| P-ISSN 2664-0422 | Pakistan Social Sciences Review | October-Dec 2024, Vol. 8, No. 4 |
|---|---|---|
| O-ISSN 2664-0430 | https://doi.org/10.35484/pssr.2024(8-IV)64 | [706-714] |

Pakistan Social Sciences Review
www.pssr.org.pk

**RESEARCH PAPER**

# Cybersecurity and Sovereignty: The Conflict among States in Governing Cyberspace

**Dr. Sabir Ijaz**

Assistant Professor (visiting) Department of International Relations, National University of Modern Languages (NUML) Karachi Campus, Sindh, Pakistan

***Corresponding Author:** sabir.ijaz@numl.edu.pk**

**ABSTRACT**

The main objective of the paper is to highlight the problems the modern states face from prevailing cyberspace and usage of internet. It explains how cyberspace undermines/threats the state sovereignty. It also focuses how states can negotiate/cooperate to solve this problematic issue. Sovereignty is regarded as one of the requisite component of state formation. A state tends to establish its sovereignty over its territories by all possible means to prove its identity. However, technological advancements and new innovations present novel challenges to the state's sovereignty in maintaining its cyber space. Political leaders predicted in 1990s that information age would undermine states' territorial integrity and sovereignty. States and international organization have not been successful in yielding consensus how to regulate cyberspace under strict international laws to meet these new developments. Presently, prevalent digital technologies and ubiquitous cyber incidents are challenging national sovereignty more than some of the rising international tensions. This study signposts these emerging challenges in detail which are presented by cyberspace. The study qualitative in nature. It mainly investigates and reviews the books, journal articles and reports on the topic. The study concludes that cyberspace and extensive growth of internet usage would become a global concern. It also clarifies how cyberspace might threat the state sovereignty in modern era. The study recommends that states must cooperate to mitigate cyberwarfare to avoid future conflicts and technological warfare.

**KEYWORDS** Cyberspace, Cybersecurity, Sovereignty, Warfare

## Introduction

Traditionally, sovereignty has grounded itself on physical space and territoriality. Every state aims to establish its jurisdiction within its territorial authority and compromise no external interference or authority (Mueller, 2020). On the contrary, cyberspace, according to Jason Andress and Steve Winterfeld (2013) is a global domain made up of internet, telecom networks, controllers, and embedded processors that gather, analyze, alter, transmit, store, and secure data. Its original purpose was to improve connectivity and communication (Andress & Winterfeld, 2013). However, destructive technological advancements and growing human reliance on cyberspace, it has become a battlefield where data and information technology are both used as weapons and targets of war to incite instability, destroy vital infrastructure, and conduct espionage. Bellanger and Williams (2011) explained a comparison between these two concepts stating that "states are like places while internet/cyberspace is a link. Sovereignties are mainly bounded in confined physical space. Whereas internet is a dimension that connects all areas. Although there are many and different States, the Internet is universal one." This description provides that internet or the whole

cyberspace cannot be regarded as a legal entity bounded or restricted by geographical boundaries (Belanger & Williams, 2011).

Liaropoulos (2016) describes as the 'environment formed by physical and nonphysical components characterized by the use of computers and the electromagnetic spectrum to store, modify and exchange data using computer networks' (Liaropoulos, 2016). Radvanovsky and McDougall (2023) maintain that it is a worldwide digital network that permeates every facet of our everyday existence. In addition to the internet, it includes the vital infrastructure that underpins contemporary societies, such as banking operations, transportation networks, water supply systems, and electrical grids. According to some estimates more than ninety percent of vital computer infrastructures in the western countries are run by individuals and organizations belonging to private sector (Radvanovsky & McDougall, 2023). In recent years, it is rapidly becoming trending for human interaction, communication and information. The expansion of cyberspace has excess to all parts of the world. According to some estimates internet is used by majority of individuals and all the states have access to it hence a vital part of transition for all states (Mbanaso & Dandaura, 2015). The rapid growth of it is not free from dangers like crime and competition. Cases of spying are happening frequently in many parts of the world almost every day. States, individuals, companies and activists are struggling and finding it difficult to regulate activities which are taking place in cyberspace. Increase dependence on technology carries threats to the fundamental systems that support the functioning of modern society. This upturn interdependence has become a major concern for states in the contemporary affairs. Resultantly, states are more vulnerable to cyber threats and need innovative measures, cooperation, integrated policies, anticipation and continuously investing in research to meet the emerging challenges in the cybersecurity domain (Roşca, 2024).

The conventional notion of global governance, which is mostly state-centric, is seriously challenged by cyberspace. It challenges conventional understanding of important concepts like security and sovereignty because of its asymmetrical and anonymous aspects (Dalla Guarda, 2015; Liaropoulos, 2016, 2015; Slack, 2016). The rationale is that this new domain's technological and socio-political features are continually being redefined. In cyberspace, the interests of every individual or organization are being impacted by the quick speed of technology advancement and how societies react in the digital sphere. Big Data, the Internet of Things (Weber, 2013), and the Dark Web are examples of information technology advancements that have outperformed governments and international organizations in providing effective governance (Romeo, 2016). States lack the technical and human resources which are needed to protect their citizens. In cyberspace, the connection between the public and private sectors is similar to a contradiction. The private sector cannot be shielded from all cyber threats by governments acting as a security provider. However, the private sector is asked to help the government with cyber security issues by carrying out surveillance and censorship.

## Literature Review

Cyberspace has engulfed all national and international domains in security, economic and humanitarian terms. Different malwares (Ransomware, NotPetya) have infected millions of computer networks in more than hundreds countries causing losses of nearly $4 billion. In 2016 alone, various malicious cyberattacks caused almost hundred billion worth of damage to the U.S. economy (Gordon, 2018). Individuals, meanwhile, have become all too accustomed to losing access to or control over

otherwise confidential information (Butt, Abbod, & Kumar, 2020).. Besides, prominent cyber episodes like foreign intervention in US election and the targeting of an Iranian nuclear plant clarify the national security stakes of cybersecurity. Moreover, cyberspace has impacted the sovereignty of many states by violating national laws particularly in online disputes resulting from trans-border exchanges. There is no controversy that Cyberspace has played a significant role to a role to allow individual to enjoy freedom from the strict laws of state or government control. Such freedom or liberation from governments' laws is a serious violation to the sovereignty of the state. Jacquot and Weitzel (2001) emphasized the necessity of implementing new legal frameworks to control cyberspace concerns in response to these conundrums. Traditional rules and regulations have frequently been criticized in this regard for their incapacity to handle the rapid advancements of internet usage. Cyberspace appears to be a haven for criminals whose violating actions could potentially jeopardize state sovereignty (Jacquot, & Weitzel, 2001). According to Lin (2012), the modern criminal can steal more with a computer than with a gun, demonstrating how cyberspace is rife with cybercrime. The terrorist of the future might be able to cause more harm with a keyboard than with a bomb. Because of the internet's boundarylessness, which suggests that state lines are becoming less distinct, cybercrime becomes more complex (Lin, 2012). Some argued for government intervention to regulate the internet and safeguard state sovereignty because they believed that the independence of cyberspace was highly dangerous. The non-governmental approach, which stresses the role of individuals in reorganizing cyberspace, is in opposition to this. Many countries have already been compelled by this concern with the boundarylessness of cyberspace to create and regulate policies, procedures, or systems that can monitor their own cyberspace and preserve state sovereignty. These issues have made cyberspace from a matter of low politics to higher national security concern (Brainard & Siplon, 2002).

The World Wide Web is a new sphere of economic, political, and social activities; it poses hard questions to the state and international systems. Cyberspace is in contrast disjointed and does not follow physical territories, and hence states cannot easily assert their control (Lonergan & Poznansky, 2024). This is made worse by the fact that there is no globally agreed legal regime governing cyberspace and instead most states act in their self-interest as opposed to a collective comity of nations (Efrony, 2024). This leads to a piecemeal system of governance as there are contrasting common approaches to digital governance and cybersecurity.

This problem is exacerbated by the geopolitical struggle between great powers such as the United States, China, and Russia that put forward different visions of the regulation of cyberspace (Calderaro, & Craig, 2020). While liberal democratic countries reveal a concept of free and open internet, autocratic societies reveal a concept of state domination over internet sovereignty. These different strategies are not only a blow to international interactions but also a favorable landscape for cybercriminals and attackers sponsored by states. Solving these challenges implies achieving a goal of such approach which assumes collaborative interstate cooperation, engagement of all relevant stakeholders' perspectives, and orientation on the development of the most effective technologies to maintain the safety and openness of the internet space (Topor, 2024).

## Methodology

The research is qualitative in nature. The study mainly focuses on secondary data on cyberspace. The data includes books, journal articles and reports. Researcher

has also investigated literature on sovereignty and security and its connection to cyberspace.

**Results and Discussion**

The value of this research is based in understanding how the relationships between cybersecurity and sovereignty are changing, an important field that defines the current world politics and international law. Every once in a while, it is important to look at how states are adapting to these sovereignty challenges in a world where cyberspace is a rapidly growing element of economic, political, and social institutions. This paper advances the current literature on global cybersecurity by establishing that the current structures of governance are deficient in their provisions for managing cybersecurity risk and by elucidating how these inadequacies will continue to challenge the international relations framework, global trade, and national security in the future. Analyzing the actions of the US, China, and Russia, this work reveals the effects of various governance systems on the interaction of states and the availability of conflict in the area of cyberspace (Riordan, 2018). In addition, the research offers insights into the flaws of the present global efforts, particularly the UN GGE and the OEWG, in failing to reconcile the existing discord between different States' interests (Sukumar, Broeders & Kello, 2024). These insights are particularly important for policymakers, intergovernmental organizations, and other stakeholders who are interested in developing coherent strategies and avoiding potentially adverse consequences stemming from the fragmented and (more often than not) ineffective governance of cybersecurity (Nilsson et al, 2012).

Also, this work is valuable due to its emphasis on the implication of novel technologies, including AI and quantum computing, in redetermining the cybersecurity environment. Since these technologies provide both the opportunities and threats we need to understand the mixes that are essential for building strong defense measures and governments. A multi-stakeholder approach is presented as a suitable approach the study, including input from the governments and state institutions as well as private businesses and civil society (Ciglic, & Hering, 2021; Kaufmann, 2016). Introduced in a manner that identifies the goals of a collective management of the cyber space, this dissertation provides recommendations on how regionalism can be promoted to foster capacity building and the creation of an inclusive legal framework. This is important in the pursuit of states and global cooperation and management to realize on the one hand sovereignty and on the other hand to harness technology to enhance human welfare while containing its risks. Finally, it is anticipated that ideas in this work will enlighten policy-making processes, shape international policies and lead to sustainable resolution of cybersecurity management issues across the world (Hossain, Yigitcanlar, Nguyen & Xu, 2024).

The governmental organizations and unofficial regulatory frameworks that direct and control a society's collective actions are referred to as governance. When the connection among different sectors are blurred, governance serves as an example of a system of governing techniques. Government is only one aspect of governance. While the former needs to be accepted by the majority of people it impacts, the latter is an executive apparatus that can function even when there is strong opposition to its policies. In the literature on international relations, the term "governance" has been employed in a number of ways and is quite ambiguous. The efforts from different sectors to address shared issues that cut beyond national borders are referred to as

global governance rather than the establishment of a global government (Patrick, 2014). One way to think of global governance is as an example of governance without a government (Finkelstein, 1995).

To summarize, the following are the primary points of contention in the literature on global governance (Dingwerth & Pattberg, 2006; Nye, 2010; Rosenau, 1995). The first is the change in regulation from the federal level to suprastate levels. Second, the scope of power outside of the state has expanded, and global politics is more than just intergovernmental politics. Lastly, if representatives of impacted interests have decided on rules outside of the state through a decision-making process that satisfies realistic norms of accountability, transparency, and inclusivity, then those regulations are legal (Dingwerth, 2008). The business sector and non-governmental organizations (NGOs) are also involved in global governance, in addition to governments and international organizations. As a result, other players complement states as the main tool of global governance rather than replacing them (Ruhlman, 2014).

A number of concerns should be taken into account when addressing cyberspace governance (Deibert, 2013; DeNardis, 2014). In the first place, should cyberspace be regulated? Who ought to be in charge of governance? How ought cyberspace to be regulated? Can public-private partnerships in hybrid governance be applied in cyberspace? How can nations use cyberspace to assert their sovereignty?

The three primary techniques of distributed governance, multilateral governance, and multi-stakeholders can be used to classify the aforementioned difficulties (West 2014: 4). One way to characterize governance in the early stages of Internet growth would be as a distributed system. Online communities, which claimed that knowledge must be freely available and unrestricted, have little, disorganized governance (Deibert & Crete-Nishihata, 2012). This strategy mirrored a time when online groups were tiny, uniform, and self-policing.

As stated by Electronic Frontier Foundation (EFF) founder John Perry Barlow in The Declaration of the Independence of Cyberspace that we are forming our own Social Contract Governments are not welcome among us. It does not lie within your borders. This government will be determined by the conditions of our planet, not yours (Barlow, 1996; Wilske, & Schiller, 1997).). In the last decade of nineteen century, the Internet was still in its infancy, with less than a million users. There are currently billions of Internet users, and it has become a vital part of modern civilizations (Betz & Stevens, 2011). It has developed into the most significant infrastructure in the world and is now at a stage of development where laws are required. Despite its continued popularity in many online communities, the dispersed governance model is unable to offer effective policy solutions that the vast and heterogeneous community of cyberspace users can accept.

Those who see cyberspace as a global common have also adopted the concept that a limited role should be played by states. Cyberspace, in stark contrast to land, sea, air, and space, is a man-made area devoid of physical boundaries. It is not a worldwide common, but it does have a global common infrastructure (Cornish, 2015). Although it appears to have no boundaries, cyberspace is actually limited by the physical infrastructures that make data and information transit possible. These facilities are found on states' sovereign territory and are primarily held by the private sector. States are undoubtedly attempting to create virtual boundaries in an effort to get around the so-called border dilemma (Demchak & Dombrowski, 2011). Cyberspace is a condominium with multiple owners, as James Lewis so brilliantly put it (Lewis, 2010).

In the same way that the water and the air are seen as global commons, Paul Cornish describes it as a virtual common that nullify both private property and as well as sovereign territory (Cornish, 2015).

For proponents of international governance, the question of state sovereignty is crucial. The multilateral approach adopts a Hobbesian perspective on cyberspace. Proponents of this state-centric approach contend that states should be in charge of creating policies in cyberspace because these scholars perceive it as a problem that exacerbates insecurity (Liaropoulos, 2016). According to this strategy, the United Nations (UN) should establish a body that will oversee internet governance while allowing governments to establish their own national policy. Historically, Saudi Arabia, China, India, Iran, and Russia have backed the multilateral model. Even certain states in European Union that aim to safeguard their data from US surveillance technologies, global governance has gained importance in the wake of the Edward Snowden revelation (West, 2014).

## Conclusion

The protection of cyberspace is essential for states' national security and safety and also for the prosperity of people. It is a fundamental part of states economy and defence. Even with the much advancement private sector as well public entities are struggling for the complete protection of their systems. The frequency of adversaries related to cyberspace has increased to high level. States need cooperation and agreements to stop malicious cyber activities. A close partnership of states can promote safe, protected and reliable information and communications infrastructure that supports international trade and commerce, strengthens international security, and fosters free expression and innovation.

## Recommendations

- All the states must take the cyber issue seriously to prevent future espionage and loss of confidential data.
- Private organizations and individuals must respect other states integrity to avoid confrontations.
- It is important for states to implement strict measures to safeguard their sovereignty from cyber related threats.
- International organization must come forward to restrict individuals/private sector to violate state sovereignty.
- States must safeguard its sovereignty by implementing strict laws and regulations
- States must ensure measures to punish those who violate its sovereignty.
- There must be a consensus among states about how to ménage cyberspace.
- States must literate its individuals about the perils of cyberspace.

**References**

Andress, J., & Winterfeld, S. (2013). *Cyber warfare: techniques, tactics and tools for security practitioners*. Elsevier.

Barlow, J. P. (1996). *A Declaration of the Independence of Cyberspace.* London: Routledge.

Belanger, Y., & Williams, R. 2011). Virtual sovereignty: Exploring Canadian First Nations internet gaming ventures. *First Nations Gaming in Canada, 4(2),*52-76.

Betz, D., & Stevens, T. (2011). *Cyberspace and the state. Toward a strategy for cyber-power* (Adelphi Paper 424). Oxon: IISS, Routledge.

Brainard, L. A., & Siplon, P. D. (2002). The Internet and NGO–government relations: injecting chaos into order. *Public Administration and Development: The International Journal of Management Research and Practice*, *22(1),* 63-72.

Broeders, D. (2016). *The public core of the internet: An international agenda for internet governance* (p. 116). Amsterdam University Press.

Butt, U. J., Abbod, M. F., & Kumar, A. (2020). Cyber threat ransomware and marketing to networked consumers. In *Handbook of research on innovations in technology and marketing for the connected consumer* (pp. 155-185). IGI Global.

Calderaro, A., & Craig, A. J. (2020). Transnational governance of cybersecurity: policy challenges and global inequalities in cyber capacity building. *Third world quarterly, 41(6),* 917-938.

Ciglic, K., & Hering, J. (2021). A multi-stakeholder foundation for peace in cyberspace. *Journal of Cyber Policy*, *6(3),* 360-374.

Cornish, P. (2015). Governing cyberspace through constructive ambiguity. *Survival*, *57(3),* 153-176.

Dalla Guarda, N. (2015). Governing the ungovernable: International relations, transnational cybercrime law, and the post-Westphalian regulatory state. *Transnational Legal Theory*, *6(1),* 211-249.

Deibert, R. (2013). *Bounding cyber power: Escalation and restrain in global cyberspace* (Internet Governance Papers: Paper No. 6). The Centre for International Governance Innovation.

Deibert, R., & Crete-Nishihata, M. (2012). Global governance and the spread of cyberspace controls. *Global Governance, 18(1),* 339–361.

Demchak, C., & Dombrowski, P. (2011). Rise of a Cybered Westphalian age. *Strategic Studies Quarterly, 5,* 32–61.

DeNardis, L. (2014). *The global war for internet governance.* New Haven: Yale University Press.

Dingwerth, K. (2008). From international politics to global governance? The case of nature conservation (Garnet Working Paper No. 46(8)). *Institute for Intercultural and International Studies*, University of Bremen.

Dingwerth, K., & Pattberg, P. (2006). Global governance as a perspective on world politics. *Global governance*, *12*, 185.

Efrony, D. (2024). Enhancing Accountability in Cyberspace Through a Three-Tiered International Governance Regime. *International Law Studies*, *103*(1), 13.

Finkelstein, L. S. (1995). What is global governance?. *Global governance, 1,* 367.

Gordon, M. S. (2018). *Economic and national security effects of cyber attacks against small business communities* (Master's thesis, Utica College).

Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Local government cybersecurity landscape: A systematic review and conceptual framework. *Applied Sciences, 14(13),* 5501.

Jacquot, F., & Weitzel, B. (2001). *Litigations regulation. The Legal Guide of Electronics Traders* (Version Préliminaire), 204-243.

Jayawardane, S., Larik, J., & Jackson, E. (2015). Cyber governance: Challenges, solutions and lessons for effective global governance (Policy Brief No. 17). *The Hague Institute for Global Justice.*

Kaufmann, C. (2016). Multistakeholder Participation in Cyberspace. *Swiss. Rev. Int'l & Eur. L., 26(1),* 217.

Lewis, J. A. (2010). Cybersecurity: next steps to protect critical infrastructure. *Testimony to the US Senate Committee on Commerce, Science and Transportation, 23(1).*

Liaropoulos, A. (2016, June). Exploring the Puzzle of Cyberspace Governance. In *ECCWS2016-Proceedings fo the 15th European Conference on Cyber Warfare and Security* (p. 198). Academic Conferences and publishing limited.

Liaropoulos, A. (2016). Exploring the complexity of cyberspace governance: state sovereignty, multi-stakeholderism, and power politics. *Journal of Information Warfare, 15(4),* 14-26.

Lin, H. (2012). A virtual necessity: Some modest steps toward greater cybersecurity. *Bulletin of the Atomic Scientists*, 68(5), 75-87.

Lonergan, E. D., & Poznansky, M. (2024). Competing Visions for US Grand Strategy in Cyberspace. *Security Studies, 33(4),* 607-639.

Mbanaso, U. M., & Dandaura, E. S. (2015). The cyberspace: Redefining a new world. *IOSR Journal of Computer Engineering (IOSR-JCE), 17(3),* 17-24.

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International studies review, 22(4),* 779-801.

Nilsson, M., Zamparutti, T., Petersen, J. E., Nykvist, B., Rudberg, P., & McGuinn, J. (2012). Understanding policy coherence: analytical framework and examples of sector–environment policy interactions in the EU. *Environmental policy and governance, 22(6),* 395-423.

Nye, J. S. (2010). *Governance in a globalizing world*. Brookings Institution.

Nye, J. S. (2014). *The regime complex for managing global cyber activities (Global Commission on Internet Governance*: Paper Series No. 1). The Centre for International Governance.

Patrick, S. (2014). The unruled world: the case for good enough global governance. *Foreign Affars, 93,* 58.

Riordan, S. (2018). The geopolitics of cyberspace: A diplomatic perspective. *Brill Research Perspectives in Diplomacy and Foreign Policy, 3(3),* 1-84.

Rosenau, J. (1995). Governance in the twenty-first century. *Global* Governance, 1, 13–43.

Rosenau, J., & Czempiel, E. O. (1992). *Governance without government: Order and change in the world politics*. Cambridge: Cambridge University Press.

Radvanovsky, R., & McDougall, A. (2023). *Critical infrastructure: homeland security and emergency preparedness*. CRC Press.

Ruhlman, M. (2014). *Who participates in global governance?: states, bureaucracies, and NGOs in the United Nations*. Routledge.

Romeo, A. D. (2016). Hidden threat: the dark web surrounding cyber security. *N. Ky. L. Rev., 43,* 73.

Slack, C. (2016). Wired yet disconnected: the governance of international cyber relations. *Global Policy, 7(1),* 69-78.

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy, 45(1),* 7-44.

Topor, L. (2024). Sovereignty, Power, International Security and a Lack of International Law. In *Cyber Sovereignty: International Security, Mass Communication, and the Future of the Internet* (pp. 45-73). Cham: Springer Nature Switzerland.

Weber, R. H. (2013). Internet of things–governance quo vadis?. *Computer law & security review, 29(4),* 341-347.

Weitzenboeck, E. M. (2014). Hybrid net: The regulatory framework of ICANN and the DNS. *International Journal of Law and Information Technology, 22,* 49–73.

West, S. (2014). *Globalizing Internet governance: Negotiating cyberspace agreements in the post Snowden era*. Conference Paper, TPRC 42: The 42nd Research Conference on Communication, Information and Internet Policy.

Wilske, S., & Schiller, T. (1997). International Jurisdiction in Cyberspace: Which states may regulate the Internet. *Fed. Comm. LJ, 50,* 117.