of democratic values, i.e. the states have to find the way to balance between security and rights and openness. Overall, it can be stated that digital realities are challenging sovereignty in the 21st century, and it is necessary to reconsider the power of the state and address the emerging challenges.

Recommendations

- To effectively negotiate the evolving nexus between cyber security and state sovereignty, governments should consider the introduction of comprehensive national strategies to cyber that include defence, governance, and digital rights together with developing mature public to private relations in the sharing of information and response to cyber attacks.
- Investment in cyber capacity-building, digital literacy, and research organizations is also important in order to curb the weaknesses of the society and make nations more resilient.
- States should be able to come up with clear regulations and laws, which would ensure that there is a balance between cyber sovereignty and civil liberties in a manner that will be transparent and under judicial check, to ensure the people will not lose trust.
- At the international level, the states should increase cooperation in the sphere of multilateral forums, come up with norms of responsible state behavior in the cyberspace, and in formalize cyber diplomacy to prevent the growth of the conflicts and control them.
- Moreover, the ethical technologic innovation, inculcating the security-by-design implementation and enhancing national incident response capacity such as the CERTs and joint crisis exercises will help the states be prepared to combat the new threats.
- The collective security can be cemented with regional cooperation via common platforms and common training programs in the interconnected digital world.

References

1. Topor, L. (2024). Cyber sovereignty: International security, mass communication, and the future of the Internet. Springer. https://doi.org/10.1007/978-3-031-58199-1
2. Rid, T. (2013). Cyber war will not take place. Oxford University Press.
3. Goldsmith, J., & Wu, T. (2006). Who controls the Internet? Illusions of a borderless world. Oxford University Press. https://doi.org/10.1093/oso/9780195152661.001.0001
4. MacKinnon, R. (2012). Consent of the networked: The worldwide struggle for internet freedom. Basic Books.
5. Mueller, M. (2017). Will the Internet fragment? Sovereignty, globalization, and cyberspace. Polity Press.
6. Nye, J. S. (2010). Cyber power. Belfour Center for Science and International Affairs.
7. Krasner, S. D. (1999). Sovereignty: Organized hypocrisy. Princeton University Press.
8. Castells, M. (2009). The rise of the network society. Wiley-Blackwell.
9. Choucri, N. (2012). Cyberpolitics in international relations. MIT Press.
10. Kello, L. (2017). The virtual weapon and international order. Yale University Press.
11. Westcott, N. (2020). Digital diplomacy: The impact of the digital revolution on international relations. International Affairs, 96(3), 679–696. https://doi.org/10.1093/ia/iiaa023
12. Durojaye, H., & Raji, O. (2022). Impact of state and state-sponsored actors on the cyber environment and the future of critical infrastructure. arXiv preprint arXiv:2203.10211. https://arxiv.org/abs/2203.10211
13. Maurer, T. (2018). Cyber Sovereignty: State Control in the Digital Age. Carnegie Endowment for International Peace. https://carnegieendowment.org
14. Libicki, M. C. (2007). Conquest in Cyberspace: National Security and Information Warfare. Cambridge University Press.
15. Cornish, P., & Edwards, G. (2009). Cyber security and national power. Royal Institute of International Affairs. https://www.chathamhouse.org/2009/04/cyber-security-and-national-power