Lahore Institute for Research and Analysis Journal
ISSN: 3007-2700 (Online); 3007-2719 (Print)

Volume 3, 87-104, 2025
© 2025 The University of Lahore

# Cyber Sovereignty: National Security in the Digital Age

Noureen Akhtar[1], Dr. Abdul Rauf Iqbal[2]

[1] *PhD Scholar, Quaid-i-Azam University Islamabad, Pakistan.*
[2]*Senior Research Scholar, National Defence University, Islamabad, Pakistan.*

*Corresponding Author: [2]abdulraufiqbal@gmail.com*

Received: 04-12-2024 Revised: 16-01-2025 Accepted: 22-01-2025 Published: 04-02-2025

Suggested Citation: Noureen Akhtar, Abdul Rauf Yousaf "Cyber Sovereignty: National Security in the Digital Age." *Lahore Institute for Research and Analysis Journal* 3 (2025): 87–104.

***Abstract -*** *In an era of increasingly sophisticated cyber threats, cyber sovereignty has become the latest fad as states seek to assert control over their digital domains. This paper explores how each of these leading nations is navigating the complex landscape of cyber sovereignty to safeguard national security, including China, Russia, the United States, and the European Union. States like China and Russia, with strict cyber regulations, have managed to curb data flows, track Internet activities, and cap foreign influence through the sovereignty of cyberspace as a tool of state surveillance and censorship. However, such actions are difficult to do, especially in democratic countries, in the presence of the European Union's GDPR and the US CLOUD Act. This paper investigates the ethical implications resulting from the domination of a state over cyberspace, especially in authoritarian regimes. It discusses the economic impact of local laws, which limit international trade and digital innovation. Fragmentation in the digital space is already leading to warnings about the future of an open internet at a time when more nations are promoting sovereignty over cooperation. An international cooperation, international norms on cyber, and a public-private partnership to enhance the resilience of cybersecurity would be good ways forward in addressing the challenges and gaps identified above. It is argued that national security, global digital cooperation, and individual rights should be balanced in such a way that cyberspace should be safe yet open for everybody.*

***Keywords - Cyber sovereignty, data localization, cybersecurity, and privacy vs. security, digital governance, and international cooperation***

## 1. Introduction

Cyber sovereignty will increasingly feature as a new ingredient in the globalized world with respect to how states exercise and secure their digital space. Cyber sovereignty is nothing but the nation's rights over control and management of the internet in its territory as the latter has the power over the land. This resonates with the right of a state to decide its digital infrastructure, maintain cybersecurity, and protect the citizen's information from external threats. The pace at which this technology is evolving has perhaps never been so pressing towards the need for the security of a country's electronic frontier. Cyber warfare and cyber espionage, and to some extent, state sponsored hacking, have made cyber space a new strategic playground like land, sea, air, and outer space. Today, states understand that sovereignty extends into the cyber world and that protection of this sphere is important for the realization of national security.

Where virtual platforms are increasingly being used for communication, commercial transactions and the management of infrastructure, cyber sovereignty is a very special concern[1]. Yet another deeper underlying significance: as the world at large becomes increasingly dependent on such technology, so too do the dangers of it. It not only refers to the physical borders of different countries but also digital intrusions that bring disruption to national economies, compromise sensitive information, and can indeed influence political outcomes. This is exacerbated by the transnational nature of the internet, where data freely flows across borders, hence difficult for any country to fully control the digital environment of its citizens.

### 1.1 National Security in the Digital Age

National security is soon turning out to become a staple matter that policy-makers throughout the globe will concentrate upon.[2] In this digital era, what one perceives as national security becomes transformed from protection of actual or physical resources to covering attributes of an electronic infrastructure coupled with data integrity for a nation. Alteration in its nature form from the very traditional and conventional form of warfare, cyber warfare brought a total twist to this entire idea of national defence. For example, cyber-attacks targeting some critical infrastructures such as power grids or financial systems may make the entire country freeze up but not shoot a single bullet. So it has significantly invested in cybersecurity to protect its people and their interests at the national level.

But the pursuit of cyber sovereignty brings along its own set of problems. The Internet was to be an open borderless network and freedom of information flow and openness were to be fostered within it. Most often it is at the cost of national controls over cyberspace that the ideals of Internet freedom and openness replace security interests in the run of things. It is where tension has been most palpable, especially in countries whose governments employed the rhetoric of cyber sovereignty to push censorship and surveillance well beyond what could be practically managed of dissent and access to information[3]. In parallel, states do support the right of cyber sovereignty as a legitimate means toward guaranteeing national security in an era where cyber threats have proliferated and grown sophisticated.

### 1.2 Research Question

This paper tries to analyze *how the concept of cyber sovereignty influences national security*? Which challenges and strategies go along with it? Elucidating this, the research analyzes how different nations apply their cyber sovereignty approach further and analyzes the capability such approaches would have in combating cyber threats and in enlarging how it would influence international internet governance. The aim is to find if the exercise of cyber sovereignty can be compatible with principles of free and open Internet or leads to more fracture and digital authoritarianism automatically. This paper goes deep into how cyber sovereignty changes the dynamics in the domains of national security and discusses whether it makes national security more or less robust. The paper shall outline theoretical foundations underpinning cyber

[1] Mueller, Milton L. "Against sovereignty in cyberspace." *International studies review* 22, no. 4 (2020): 779-801.

[2] Zeeshan; Bilal, A. Ahmed; Munib, Werdah; Zaighum, "The Media-Policy Nexus: Analyzing the Media's Role in Policy Formation in Pakistan," *Lahore Institute for Research and Analysis Journal* 2 (2024): 24–34.

[3] ÜNVER, H. Akin. "Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights."

sovereignty, its applications across different global geopolitical contexts, and then proceed to case studies on states testing out the relationship between security and openness in the cyber context.

## 2. Theoretical Framework

Cyber sovereignty draws, in its very essence, from the concept of state sovereignty under the Westphalian model wherein each country has exclusive jurisdiction over its territory and sovereign right to govern without interference by external parties[4]. This had been applied traditionally to borders in the physical world but has since been extended to cyberspace because states have recognized the strategic value of the control of cyberspace. Cyber sovereignty thus represents a shift from the initial vision of the Internet as borderless, decentralized, free, and open communication to a more fractured digital space where states attempt to regain control over their national cyberspaces.

From a theoretical standpoint, cyber sovereignty is in step with realist theories of international relations, which emphasize the sovereignty and national interest of the state. It is the view that security trumps everything in an anarchic international system, meaning the state will seek to claim ownership of any domain through which a threat could arrive or be transmitted, which now includes cyberspace[5]. This is even more so in the cases of China and Russia, which view an unfettered internet as an opportunity for regime instability or national security to be threatened.[6] In these regards, liberal theories support global cooperation and collective governance views of the internet as representing a global commons that deserves to be managed through multi-stakeholder approaches involving governments and private sector entities as well as civil society.

### 2.1 Contrasting Theoretical Concepts: Cyber Diplomacy, Internet Governance, and Digital Sovereignty

For one to really understand how subtle cyber sovereignty is, one must look into how it differs from other notions:

- *Cyber diplomacy* is the process through which diplomatic channels are used to set norms, agreements, and cooperation in cyberspace. This is a different approach from cyber sovereignty since the latter is unilateral in contrast to cyber diplomacy, whose basis is constructivist theory that emphasizes the role of international institutions, shared norms, and collaborative frameworks that promote stability[7]. In such a manner, the UN Group of Governmental Experts sought to establish standards of responsible conduct by the states in cyberspace while helping initiate a dialogue between states toward mutual understanding[8].

- *Internet governance* is a concept founded on liberal institutionalism that enforces a multi-stakeholder approach to the management of the internet's technical infrastructure through cooperation between governments, private entities, and non-governmental organizations[9]. This, by far, is in opposition to cyber sovereignty, wherein the state controls Internet

[4] Stavridou, Vaia. "Balancing Sovereignty and Integration: Digital Policy Dynamics in the European Union." (2024).

[5] Zinovieva, Elena, and Sergey Shitkov. "Sovereignty as Practice in Digital Age." In Digital International Relations, pp. 75-90. Singapore: Springer Nature Singapore, 2023.

[6] Syed Raghab Ali and Ishtiaq Ahmed Chaudhri, "CPEC-A Flagship of New Silk Road: Perceptions of 'Sinophilia' and 'Sinophobia' in Pakistan *," *Journal of Political Studies* 25, no. 2 (2018): 155.

[7] Attatfa, Amel, Karen Renaud, and Stefano De Paoli. "Cyber diplomacy: A systematic literature review." Procedia computer science 176 (2020): 60-69.

[8] Meyer, Paul. "Norms of responsible state behaviour in cyberspace." The ethics of cybersecurity (2020): 347-360.

[9] Neyer, Jürgen. "After global governance: Technological innovation and the new politics of sovereignty in internet governance." Zeitschrift für Politikwissenschaft 32, no. 2 (2022): 361-382.

resources. The theoretical underpinning of internet governance is that a free and open internet contributes to economic growth, innovation, and human rights. However, with data localization laws and national regulations on the rise, it can be claimed that the trend between global governance and state-centric control is in conflict.

- *Digital sovereignty* is more than control over cyberspace; it encompasses data privacy, digital infrastructure, and technological self-sufficiency. It is also connected to neo-mercantilist theories, which emphasize economic protectionism, with state control over basic resources[10]. For instance, the General Data Protection Regulation of the European Union[11] manifests its commitment to digital sovereignty in safeguarding citizens' data from the external surveillance and control mechanism.

### 2.2 Legal and Policy Perspectives: Application of Theoretical Framework to Cyber Sovereignty

The theoretical postulates of cyber sovereignty are precisely implemented in the different frameworks of law and national policies directed toward the assertion of control by the state over cyberspace. Usually, the legal and policy choice of the states mirrors the cyber sovereignty-global internet freedom dichotomy.

- *Realism and the Pursuit of Cyber Sovereignty*: It is within the realist paradigm that states think that the cyber-control holds the solution to national security[12]. In this respect, Russia had enacted the Sovereign Internet Law wherein if they fear threats or danger they have the option of disengaging from the global net. Once more, a very tight noose Chinese Cyber security law had undertaken in regard to foreign technologies forcing data localisation strictly to save their national interest.

- *Liberalism and Global Internet Governance:* Liberal theories contend that states should collectively work toward establishing international guidelines for cyber governance. One example of such an agreement is the Budapest Convention on Cybercrime[13], which works to harmonize border-crossing laws toward regulating cybercrime but opening up the internet. In this regard, the convention has faced opposition from the likes of China and Russia, as they interpret cyber sovereignty in line with a state-led approach.

- *Constructivism and Cyber Diplomacy:* This category considers norms shared, and dialogue as essential constructs in cyberspace. The efforts developed by the Paris Call for Trust and Security in Cyberspace[14], which strives to outline norms around states' conduct in cyber space, give evidence of contribution from non-state actors together with international

[10] Huotari, Mikko, Jan Weidenfeld, and Claudia Wessling. "Towards A “Principles First Approach” In Europe’s China Policy." Drawing lessons from the Covid-19 crisis. MERICS–Mercator Institute for China Studies 9 (2020).

[11] Chalmers, Damian, Gareth Davies, Giorgio Monti, and Veerle Heyvaert. European Union law: text and materials. Cambridge university press, 2024.

[12] Weber, Valentin. "The diffusion of cyber norms: technospheres, sovereignty, and power." PhD diss., University of Oxford, 2021.

[13] Polyzoidou, Vagia. "Combatting the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime." In EU Internet Law in the Digital Single Market, pp. 355-375. Cham: Springer International Publishing, 2021.

[14] Lété, Bruno. Paris Call and Activating Global Cyber Norms. German Marshall Fund of the United States., 2022.

cooperation towards cyber policies and not unilateral, where only cyber sovereignty will be underscored.

| Theoretical Approach | Key Principles | Real-World Application |
|---|---|---|
| *Realism* | - State-centric control, national security | - China's Great Firewall, Russia’s Sovereign Internet Law |
| *Liberalism* | - Cooperation, multi-stakeholder governance | - Budapest Convention, Internet Governance Forum |
| *Constructivism* | - Norms, shared values, cyber diplomacy | - UNGGE, Paris Call for Trust and Security |
| *Neo-Mercantilism* | - Economic protectionism, digital autonomy | - EU’s GDPR, India’s Data Protection Bill |

The above theoretical frameworks form the basis for understanding divergent approaches to cyber sovereignty and their ramifications for national security. Realism, emphasizing state control, closely identifies with the actions of authoritarian regimes that will seek to secure their frontiers digitally. On the other hand, liberal and constructivist models suggest that a more multiparty model is better apt to promote greater global internet freedom.

## 3. Key Dimensions of Cyber Sovereignty

The argument has it that the digital age has elevated the issue of cyber sovereignty core in a country's mission to address regulation of cyberspace and realization of national security. Cyber sovereignty reflects an assertion of the right of nations to govern and exercise control over the internet inside their borders, thus constituting an extension of the Westphalian concept of territorial sovereignty in the digital space[15]. But, at the national level, such a stand encounters huge challenges posed by necessities that have to be balanced against the compulsion to interconnect countries. The gulf between that which an authoritarian government succeeds in getting as compared with a democratic government in this effort at trying to make amends for security flaws on this cyber sovereignty will make it harder to solve. Thus, understanding these dimensions becomes indispensable when the question of how states address the increasingly complicated cyber space arises and especially about the changing threat from states and non-state actors.

This is where exercising cyber sovereignty appears needed more than ever given rising threats to national security through cyber spying, cyber terrorism, and virtually all forms of electronic violence. When it seeks control over cyberspace and enhanced national security in the process, it poses rather serious problems for open internet, multilateralism, and all those fundamental challenges of connection globally.

Cyber sovereignty is not then a matter of policy it is a statement of the strategic intent of a country. For authoritarian regimes it is consequently of the utmost priority to establish dominance in cyberspace as the foundation for regime stability when democratic nations struggle to determine that balance of security and civil liberties[16]. They also require a reminiscence of the advancing

[15] Branch, Jordan. "Territory, sovereignty and boundaries in digital battlespace." Research Handbook on Cyberwarfare (2024): 301-315.

[16] Babb, Casey. "Digital Dictators: How Different Types of Authoritarian Regimes Use Cyber Attacks to Legitimize Their Rule." PhD diss., Carleton University, 2022.

security domino and a devising of a new security paradigm-a cross signal to the need to have complex yet mobile security systems.

### 3.1 National Control vs. Global Connectivity

It's where cyber sovereignty comes from: in the middle of an even that is a typical civil conflict between the state which wants to have some control over the technical structures it relies on and the internet that, by its very nature, is global. It was originally developed with an architectural foundation of openness and decentralization with the belief that information would flow across borders in achievement of the objectives of communication, commerce and development. However, the raised strategic importance of the cyberspace has made the control of one's environment by the states to protect oneself from the outside interferences and guarantee the privacy of information besides sometimes limiting some foreign influences.

This is best captured by the manner in which China applies the Great Firewall which is an elaborate system of filtering content and monitoring use of the internet to regulate information within that country. The Chinese government could then control the content and tone of all messages put up online because the internet will be a tool for enhancing social stability rather than a means for spreading dissent by restricting the website the Chinese have access to and banning certain words or phrases[17]. This is predicated on the premise that structured flows of information constitute a threat to regime stability, especially in the light of the internet that gives vent to social mobilization against authoritarian rule.

On the other hand, the EU appears to safeguard individualism and human rights but does not take into consideration the cybersecurity. For instance, the GDPR requires strict safeguard measures of data that are even collected outside the EU territorial borders but concern EU citizens[18]. This is a data sovereignty and privacy promise without letting go of connection from the internet at all. Contrarily, the Russia Sovereign Internet Law is an isolationist move to be made in 2019 which will let the country unplug itself during emergencies from the rest of the internet[19]. This allows the government to manage internet traffic and block access to servers external to it, under claims of national security. This is where it has placed its authority to suppress dissent and monitor the activities of its citizens on the Internet.

| Country | Cyber Sovereignty Approach | Impact on Global Connectivity |
|---|---|---|
| China | • Strong state control, censorship, data localization | • Limits external access, controls information flow |
| Russia | • Sovereign internet infrastructure, surveillance | • Increases state control, reduces foreign influence |
| European Union | • Data protection with cross-border cooperation | • Balances privacy with connectivity |

[17] Zoetbrood, J. P., E. B. A. van der Vleuten, A. J. Wieczorek, and F. C. A. Veraart. "The Emergence of Another Internet: Studying the Evolution of Chinese Cyberspace through a Large Technical Systems Lens." Innovation (2021).

[18] Veit, Raoul-Darius. "Safeguarding regional data protection rights on the global internet—The European approach under the GDPR." In Personality and Data Protection Rights on the Internet: Brazilian and German Approaches, pp. 445-484. Cham: Springer International Publishing, 2022.

[19] Sayapin, Sergey. "Russian approaches to international law and cyberspace." In Research Handbook on International Law and Cyberspace, pp. 525-546. Edward Elgar Publishing, 2021.

| | | |
|---|---|---|
| United States | • Open internet with targeted cybersecurity | • Promotes innovation while enhancing defense |

These developments indicate the geopolitical effects of cyber sovereignty. Democratic states may embrace such principles of an open Internet, but imperatives to enhance cybersecurity cannot be avoided.

Indeed, in recent years the U. S. has repeatedly signalled the need to protect "soul structures" from cyber threats on the Internet without resorting to general government control of the Net[20]; however, the emerging reality of state-sponsored cybercrime has even liberal democracies questioning their stance toward "data localization" and the "sovereignty in the digital".

### 3.2 Cyber Sovereignty in Authoritarian vs. Democratic States

The application of cyber sovereignty varies markedly between authoritarian versus democratic states, reflecting the larger ideological differences over the appropriate role of the state within information regulation. Authoritarian regimes of China and Russia, for example use cyber sovereignty to strengthen their hands to restrict dissent and control the information[21]. The aim of having full control over their digital spaces through cyber sovereignty is to safeguard them from the ideological influence by others and to minimize the threats of cyber-enabled subversion. In these situations, cyber sovereignty is an extension of their interior security policies rather than a tool of defense policies.

On the other hand, in the democratic systems, protection of civil rights is always under a check with security concerns of a given country. Legal requirements like the one present on EU through GDPR appear highly committed towards safeguarding rights to privacy and enhancing cyber security[22]. While the United States has launched such values as innovation and the open internet, it has developed measures, such as CISA, to support the enhancement of interaction between the public and the private sector when addressing the problem of cyber threats.

While every system has its own set of problems and prospects, more importantly, this is where, despite the authoritarian and democratic state differences, one seems to find similar coinage in addressing cyber espionage, cyber terrorism, and non-state actors.

### 3.3 Challenges to National Security

In fact, this claim of cyber sovereignty is more in relation to issues of national security as earlier hinted. Thus, as cyberspace is gradually transmuting into the world war theatre, cyberspace requires states to defend their information technology systems. The greatest threat is cyber espionage – which is a sophisticated form of attack from state level hackers, who are interested in gaining access to sensitive, corporate, and strategic information. Such events, highly profiled, for instance, the recently attacked SolarWinds hack that was done by Russian operators[23], tell of the vulnerability of a secure network.

Likewise, cyberterrorism threat has risen because non-state players have deployed cyberspace to perpetrate attacks that can cripple structures, create panic or advance agendas. Albeit in recent times, terrorist groups have effectively used the decentralized platforms in the dark web for

[20] Ruohonen, Jukka. "The treachery of images in the digital sovereignty debate." Minds and machines 31, no. 3 (2021): 439-456.

[21] Howells, Laura HC. "Digital Authoritarianism in China and Russia: A Comparative Study." (2020).

[22] Bharti, Simant Shankar, and Saroj Kumar Aryal. "The right to privacy and an implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the companies." Journal of Contemporary European Studies 31, no. 4 (2023): 1391-1402.

[23] Willett, Marcus. "Lessons of the SolarWinds hack." In Survival April–May 2021: Facing Russia, pp. 7-25. Routledge, 2023.

communication, recruiting and fund raising due to near anonymity and therefore making it difficult for the states to deal with them effectively without violating civil liberties. One of the most recent classic cases is the WannaCry ransomware attack[24] which frozen organizations globally by targeting the susceptibility of old systems and underline the importance of stringent, preventive yet robust and flexible cybersecurity measures.

## 4. Case Studies

The actions of the assertion of cyber sovereignty from different countries are coloured with their political, economic and security interests. Authoritarian states like China and Russia use cyber sovereignty to regulate their respective cyber spaces while democratic states like the United States and the European Union are left with a challenge in determining the median between protecting the nation's' cyber space and freedom of Internet use.

### 4.1 China: Leveraging Cyber Sovereignty for Control and National Security

China has been a strong proponent of cyber sovereignty in the sense that it believes control over its digital space is critical to national security and social stability. Since the early 2000s, China built an extremely sophisticated system of internet control that is known as the Great Firewall[25]: limits on access to foreign web sites, filtering of online content, and monitoring activities of citizens. A free Internet poses a threat to the Chinese Communist Party's authority because the manner in which social media implicated the Arab Spring may be just a precursor.

China's Cybersecurity Law had been enacted in 2017-a major step toward tighter regulation of cyberspace and data flows[26]. It mandates data localisation, compelling companies to store locally data collected within China on Chinese servers and granting the government comprehensive powers to access and control its data flows. This move significantly enhances state surveillance capabilities; it also limits the influence exerted by foreign technology corporations like Google and Facebook when they are effectively barred from operating freely in China. Recently, China also clamped down even more in cyberspace with its Data Security Law, effective September 2021, and the Personal Information Protection Law (PIPL), November 2021[27]. Data Security Law categorizes data based upon its sensitivity to national security and has very stringent control over cross-border data transfers. Data transfer which involves any risk on the nation's security shall pass under a review and eventually block through the Chinese Government that leaves the country an Internet world of a 'walled garden'.

Part and parcel of China's expansion, Belt and Road, that pushes at its borders include, of course, its own Belt and Road, called Digital Silk Road[28], aiming for exporting internet control technologies across all regions of the continent such as Africa, Latin America, and Southeast Asia through more solid plans which entail spreading out the Chinese model to bring about an unscathed state control on cyber sovereignty, while enforcing, and ultimately giving a thrust and full endorsement towards China's endeavor towards strengthening its geopoliticaI influence.

[24] Bansal, Urvashi. "A review on ransomware attack." In 2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC), pp. 221-226. IEEE, 2021.

[25] Taylor, Monique. "Building Digital Authoritarianism: From the Great Firewall to the New IP." In China's Digital Authoritarianism: A Governance Perspective, pp. 1-24. Cham: Springer International Publishing, 2022.

[26] Huang, Daoli. Research on the Rule of Law of China's Cybersecurity: China's Rule of Law in Cybersecurity Over the Past 40 Years. Springer Nature, 2022.

[27] Chaskes, William. "The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet." Wash. & Lee L. Rev. 79 (2022): 1169.

[28] Chang, Yung-Yung. "China beyond China, establishing a digital order with Chinese characteristics: China's growing discursive power and the Digital Silk Road." Politics & Policy 51, no. 2 (2023): 283-321.

Critics claim that cyber sovereignty by China strangles innovation, restrains freedom of expression, and raises barriers to international collaboration. Human rights organizations widely condemned aggressive surveillance measures that the Chinese government adopted into its use. Facial recognition and AI monitoring systems are but a few of them.

### 4.2 Russia: Cyber Strategies, Surveillance, and Influence Operations

Like China, Russia believes that cyber sovereignty is a matter of national security and a way to make its presence felt in the global arena. The passage of the Sovereign Internet Law in 2019 was a significant step towards Russia's goal of building a national internet infrastructure that can operate independently of the global web[29]. This enables the Russian government to have a complete control over internet traffic, limit access to the foreign servers and effectively cut off a whole nation from the global internet, in case of crisis.

These steps, the Russian government explains, are aimed at protecting Russia against foreign cyber threats-most of them coming from the West. The Sovereign Internet Law, to critics, is an attempt primarily to maximize state control over information and to minimize dissent. A great number of these measures did indeed add up to government surveillance capacities-for instance, the Yarovaya Law, passed in 2016, stipulates that communications firms store all user information for up to six months and make them available to scrutiny by security agencies[30]. Russia has been directly involved in cyber operations across national borders. Indeed, it has been associated with Russian state-sponsored hackers conducting influence operations during the 2016 United States' presidential election as an attempt to destabilize and weaken the basis for democratic institutions[31]. Recent ones relate to Russia's attacks involving critical infrastructure in Ukraine regarding Ukrainian electric power grids and other parts of the communications system.

The NotPetya malware attack by Russian hackers in 2017 resulted in billions of dollars in damages across the globe and proved that Russia was willing to use cyber tools as part of its overarching geopolitical strategy[32]. This emphasis on cyber sovereignty by Russia brings with it its economic and social implications. The isolation of the internet infrastructure may lead to subpar technological innovation, restriction of exposure to global information, and isolation of the tech-savvy younger generation.

### 4.3 United States and European Union: Balancing Cybersecurity and Internet Freedom

China and Russia opted for an autocratic approach while the United States and the European Union are more likely to strike a balance of cybersecurity and internet openness. The updated 2023 U.S. National Cybersecurity Strategy is focused on cooperation with the private sector in keeping the critical infrastructure immune from cyber-attacks while maintaining internet openness and openness[33]. This reflects a commitment by the U.S. to internet freedom, but growing concerns over foreign interference and cybersecurity have led to increased regulation on technology firms, with particular attention to Chinese companies like Huawei and TikTok.

[29] Thumfart, Johannes. "The Construction of Digital Sovereignty in Struggles for Recognition." In The Liberal Internet in the Postliberal Era: Digital Sovereignty, Private Government, and Practices of Neutralization, pp. 55-140. Cham: Springer Nature Switzerland, 2024.

[30] Khusnetdinova, Agdaliya, and Peng Wang. "Rethinking the Principle of Cyber Sovereignty: Key Takeaways from China and Russia." Available at SSRN 4690571.

[31] McMasters, Daniel H. "Subversive Influence: Vulnerabilities of The United States And Its Elections to Russian Interference Campaigns." PhD diss., Monterey, CA; Naval Postgraduate School, 2020.

[32] Krasznay, Csaba. "Case study: The notpetya campaign." Információés kiberbiztonság (2020): 485-499.

[33] Medcalfe, David. "Critical Infrastructure in the Face of Global Cyber Threats." (2024).

However, the European Union has been very proactive on questions of data privacy and digital rights. Since 2018, there exists a law called the General Data Protection Regulation that lays down severe requirements concerning protection and data privacy[34]. Such regulation about personal data secured in an EU citizen incurs stiff penalties on organizations around the globe if they disregard the rule of the law. Recent legislative measures of the EU regarding digital sovereignty include the Digital Services Act and the Digital Markets Act[35], which were lately adopted to introduce a safer digital environment while ensuring fair competition.

Though the U.S. and the EU have both been focusing on openness, they also have realized the need to secure their cyberspace due to the growing threat of state and non-state actors. The Russian hackers attack on SolarWinds in 2020 exposed the vulnerability of the U.S. government networks, prompting policy review on cybersecurity[36]. Similarly, the EU has also been concerned with the spreading of disinformation mainly by Russia, and efforts to stop foreign influence operations are ongoing.

## 5. Policy Implications

As the cyber threats change, most nations increase attempts toward achieving cyber sovereignty through policies and regulatory frameworks. National security concerns drive the assertion of cyber sovereignty, but this influence global cyber norms, data flows, and internet governance. Therefore, understanding the balance between the need for security with principles of openness and cooperation in the digital world means taking on the implications of such policy effects.

### 5.1 Existing Policies and Frameworks

- **The European Union’s General Data Protection Regulation (GDPR)**

Perhaps the most comprehensive data protection legislation globally, the General Data Protection Regulation was introduced in 2018[37]. It was implemented in the hopes that citizens in the European Union will be given a sense of ownership over their personal information while imposing rigid regulations on the companies handling, storing, or processing such information. The extraterritorial application of the GDPR extends its applicability to any company that handles the data of a resident of the EU, irrespective of the company's location.

The GDPR has set a world standard for data privacy and countries like Brazil and India have actually moved forward to adapt their domestic privacy laws within the EU model. For instance, Brazil's Lei Geral de Proteção de Dados or LGPD, introduced in 2020, is essentially similar in provisions to that of the GDPR. As much as the GDPR tries to shield individual privacy, it, on the other hand creates problems for tech firms because high compliance costs.

From the perspective of cyber sovereignty, the GDPR restates the EU commitment to digital sovereignty, considering that data produced under its borders falls under EU control. This is essentially towards protecting its citizens against surveillance by foreign powers. In any case, other people are against data localization by saying it is becoming the cause of the globalization internet

[34] Fiero, Anna Wright, and Elena Beier. "New global developments in data protection and privacy regulations: Comparative analysis of European Union, United States, and Russian legislation." Stan. J. Int'l L. 58 (2022): 151.

[35] Akman, Pinar. "Regulating competition in digital platform markets: A critical assessment of the framework and approach of the EU Digital Markets Act." (2021).

[36] Fey, Laura Clark, and Sarah D. Wiese. "America the Vulnerable: The Nation State Hacking Threat to Our Economy, Our Privacy, and Our Welfare." Kan. JL & Pub. Pol'y 30 (2020): 370.

[37] Булгакова, Валентина Анатоліївна. "The compliance of facial processing in France with the article 9 paragraph 2 (a)(g) of (EU) general data protection regulation." Наукові записки НаУКМА. Юридичні науки 11 (2023): 64-76.

fragmentation. Localization requirements indeed hinder innovation and create barriers on the free flow of information.

- **Russia's Data Localization Laws**

Russia has taken a more limited approach toward data control to assert its cyber sovereignty, in contrast to the EU approach. Russia passed the Data Localization Law in 2015[38], which requires all personal data of Russian citizens to be kept on local servers. It aims to limit dependence on foreign technology and protect itself from external cyber threats, particularly from the West.

The data localization requirements help the Russian government monitor and control the inflow of information. The law allows state agencies to access data stored in Russia, thus strengthening the capacity of state surveillance. For the last couple of years, the Russian government has increased efforts to implement these regulations; it blocked LinkedIn and even penalized Google and Apple for failure to comply. These critics believe nothing more of it as a strategy to silence the public, to reduce content access from foreigners and to reign supreme over the internet.

In this case however, economic implications are rather significant. Local data centers which have to be set up increase the cost of operation for international companies, thereby discouraging foreign investment in Russia's digital economy. Data localization can also be detrimental to cross-border data transfer, and therefore harm international digital trade.

- **China's Cybersecurity and Data Protection Laws**

In comparison, the approach that China is taking towards cyber sovereignty could maybe be seen as the most sustainable among all the main powers. China's Cybersecurity Law of 2017 and Data Security and Personal Information Protection Law of 2021 are highly developed to regulate its cyberspace for the state[39]. Those pieces of legislation will mandate highly sensitive requirements for data localization, grant the government broad discretionary authority to surveil data communications, and sort data based on how they affect national security.

Currently, cyber sovereignty is regarded as an important measure of the Chinese authorities to protect the country from cyber threats and improve social stability. The effect of such regulations means that legally the companies operating in foreign countries cannot but hand over such details to the Chinese authorities. Some have posited that, apart from security, China's regulation is even more intrusive since cyber laws are instruments of state spying and repression. For instance, such a surveillance of the citizen's behaviour through big data enabler makes way for the Social Credit System that question its privacy and human rights implications.

## 5.2 Impact on Global Cyber Norms

Such policies have started producing indents shaping the international norms of cyberspace and the internet governance in the EU, Russia and China. Such data localization and cyber sovereignty patterns are consistent with the tendency toward the fragmentation of the Internet as they venture into the drawing of informational borders, all undertaken for security's sake. Balkanization is not operable with the long-sustained model of an open internet that has shaped the model of digital interconnectivity in the world in the last few decades.

Having demonstrated how the two countries in particular have moved the cyber governance debate with the controls they have put in place, the next section expounds on self-regulation. The debate is shifting and more countries are coming forward making claims to their cyber sovereignty

[38] Taylor, Richard D. ""Data localization": The internet in the balance." Telecommunications Policy 44, no. 8 (2020): 102003.

[39] Creemers, Rogier. "China's emerging data protection framework." Journal of Cybersecurity 8, no. 1 (2022): tyac011.

making the cyberspace divided into a multitude of national jurisdictions where the control varies. This poses great winds of difficulty to international businesses especially as they implement their business across the globe in areas of regulation.

Besides, the difference in their cyber policies of organise main world forces such as EU, China and Russia expose deeper geopolitical contest. Such an increase of the probability of the cyber conflicts, spying, and influence operations results from the conflict in space superiority between states because it does not own a single global pattern of the cybersecurity.

## 6. Challenges and Criticisms

Despite its appearance that cyber sovereignty serves to boost a country's security and protect information assets, the concept is not without stir. Such criticisms are, therefore, the assumption of sovereignty with regard to cyberspace, ethical issues, and the balances between privacy and security, and the implications of sovereign control over the digital trade. This section examines those issues: the problem of misuse of cyber sovereignty, the privacy-security paradox, and the consequences for international business.

### 6.1 Ethical Concerns: Potential Misuse of Cyber Sovereignty for Surveillance and Censorship

This is perhaps one of the biggest ethical issues that are associated with cyber sovereignty is that authoritarian states can easily use it in a bid to justify government spying and prohibition of rights of Freedoms. By passing correcting sovereignty laws, governments can use national security as a way of controlling the flow of information and powing down dissent. Take for instance the Chinese Great Firewall, where most of its uses are mainly for an act of restricting its citizens' political content and monitoring their activities online.

This almost leaves aside the suppression of freedom of expression while crossing directly into the right of privacy. In Russia, the 2019 Sovereign Internet Law allows the state to review internet traffic and content as being injurious to its national interest. Critics view such a move as providing justifications to the state for blocking sources of independent news and social networks, basically putting a cork on free speech. Notably, the control over digital content has been strengthened much more seriously since the invasion of Ukraine 2022[40]. Officials have blocked those so-called social networks like Facebook and Instagram that carried the anti-war stories.

These practices raise very basic questions of ethics in the direction of balance between national security and individual freedoms. Cyber sovereignty could be a very easy and powerful tool for expanding state control, which might lead to digital authoritarianism and will undermine democratic values or make the public lose trust in an internet meant for free communication.

Cyber sovereignty-extended surveillance technologies are facial recognition and AI-powered analytics. Monitoring citizen behaviour is what the Social Credit System of China does through big data-the issue here relates to privacy and state overreach[41]. There is a lot of space for such abuse because of the fact that these technologies can follow dissidents, minority groups, and activists, in turn silencing opposition and reinforcing state control.

[40] Susi, Mart, Wolfgang Benedek, Gregor Fischer-Lessiak, Matthias Kettemann, Birgit Schippers, and Jukka Viljanen. "Governing information flows during war: a comparative study of content governance and media policy responses after Russia's attack on Ukraine." (2022).

[41] Klinsawai, Worawan. "Deciphering China's social credit systems: Big data, surveillance, and political control." (2022).

### 6.2 The Privacy vs. Security Dilemma

Cyber sovereignty also places more emphasis on the long-standing tension between privacy and security. States therefore argue that this control over their digital space is necessary for protection of it from cyber threats such as espionage, cyberterrorism, and data breaches; however, measures taken to ensure cybersecurity come at the cost of individual rights to privacy. The most remarkable attempt to find a balance between privacy and security is that of the European Union through the GDPR. High standards of data protection create a position for companies that makes them very accountable, such as reporting breaches and keeping user data secure. In this attempt at enforcing compliance, companies are encouraged to collect more data, ironically increasing risks of violation of privacy.

It also raises questions in these circles, whether the desire for cybersecurity can coexist with private laws, as the world becomes increasingly interconnected. On the other hand, there are countries like the U.S. that are more security-driven, especially when there is more cyber-attack threat arising from a state actor from China or Russia. For instance, in the U.S., the CLOUD Act permits law enforcement agencies to access data based on a server[42], provided that such a server is even located in a foreign state.

While this law is deemed justified enough in combating terrorism and cybercrime, it has, however, worried and raised safety concerns over government overreach among the advocates of privacy. This has further complicated matters through use of encryption technologies. There must indeed be demands that encryption secure personal data, but encryption surely does reduce the investigating ability of the law enforcing authorities. The case in 2016 Apple and the FBI standoff highlighted the issue much more strongly when Apple declined the unlocking of one iPhone[43], which was attributed to an attack by a terrorist citing an issue regarding privacy concerns. In the case, it was depicted that the quest for security went against an individual's rights.

### 6.3 Impact on Businesses and Global Digital Trade

Cyber sovereignty significantly impacts businesses, especially technology companies facing stringent data localization laws in countries like China and Russia, Which Makes Operations Even More Costly as It Incurs Compliance Burdens as well; recently, Russia even enforced a fine upon Google and Meta formerly known as Facebook for not following data localization rules set by Russia. The costs incurred are not only added to the expenditures but discourage foreign investment as well since firms detest to invest in economies in which compliance is costly and time-consuming. China's Data Security Law and its Personal Information Protection Law enacted in 2021 require any foreign firm to go through security reviews before transferring the data out of the country[44]. This has forced Tesla and Apple to build their local data centers, hiking their operational costs.

This could also expose business risks on the issue of complying with Chinese regulations since they will have to provide sensitive information to the Chinese government.

Fragmentation is also being driven in the global digital market due to cyber sovereignty, simply because companies have to face a patchwork of rules which are significantly different in terms of

[42] Saini, Jaskaran Singh, Dinesh Kumar Saini, Punit Gupta, Chhattar Singh Lamba, and G. Madhusudhana Rao. "[Retracted] Cloud Computing: Legal Issues and Provision." Security and Communication Networks 2022, no. 1 (2022): 2288961.

[43] Zottola, Alyssa. "All Powerful? How the FBI's Request of Apple to Unlock an iPhone Using the All Writs Act Fails the New York Telephone Test." JL & Com. 39 (2020): 157.

[44] Klosowski, Thorin. "The state of consumer data privacy laws in the US (and why it matters)." New York Times (2021).

one jurisdiction versus the next. The extraterritorial scope of the GDPR coupled with China's data protection laws creates an awful complexity for companies trying to cope with several markets[45]; businesses have to spend lavishly on their compliance programs which could redirect resources away from innovation and growth.

The divergence in cyber policies among major powers further elevates the risk of conflicts in regulations. Data-sharing agreements between the EU and the US have also led to tensions, largely because of the former's stiff privacy laws and the latter's orientation towards security. In fact, the European Court of Justice has invalidated the EU-US Privacy Shield in 2020, citing surveillance issues surrounding US practices[46]. These court decisions have obliged businesses to seek alternative means to facilitate data transfers across national borders, further complicating cross-border digital trade.

The challenges and criticisms of cyber sovereignty emphasize the subtle play among national security, privacy, and economic interests. Even though purposed to preserve state sovereignty in the new world, its practice provokes some ethical questions and thwarts international cooperation toward global digitization. For this reason, the protection of private individual information is now imperative and simultaneously allows for preservation of national security for each nation as they seek to be masters of their evolving digital cyberspace.

## 7. Conclusion: Balancing Cyber Sovereignty and Global Cybersecurity

This development of cyber sovereignty in international politics therefore calls for states to ensure their digital space against the proliferation of emergent cyber threats. However, this paper has shown that such cyber sovereignty carries significant implications for privacy, international cooperation, and global digital trade. This conclusion will draw together all the findings from this study to discuss tensions that inevitably exist between national security and internet openness, making recommendations to bring cyber sovereignty and global cooperation into greater balance, while pointing to areas of further research in order to direct policymakers within this challenging field.

### 7.1 Recommendations for Balancing Cyber Sovereignty with International Cooperation

This conclusion shows that the need for cyber sovereignty is very essential, though it cannot affect the world on the connection for its internet or individual rights at its practice:

- **Establishing Global Cyber Norms and Frameworks**

International cooperation is desperately needed to establish cyber norms that encourage responsible state behaviour in cyberspace. Some progress has been made through the United Nations Group of Governmental Experts, but the lack of binding agreements remains a significant challenge. States need to focus on building consensus over issues like protecting critical infrastructure, refraining from cyberattacks against civilian targets, and refraining from cyber-enabled influence operations.

It would be the global cybersecurity treaty, much like the Paris Agreement on climate change. This would allow states to cooperate and respect sovereignty at the same time. It would represent a balance between the security concerns of authoritarian regimes and the privacy and freedom values of democratic nations. It would be an extremely big diplomatic challenge at this time when tensions between geopolitics are at their peak.

[45] Niebel, Crispin. "The impact of the general data protection regulation on innovation and the global political economy." Computer Law & Security Review 40 (2021): 105523.

[46] Fahey, Elaine, and Fabien Terpan. "Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield." Ind. J. Global Legal Stud. 28 (2021): 205.

- **Fostering Regional Cybersecurity Cooperation**

In the absence of a comprehensive international framework, regional cooperation becomes a more feasible option. The European Union has already set an excellent precedent through its Cybersecurity Strategy and the NIS Directive to encourage action by its member states in this direction. Regional organizations like SCO and ASEAN can play crucial roles in promoting cybersecurity cooperation in Asia. Building trust among the regional partners is what allows states to develop collective defense mechanisms against cyber threats.

- **Encouraging Public-Private Partnerships**

With much of the world's digital infrastructure in the hands of the private sector, there will be a need to get technology companies on board regarding the enhancement efforts in connection with cybersecurity. The model of how public-private partnership is used is set forth by the United States under initiatives of CISA. These should include threat intelligence, best practices for cybersecurity development, and investing in research as efforts in countering emerging threats.

However, such collaborations should not be made at the cost of those rights. Transparency seems to be one underpinning of building trust both between the public and private sectors and with the public at large. Proper guidelines in data sharing and accountability in the uses of shared information will also prevent abuse by either state power or corporate power.

- **Implementing a Balanced Approach to Data Localization**

Data localization laws boost national security at the expense of creating undue barriers to digital trade and innovation. States could therefore choose hybrid models: critical data may be local, while free flow continues for less sensitive data crossing borders. This would thus reduce the cost of complete data localization without compromising national security interests.

International standards for setting clear-cut limits for cross-border data flows could also reduce friction in global digital trade. New agreements, for example, based on the OECD Guidelines on Cross-Border Data Flows, could better balance security and economic growth.

### 7.2 Future Directions for Research

This is because the threat from cyber-crime changes day by day, due to the fast evolution of other innovation technologies like artificial intelligence and quantum computing. Future research should focus on several key areas:

| Key Areas for Future Research | Focus | Expected Outcomes |
|---|---|---|
| Impact of Emerging Technologies on Cyber Sovereignty | • Examine how advancements in AI and quantum computing affect cybersecurity and sovereignty. | • Insights into leveraging technologies for defense while mitigating new vulnerabilities. |
| Ethical Implications of State Surveillance | • Explore the balance between state surveillance for security and the protection of privacy. | • Frameworks for safeguarding individual rights without compromising national security. |
| Cyber Sovereignty in Developing Nations | • Investigate challenges like limited infrastructure and dependence on foreign technology. | • Strategies for capacity-building and international assistance to enhance cyber resilience. |

| | | |
|---|---|---|
| Assessing the Economic Impact of Data Localization | • Analyze how data localization laws influence trade, innovation, and foreign investment. | • Data-driven insights for balancing national security with economic growth. |

The concept of cyber sovereignty exemplifies a necessary evolution of how a state should confront growing cyberspace threats. Here, however, lies a challenge: balancing protection and safeguarding of national interest without undermining cooperation on global levels, individual privacy rights, and economic development opportunities. Thus, regional cooperation would become the vehicle through which international dialogue and public-private partnerships could lead to a more balanced approach in states' approach towards cybersecurity. The way ahead is not just developing newer technologies but also about the ethics of governance, transparency, and international cooperation. Our capability to negotiate these complexities shall define the future of the internet as secure and open.

## References

Akman, Pinar. *Regulating Competition in Digital Platform Markets: A Critical Assessment of the Framework and Approach of the EU Digital Markets Act*, 2021.

Attatfa, Amel, Karen Renaud, and Stefano De Paoli. ‘Cyber Diplomacy: A Systematic Literature Review’. *Procedia Computer Science* 176 (2020): 60–69.

Babb, Casey. *Digital Dictators: How Different Types of Authoritarian Regimes Use Cyber Attacks to Legitimize Their Rule*, 2022.

Bansal, Urvashi. ‘A Review on Ransomware Attack’. In *2021 2nd International Conference on Secure Cyber Computing and Communications (ICSCCC)*, 221–26. IEEE, 2021.

Bharti, Simant, and Saroj Shankar. ‘The Right to Privacy and an Implication of the EU General Data Protection Regulation (GDPR) in Europe: Challenges to the Companies’. *Journal of Contemporary European Studies* 31, no. 4 (2023): 1391–1402.

Branch, Jordan. ‘Territory, Sovereignty and Boundaries in Digital Battlespace’. *Research Handbook on Cyberwarfare*, 2024, 301–15.

Chalmers, Damian, Gareth Davies, Giorgio Monti, and Veerle Heyvaert. *European Union Law: Text and Materials*. Cambridge university press, 2024.

Chang, Yung-Yung. ‘China beyond China, Establishing a Digital Order with Chinese Characteristics: China’s Growing Discursive Power and the Digital Silk Road’. *Politics & Policy* 51, no. 2 (2023): 283–321.

Chaskes, William. ‘The Three Laws: The Chinese Communist Party Throws Down the Data Regulation Gauntlet’. *Wash. & Lee L. Rev* 79 (2022).

Creemers, Rogier. ‘China’s Emerging Data Protection Framework’. *Journal of Cybersecurity* 8, no. 1 (2022).

Fahey, Elaine, and Fabien Terpan. ‘Torn Between Institutionalisation & Judicialisation: The Demise of the EU-US Privacy Shield’. *Ind. J. Global Legal Stud* 28 (2021).

Fey, Laura, and Sarah D. Clark. ‘America the Vulnerable: The Nation State Hacking Threat to Our Economy, Our Privacy, and Our Welfare’. *Kan. JL & Pub. Pol’y* 30 (2020).

Fiero, Anna, and Elena Wright. ‘New Global Developments in Data Protection and Privacy Regulations: Comparative Analysis of European Union, United States, and Russian Legislation’. *Stan. J. Int’l L* 58 (2022).

Howells, Laura. *Digital Authoritarianism in China and Russia: A Comparative Study*, 2020.

Huang, Daoli. *Research on the Rule of Law of China’s Cybersecurity: China’s Rule of Law in Cybersecurity Over the Past 40 Years*. Springer Nature, 2022.

Huotari, Mikko, Jan Weidenfeld, and Claudia Wessling. ‘Towards A “Principles First Approach” In Europe’s China Policy." Drawing Lessons from the Covid-19 Crisis’. *MERICS-Mercator Institute for China Studies* 9 (2020).

Khusnetdinova, Agdaliya, and Peng Wang. *Rethinking the Principle of Cyber Sovereignty: Key Takeaways from China and Russia*, n.d.

Klinsawai, Worawan. *Deciphering China’s Social Credit Systems: Big Data, Surveillance, and Political Control*, 2022.

Klosowski, Thorin. ‘The State of Consumer Data Privacy Laws in the US (and Why It Matters)’. *New York Times*, 2021.

Krasznay, Csaba. ‘Case Study: The Notpetya Campaign’. *Információés Kiberbiztonság*, 2020, 485–99.

Lété, Bruno. *Paris Call and Activating Global Cyber Norms. German Marshall Fund of the United States*, 2022.

Mcmasters, Daniel H. *Subversive Influence: Vulnerabilities of The United States And Its Elections to Russian Interference Campaigns*. Monterey, CA, 2020.

Medcalfe, David. *Critical Infrastructure in the Face of Global Cyber Threats*, 2024.

Meyer, Paul. ‘Norms of Responsible State Behaviour in Cyberspace’. *The Ethics of Cybersecurity*, 2020, 347–60.

Mueller, Milton L. "Against sovereignty in cyberspace." *International studies review* 22, no. 4 (2020): 779-801.

Neyer, Jürgen. ‘After Global Governance: Technological Innovation and the New Politics of Sovereignty in Internet Governance’. *Zeitschrift Für Politikwissenschaft* 32, no. 2 (2022): 361–82.

Niebel, Crispin. ‘The Impact of the General Data Protection Regulation on Innovation and the Global Political Economy’. *Computer Law & Security Review* 40 (2021).

Polyzoidou, Vagia. ‘Combatting the Cybercrime: Thoughts Based on the Second Additional Protocol (Draft) to the Budapest Convention on Cybercrime’. In *EU Internet Law in the Digital Single Market*, 355–75. Cham: Springer International Publishing, 2021.

Ruohonen, Jukka. ‘The Treachery of Images in the Digital Sovereignty Debate’. *Minds and Machines* 31 (2021): 439–56.

Saini, Jaskaran, Dinesh Kumar Singh, Punit Saini, Chhattar Gupta, and G. Madhusudhana Singh Lamba. *Cloud Computing: Legal Issues and Provision*. Vol. 2022. Security and Communication Networks, 2022.

Sayapin, Sergey. ‘Russian Approaches to International Law and Cyberspace’. In *Research Handbook on International Law and Cyberspace*, 525–46. Edward Elgar Publishing, 2021.

Stavridou, V. Balancing Sovereignty and Integration: Digital Policy Dynamics in the European Union, 2024.

Susi, Mart, Wolfgang Benedek, Gregor Fischer-Lessiak, Matthias Kettemann, Birgit Schippers, and Jukka Viljanen. *Governing Information Flows during War: A Comparative Study of Content Governance and Media Policy Responses after Russia’s Attack on Ukraine*, 2022.

Taylor, Monique. ‘Building Digital Authoritarianism: From the Great Firewall to the New IP’. In *China’s Digital Authoritarianism: A Governance Perspective*, 1–24. Cham: Springer International Publishing, 2022.

Taylor, Richard D. ‘Data Localization”: The Internet in the Balance’. *Telecommunications Policy* 44, no. 8 (2020).

Thumfart, Johannes. ‘The Construction of Digital Sovereignty in Struggles for Recognition’. In *The Liberal Internet in the Postliberal Era: Digital Sovereignty, Private Government, and Practices of Neutralization*, 55–140. Cham: Springer Nature Switzerland, 2024.

ÜNVER, H. A. Artificial intelligence (AI) and human rights: Using AI as a weapon of repression and its impact on human rights.

Veit, Raoul-Darius. ‘Safeguarding Regional Data Protection Rights on the Global Internet-The European Approach under the GDPR’. In *Personality and Data Protection Rights on the Internet: Brazilian and German Approaches*, 445–84. Cham: Springer International Publishing, 2022.
Weber, Valentin. *The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power*, 2021.
Willett, Marcus. ‘Lessons of the SolarWinds Hack’. In *Survival April-May 2021: Facing Russia*, 7–25, 2023.
Zinovieva, Elena, and Sergey Shitkov. ‘Sovereignty as Practice in Digital Age’. In *Digital International Relations*, 75–90. Singapore; Singapore: Springer Nature, 2023.
Zoetbrood, J. P., E. B. A. Van Der Vleuten, A. J. Wieczorek, and F. C. A. Veraart. ‘The Emergence of Another Internet: Studying the Evolution of Chinese Cyberspace through a Large Technical Systems Lens’. *Innovation*, 2021.
Zottola, Alyssa. ‘All Powerful? How the FBI’s Request of Apple to Unlock an iPhone Using the All Writs Act Fails the New York Telephone Test’. *JL & Com* 39 (2020).
Булгакова, Валентина. ‘The Compliance of Facial Processing in France with the Article 9 Paragraph 2 (a)(g) of (EU) General Data Protection Regulation’. *Наукові Записки НаУКМА. Юридичні Науки* 11 (2023): 64–76.