International Journal of Humanities and Social Science Research
www.socialsciencejournal.in
ISSN: 2455-2070
Received: 03-05-2025, Accepted: 02-06-2025, Published: 18-06-2025
Volume 11, Issue 3, 2025, Page No. 96-101

Cyber politics: Exploring the state's notion of cyber sovereignty

Garima Nanda
Research Scholar, Department of East Asian Studies, University of Delhi, New Delhi, India

Abstract
The concept of sovereignty has evolved in the digital age, where, in addition to its territorial meaning, it also implies cyberspace, and thus the concept of cyber sovereignty has emerged. This article describes ways in which states are renegotiating sovereignty in the context of increasing reliance on digital infrastructure, worldwide data flows and cross-border cyber threats. The main research question which will drive this investigation is: How do various states conceptualise and operationalise cyber sovereignty within global cyber politics? This paper takes a qualitative and comparative research design to analyse the cyber policies of the major global players such as China, Russia, the United States, the European Union, and India. This article engages with international relations theory, legal instruments, cybersecurity policies and multilateral forums to make sense of how state-centric cyberspace governance merely mirrors broader geopolitical and ideological fault lines. The report shows that authoritarian systems are more likely to claim a harder, state-centric vision of cyber sovereignty, whereas liberal democratic countries are nudging towards a more permissive, multi-stakeholder vision of cyberspace – albeit in the direction of regulatory nationalism. India, which is operating in a tricky digital ecosystem, seems to be developing a hybrid system, which aims at striking a balance between national security, economic prosperity, and civil liberties. The article ends with the assertion that time is running out to secure an interoperable and rights-based internet architecture reconciled against competing visions of cyber sovereignty unless the world community acts swiftly and decisively to avert this crisis.

Keywords: Cyber sovereignty, internet governance, cybersecurity, digital politics, state control, India, global internet politics

Introduction

Cyberspace has become a new theatre of political and economic as well as military competition in the 21st century. As digital technologies are growing at a vast pace, the Internet is no longer a decentralised communication medium but rather a sphere of strategic relevance among state actors. This transformation has led to the emergence of cyber sovereignty, whereby states exercise control over digital infrastructure, data traffic and online behaviour within their geographical borders. (Pierucci, 2025) [1] With cyber threats becoming more advanced, cross-border in origin, and affecting a wider array of targets, including data breaches, cyber espionage, and disinformation campaigns, states perceive ever greater importance of control over cyberspace as a key factor in their national security, political legitimacy, and economic competitiveness. The emergence of cyber sovereignty is threatening the previous version of a borderless and open internet with multi-stakeholder principles of operation. Rather, it has led to a paradigm change in favour of a state-centric regulation characterised by data localisation, digital surveillance, censorship systems and national cybersecurity systems. Authoritarian governments, like those in China and Russia, have led the charge of aggressively implementing cyber sovereignty models, focusing on digital authoritarianism and ideological isolation. (Gupta & Sony, 2021) [2] By contrast, liberal democracies have historically been inclined to global interoperability and decentralised governance, though even there the trend as of late is towards regulatory aggression. As a country geopolitically placed between these poles, India offers a peculiar case of developing a hybrid model that would respond to the priorities of domestic politics and global technological ambitions. The paper aims to research the developing concept of cyber sovereignty from a comparative and analytical perspective. It also looks at the conceptualisation and institutionalisation of the control by various states over cyberspace, legal and political issues surrounding these attempts and the ensuing tension in internet global governance. It is expected that the research will be able to enrich the onward debate on the politics of cyberspace by raising and answering the question concerning how far sovereignty in cyberspace remodels the conventional understanding of state power, autonomy, and international relations in the digital era. (Leiter, 2023) [3]

The primary objective of the presented research is to critically analyse the shifting concept of cyber sovereignty and its implementation by various states in light of international cyber politics. It aims to address the political, legal, and strategic aspects of cyber sovereignty, specifically how those aspects relate to the exercise of state control over digital infrastructure, information traffic, and cyber norms. The study is also interested in examining how the rival concepts of cyber governance, spanning from authoritarian dominance to liberal regulatory regimes, are transforming international relations and altering the global internet ecosystem. A particular focus is given to the emergent Indian stance, which tries to find the balance between security needs, digital transformation, and democracy in the new rapidly changing digital environment.

To achieve these objectives, the study is guided by the following central research questions:

1. How is the concept of cyber sovereignty being defined, interpreted, and implemented by different state actors?
2. What are the key motivations—political, legal, economic, and strategic—behind the assertion of cyber sovereignty?
3. How does India's approach to cyber sovereignty compare with other global models, and what does this imply for its role in international cyber governance?

4. What are the broader implications of rising cyber sovereignty for global internet governance, digital rights, and international law?

The paper is organised in the following way: It starts with the introduction and conceptualisation of cyber politics in the digital age and proceeds with a discussion of the theoretical background of cyber sovereignty. It next provides a comparative analysis of international strategies with a special section on India. Legal-political issues and policy implications are discussed later. At the end of the article, the author provides a conclusion of the findings, a reflection of global trends, and future research.

Contextualization of Cyber Politics in the Digital Era

The online world has transformed the playground of politics, government and global affairs considerably. Cyberspace has become a new strategic area in which the states assert their power, impact the political processes, and claim sovereignty. Cyber politics is a critical inquiry about the role of digital technologies and infrastructures in the construal of authority, control, and struggle. The internet, which was initially viewed as a means of democratisation of the world, has turned into a battleground characterised by surveillance, cyber warfare, disinformation, and dependencies. (Ördén, 2021) [4] Cyberspace has strategic worth since it can manipulate elections, economies and national security without the use of conventional force. States have thus started to securitise cyberspace and take more control of their online space. The change has led to the emergence of the concept of cyber sovereignty, which holds that states should be allowed to control their cyberspace according to national interests and laws. Authoritarian models seen in China and Russia have been described as restrictive, with practices of censorship and data localisation, whereas liberal democracies like the U.S. and the EU are beginning to regulate platforms more to combat misinformation and privacy violations. This has led to the division of the digital governance models and resulted in the fragmentation of the internet into geopolitical blocs or a "splinternet". Developmental aspirations, security, and the continuing process of balancing sovereignty and global digitalisation are some of the factors shaping cyber politics in the Global South, comprising India. (Lacy & Prince, 2018) [5]

Emergence of Cyber Sovereignty as a Political and Legal Concept

Cyber sovereignty has become an important political and legal principle of the digital era, transforming how the states envision authority, jurisdiction and control in cyberspace. Originally, sovereignty meant the supreme jurisdiction of a state over its territory, citizens and law. The traditional understanding of state sovereignty has, however, been put into question with the inception of the internet, which is a borderless and transnational space. Since digital technologies have entered the national security realm, the economic infrastructure, and the process of communication between people, states have started to claim their right to manage the information flow, regulate digital platforms, and administer cyberspace inside their boundaries. Cyber sovereignty thus means the right of a state to have complete control over its cyberspace in data, internet infrastructure, content control and cybersecurity policy. (Lahmann, 2021) [6] This cyber sovereignty has assumed varied shapes the world over. In illiberal democracies, it has been used to warrant mass censorship, online surveillance, and the development of state-orientated internet ecosystems, such as those developed in China with its Great Firewall and in Russia with its sovereign internet laws. Even the most democratic nations have been pursuing elements of cyber sovereignty, especially through data localisation, national systems of cybersecurity, and control of transnational technological giants. The concept is in legal development, regularly working in grey regions where national authority clashes with international computerised transmissions. International law, especially regarding cyber warfare and digital espionage, is underdeveloped, and experts demand new norms and agreements. So, cyber sovereignty is a politically ideologically driven concept and a developing body of law that seeks to restore state control over a fast-digitising world. (Corn & Taylor, 2017) [7]

Significance of Cyber Sovereignty in International Relations and Political Science

The increasing focus on the idea of cyber sovereignty has a very significant implication for the academic fields of international relations (IR) and political science. The emergence of cyber sovereignty in IR is transforming the conventional understanding of power, security, and diplomacy. Cyberspace is the new sphere of strategic competition since the state now projects its influence not by purely military forces but by cyber capabilities, by controlling the digital infrastructure, and by controlling the data. It has exacerbated geopolitical tensions, particularly among technologically savvy nations such as the United States, China and Russia, as each of these nations proffers a different vision of global internet governance. Such trends pose a challenge to the liberal international order, which preferred a global, open, and multi-stakeholder internet regulation model, by advocating a fragmented, state-controlled digital space. Such fragmentation sometimes called the "splinternet", is part of larger changes in the international balance of power and struggles over technological dominance. (Schmitt & Vihul, 2017) [8] Cyber sovereignty has introduced valuable discourses in political science concerning how technology and state power interact. It prompts concerns about how both democratic and authoritarian governments are reinventing their internal systems of governance to counter these digital threats, manage online narratives, and safeguard national opportunities. The idea also touches upon civil liberties, surveillance, digital rights and the involvement of privately-owned corporations in state governance. With algorithmic governance and digital surveillance, political theorists are now forced to rethink the established premises of state legitimacy and relations between citizens and the state. In that regard, cyber sovereignty is both a practically salient issue of policy and a conceptual problem that compels a re-evaluation of the assumptions that enable us to think about sovereignty, governance and international collaboration in the digital era. (Rosenbach & Chong, 2019) [9]

Evolution of Sovereignty: From Territoriality to the Digital Domain

Sovereignty was conventionally conquered as the absolute jurisdiction of a state over a territory, inhabitants and a legal order, embedded in the Westphalian system that took shape

in the 17th century. This Westphalian concept of sovereignty stressed the sacredness of national frontiers and the judicial monopoly of a state on its territory. Yet, with the beginning of the digital age in the world, these long-established principles were shaken because of the introduction of a non-territorial, yet extremely well-connected space – cyberspace. (Choucri & Clark, 2013) [10] The development of digital technologies has erased the lines that divided the internal and external space and has demanded a re-evaluation of what exactly makes up sovereignty. Control in cyberspace is not only exercised over a physical territory but over data, networks and flows of information that cross traditional boundaries. States are therefore demanding more of the right to control and protect these online spaces, which is creating the notion of cyber sovereignty. It is an extension of the conventional understanding of the concept because it includes technological infrastructure and cyber norms as tools of sovereign power and introduces a rearrangement of power relations in international relations. With states adjusting to the throttling pace of digital technologies, the legal and political foundations of sovereignty are being redefined, and the traditional territorial prerogative is being intertwined with the necessity to exercise control over a constantly growing digital environment. Cyber sovereignty is a notion which exists not only in the realm of politics and law but also in the realm of the major theoretical discussions. A number of international relations theory schools of thought provide different explanations for the emergence and implications of cyber sovereignty, and they include realism, constructivism, and sovereigntist theory. (Hassid & Matania, 2024) [11].

1. Cyber Sovereignty and Realism

With its emphasis on power, security and anarchy of international relations, realism offers an effective way to think about cyber sovereignty as the means to ensure national security and political independence of states in a world that is becoming progressively interconnected. According to realists, cyberspace (as well as any other area of international rivalry, such as land, air, and sea) has turned into an arena of state power. (Valeriano, 2018) [14] This perception of cyber sovereignty is a tool through which states control their digital infrastructure to avoid outside interference, provide security and safeguard national interests, especially against cyber threats and worldwide technological domination. As an illustration, governments such as China and Russia have come up with stringent internet governance policies to ensure that their cyber boundaries are safe and that they are not exposed to foreign influences. (Isnarti, 2016) [13]

2. Constructivism and Cyber Sovereignty

In its turn, constructivist theory puts more emphasis on the importance of social constructs, ideologies, and identities in determining international behaviour. In that regard, cyber sovereignty is not merely a reaction to material threats, but it is profoundly impacted by the identity of a state and its values as well as its ideological approach towards governance. Constructivists can advance the claim that the exercise of cyber sovereignty is a manifestation of the urge of a state to define its identity within the international system, especially regarding the question of digital freedom, state authority, and political legitimacy. Accordingly, cyber sovereignty is influenced by the ideologies and principles of a specific political regime, be it authoritarian or democratic, and, therefore, it is defined differently, depending on the ideological inclination of a state. (Pandey, 2024) [15]

3. Sovereigntist Theory and Cyber Sovereignty

The concept of cyber sovereignty is closely related to sovereigntist theory, which proposes the supremacy of the state within its territorial boundaries. According to this theory, the state as the highest order is required to be in complete control of its territory, including cyberspace. One of the arguments presented by sovereigntist academics is that the concept of sovereignty has to be applied to the virtual realm in the digital age, where the circulation of data, communication lines, and technology infrastructure is viewed as almost an extension of state power. (Petallides, 2012) [16] In this perspective, control and management of the internet by the state is imperative in preserving order, security, and cultural integrity within its boundaries. Such states as India and Russia have been pursuing a policy according to the Sovereigntist theory, promoting data localization and content regulation and challenging foreign access to national cyberspace. (Leal, 2023) [12]

Global Comparative Perspectives on Cyber Sovereignty

Cyber sovereignty is understood and applied variably by different political systems based on their ideological interests, governing principles, and strategies. The present section provides a comparison of cyber sovereignty frameworks of the four key global actors, including China, Russia, the United States, and the European Union, which have quite distinct approaches to state control, digital rights, and internet governance.

China: The Authoritarian Sovereign Model

China offers the clearest and most bellicose vision of cyber sovereignty that is based on an authoritarian philosophy of governance in general. Chinese state The Chinese state regards cyberspace as a sovereign territory equivalent to physical space. China uses strict censorship, surveillance, and access control systems through its Great Firewall. The 2017 Cybersecurity Law localizes and increases the restrictions on foreign technological firms and allows for the extensive monitoring of digital activity by state organs. China's cyber sovereignty practice is informed by the concept of internet sovereignty expounded in its official policy papers that claim that individual states should be allowed to regulate their cyberspace according to their national laws and national interests. (Sterling, 2018) [18]

Russia: Sovereign Internet and Digital Nationalism

The Russian version of cyber sovereignty is also authoritarian but influenced by national security issues and anti-Western attitudes. By creating its national internet infrastructure, Runet, Russia will be able to protect itself against foreign influence and possible cyberattacks. The Sovereign Internet Law of 2019 allows the government to sever the Russian internet connection to the global network in case of emergencies and concentrates the traffic control. (Shandler, 2025) [19] Another example of Russian digital nationalism is attempts to popularize local alternatives to Western services, including VKontakte (VK) instead of Facebook and Yandex instead of Google, which solidifies not only informational control but also technological independence. (Tavenner, 2022) [17]

United States: Liberal Democratic Model and Multi-Stakeholder Governance

Historically, the United States, on the contrary, advocates a liberal, open, and decentralized model of cyberspace governance. It promotes a multi-stakeholder approach, involving governments, the corporate world, civil society, and the technical communities in Internet governance. This open spirit is found in institutions such as ICANN or forums such as the Internet Governance Forum (IGF). Although certain national security initiatives (particularly since 9/11 and considering Chinese technological influence) have resulted in more regulation and surveillance (e.g., via the PATRIOT Act and NSA programs), the U.S. continues to oppose the complete localization of data or centralized state power to determine the contents of digital communications. Nevertheless, discourses of data privacy, misinformation, and platform regulation have led to an increased domestic discussion of the boundaries of digital freedom.

European Union: Regulatory Sovereignty

The European Union is a distinctive prototype of regulatory sovereignty, which is based on the foundations of democracy and strong institutionalization. The EU therefore exercises its sovereignty not by occupation or even monitoring but by law and regulation. The General Data Protection Regulation (GDPR) is a seminal law statement that claims user data rights and international accountability. In the same line of thought, the Digital Services Act (DSA) and Digital Markets Act (DMA) aim to bring attention to transparency, accountability of the platform, and healthy competition in the digital market. The EU model balances fundamental rights and state power and advocates the human-centric approach to digital governance. (Lambach & Monsees, 2024) [20]

Comparative Overview

Country/Region	Governance Model	Key Features	Sovereignty Mechanism
China	Authoritarian Sovereign	Great Firewall, Cybersecurity Law	Strict censorship, state surveillance
Russia	Digital Nationalism	Runet, Sovereign Internet Law	Network isolation, national control
USA	Liberal Multi-Stakeholder	ICANN, minimal data localization	Open Internet, industry-led governance
EU	Regulatory Sovereignty	GDPR, DSA, DMA	Legal regulation, user rights protection

This international comparison indicates an increasing division of cyberspace in competing versions of digital governance, each of which embodies varying conceptions of state power, state sovereignty, and the public good in the digital age.

India's Emerging Position on Cyber Sovereignty

India's approach towards cyber sovereignty is complicated, dynamic, and context-specific and is pegged on its democratic principles, development agenda, and national security imperatives. As much as it may not be on the same grid with the authoritarian approaches to cyber control like in China or Russia, India also does not conform to the liberal, laissez-faire approach that has long been the domain of the United States. Rather, India is bracketed, becoming more of a hybrid or middle-path approach, in which it claims digital sovereignty but also remains committed to openness, innovation, and international collaboration. The cyber governance system of India is built around the Information Technology Act (2000), which establishes the legal basis for controlling electronic commerce, cybercrimes, and cybersecurity in India. (Chaudhary, 2023) [21] In the course of time, India has been augmenting its arsenal of legislative instruments by presenting the Digital Personal Data Protection Bill, the first-ever endeavour to control the privacy of data, rights of users, and responsibilities of compliance on local and foreign parties. At the same time, such flagship programs as Digital India have increased the pace of development, inclusion, and delivery of services through digital infrastructure, making India an important participant in the global digital economy. (Tyagi, 2024) [22] Cybersecurity, data governance, and implementation of regulations in India are done through institutionalized mechanisms, including CERT-In (Indian Computer Emergency Response Team) and the Ministry of Electronics and Information Technology (MeitY). Nonetheless, ongoing in India are issues concerning a conflict between national security and individual digital rights, especially amidst surveillance, internet shutdowns, and platform regulation. The necessity to develop the economy with the help of digitalization regularly comes into conflict with the issues of foreign technological dominance and data sovereignty. At the global level, India is playing an active role in multilateral forums like the Internet Governance Forum (IGF) and G20 Digital Economy Working Group and has been emphasizing the need to have inclusive, democratic, and secure Internet governance. As India keeps increasing its international cyber presence, its strategic alignment as a cyber-sovereign democracy could serve as a possible example to other emerging economies balancing in the same digital quandary. (Bhavika, n.d.)

Cyber Sovereignty: Challenges and Policy Directions

Claims of cyber sovereignty raise perplexing legal and political issues as states struggle with the transnational attribute of cyberspace. One of these issues is jurisdiction and how national laws can be applied when digital operations are border-crossing and include multinational technology companies. This legal ambiguity is further complicated by the increasing phenomenon of internet fragmentation, in which nations are constructing digital boundaries around themselves via data localization legislation, national intranets, and content policing, creating a fragmented global internet, or splinternet. These actions are a challenge to the original vision of the free, open, and interoperable Internet. At the same time, cyber sovereignty brings about questions of human rights, especially those that are adjacent to privacy, freedom of expression, and democratic accountability. Mass surveillance, internet shutdowns, and algorithmic controls have been used by both authoritarian governments and democracies, establishing ethical conflicts about the power of the state in the digital environment. Additionally, the superpower of privately-owned technological giants like Google, Meta, and Amazon, among others, brings about additional issues, since their transnational power regularly overshadows the controlling abilities of the separate nations. Increasing risks of cyber warfare, such as state-sponsored hacking and

disinformation, highlight cyberspace as an unstable strategic layer with no agreed-upon rules. Such issues indicate the necessity of a binding global cyber norm and multilateral governance structures immediately. Although some forums, such as the UN GGE and IGF, provide an arena to discuss the issue, tangible international agreements are yet to be made. National cybersecurity strategies, legal frameworks, and capacity building: This is needed especially in emerging economies. Such is the divide between digital authoritarianism and digital democracy that demands a normative reckoning as well. In the Global South, countries such as India, Brazil, and South Africa, cyber sovereignty represents a possibility to influence a balanced governing approach that would correspond to democratic principles and the interests of development. The future transformation of this dynamic with the implementation of AI, quantum computing, and 5G, among other technologies, will require states to consider future-looking, rights-based, and ethics-driven cyber policies.

Conclusion

The topic of cyber sovereignty presents a picture of depth and conflict where more and more states are attempting to exercise their dominance in the digital arena according to their national interests, laws, and political philosophies. In this study, we have highlighted the conceptual transformation of cyberspace as a global common to cyberspace as a space of strategic concern—a place where sovereignty, security, and regulation meet. The qualitative analysis of the models used in the world, the authoritarian control of China, the regulatory sovereignty of the European Union, and the hybrid system of India proves that there is no dominant model. Rather, states manoeuvre between transparency and command, creativity and censorship, and autonomy and dependence. The very logic of cyber sovereignty is quintessentially state-based and focused on the territorial principle of jurisdiction, data localization, and cyber self-determination. However, these methods tend to go against the transnational quality of cyberspace and bring up issues of human rights, internet fragmentation, and the unregulated power of private tech monopolies. The article is relevant to and can add value to the academic and policy discussion as it signals the importance of a more differentiated and pluralistic view on cyber governance, one that can reconcile differences in political systems without disrupting the openness and interoperability of the global internet. With the further evolution of digital technologies, which is happening with the implementation of AI, quantum computing, and 5G, there is an increasing urgency to create inclusive, rights-respecting, and cooperative governance frameworks. Such a mediated position between national sovereignty and the ideals of global digital commons is quite desirable, if not necessary. The voices and strategies of the Global South and the influence of regional coalitions in building cyber norms should be given attention in future studies, as well as the ethical aspects of developing technologies in sovereign digital ecosystems. It is a time when digital borders are beginning to shape geopolitical borders, and the question is how to create bridges, not walls, and how cyber sovereignty does not become the cost of free, secure, and open internet to everyone.

References

1. Pierucci F. Sovereignty in the digital era: Rethinking territoriality and governance in cyberspace. Deleted Journal, 2025, 4(1). https://doi.org/10.1007/s44206-025-00189-4
2. Gupta S, Sony R. Quest of data colonialism and cyber sovereignty: India's strategic position in cyberspace. Legal in the Digital Age,2021:2(2):70–81. https://doi.org/10.17323/2713-2749.2021.2.68.81
3. Leiter A. Cyber sovereignty: A snapshot from a field in motion. Harvard International Law Journal, 2023. https://journals.law.harvard.edu/ilj/2020/04/cyber-sovereignty-a-snapshot-from-a-field-in-motion/
4. Ördén H. Securitizing cyberspace: Protecting political judgment. Journal of International Political Theory,2021:18(3):375–392. https://doi.org/10.1177/17550882211046426
5. Lacy M, Prince D. Securitization and the global politics of cybersecurity. Global Discourse,2018:8(1):100–115. https://doi.org/10.1080/23269995.2017.1415082
6. Lahmann H. On the politics ideologies of the sovereignty discourse in cyberspace. Duke Journal of Comparative International Law,2021:32:61–107. https://scholarship.law.duke.edu/djcil/vol32/iss1/2
7. Corn GP, Taylor R. Sovereignty in the age of cyber. AJIL Unbound,2017:111:207–212. https://doi.org/10.1017/aju.2017.57
8. Schmitt MN, Vihul L. Sovereignty in cyberspace: Lex lata vel non? AJIL Unbound,2017:111:213–218. https://doi.org/10.1017/aju.2017.55
9. Rosenbach E, Chong SM. Governing cyberspace: State control vs. the multistakeholder model. The Belfer Center for Science International Affairs, 2019. https://www.belfercenter.org/publication/governing-cyberspace-state-control-vs-multistakeholder-model
10. Choucri N, Clark DD. Who controls cyberspace? Bulletin of the Atomic Scientists,2013:69(5):21–31. https://doi.org/10.1177/0096340213501370
11. Hassid N, Matania E. A global regime for cybersecurity the obstacles to future progress. Global Governance: A Review of Multilateralism International Organizations,2024:30(1):13–40. https://doi.org/10.1163/19426720-03001002
12. Leal A. Beyond boundaries: The geopolitics of cyberspace. Kuppinger Cole, 2023. https://www.kuppingercole.com/events/cyberevolution2023/blog/beyond-boundaries-the-geopolitics-of-cyberspace
13. Isnarti R. A comparison of neorealism liberalism constructivism in analysing cyber war. Andalas Journal of International Studies (AJIS),2016:5(2):151–165. https://doi.org/10.25077/ajis.5.2.151-165.2016
14. Valeriano ACaB. Realism cyber conflict: Security in the digital age. E-International Relations, 2018. https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age
15. Pandey K. Chinese notion of cyber sovereignty: Building an alternate digital order. Observer Research Foundation, 2024. https://www.orfonline.org/english/expert-speak/chinese-notion-of-cyber-sovereignty-building-an-alternate-digital-order
16. Petallides CJ. Cyber terrorism and IR theory: Realism liberalism and constructivism in the new security threat.

Inquiries Journal, 2012. http://www.inquiriesjournal.com/articles/627/cyber-terrorism-and-ir-theory-realism-liberalism-and-constructivism-in-the-new-security-threat
17. Tavenner E. Russian cyber sovereignty: Global implications of an authoritarian RuNet. American University, 2022. https://www.american.edu/sis/centers/security-technology/russian-cyber-sovereignty.cfm
18. Sterling B. Meanwhile in Chinese sovereign cyberspace. WIRED, 2018. https://www.wired.com/beyond-the-beyond/2018/01/meanwhile-chinese-sovereign cyberspace
19. Shandler. Reassessing RuNet: Russian internet isolation implications for Russian cyber behavior. Atlantic Council, 2025. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/reassessing-runet-russian-internet-isolation-and-implications-for-russian-cyber-behavior
20. Lambach D, Monsees L. Beyond sovereignty as authority: The multiplicity of European approaches to digital sovereignty. Global Political Economy,2024:1–18. https://doi.org/10.1332/26352257y2024d000000007
21. Chaudhary PK. India's cybersecurity diplomacy: Building global alliances. ShodhKosh Journal of Visual Performing Arts, 2023, 4(2). https://doi.org/10.29121/shodhkosh.v4.i2.2023.3386
22. Tyagi S. A critical assessment of the Digital Personal Data Protection Act in light of the GDPR framework. IJALR, 2024. https://ijalr.in/volume-4-issue-3/a-critical-assessment-of-the-digital-personal-data-protection-act-in-light-of-the-gdpr-framework-sunidhi-tyagi
23. Bhavika. Analysis of cyber law with focus on data protection. Legal Service India, n.d. https://www.legalserviceindia.com/legal/article-7490-analysis-of-cyber-law-with-focus-on-data-protection.html