



**Digital Sovereignty and Shanghai Cooperation Organization (SCO):  
Emerging Geopolitics of Cyberspace**

Uzma Siraj<sup>1</sup>

**Abstract:**

The rapid digitalization of global politics has elevated digital sovereignty—the ability of state to govern and safeguard their data, networks and digital infrastructures into a central concern of contemporary international relations. The Shanghai Cooperation Organization (SCO) has surfaced as an influential yet unexplored platform where divergent visions of cyberspace governance are contested. This study aims at exploring the engagements of SCO with digital sovereignty by analyzing the policy documents, declarations of SCO summit, declarations, and national cyber strategies through a qualitative discourse analysis. The research paper explores how digital governance norms of the west are being challenged? It argues that the SCO functions less as cohesive digital bloc and more as discursive and diplomatic arena, where narratives of security, autonomy, and resistance to western dominance are negotiated. By applying critical geopolitics theoretical framework, the paper highlights how digital sovereignty debates within the SCO reflects broader struggle over spatial imaginaries of cyberspace and contribute to the emerging multipolar order in digital governance. The findings reveal that while SCO members converge rhetorically in opposing western digital governance model, their narratives diverge in substance. It highlights SCO as a discursive arena rather than a unified policy making bloc.

**Keywords:** Shanghai Cooperation Organization, digital sovereignty, cyberspace governance, geopolitics of technology, multi-polarity, digital silk road

**INTRODUCTION**

The digital transformation of the international system has reconfigured the foundation of global politics. As cyberspace has become a critical domain for economic growth, security and governance, the question of digital sovereignty, the authority of state to regulate, control, and secure their digital infrastructure has emerged as one of the most contested issues in international relations (DeNardis 2020). Digital sovereignty is not merely a technical issue of internet governance; it represents a fundamental geopolitical struggle over ownership of data, the regulation of informal flows, and the capacity to project power in cyber space. Within this evolving context, Shanghai Cooperation Organization (SCO) has become an increasingly relevant forum. Established in 2001, initially as a regional security bloc focused on counter terrorism, extremism, and separatism, SCO has gradually expanded its agenda to encompass economic cooperation, energy, connectivity, and more recently digital governance (Aris 2009). SCO member states including China, Russia, India, Pakistan, and

---

<sup>1</sup> Assistant Professor, Department of International Relations, Federal Urdu University Islamabad, Pakistan. Email: uzma.siraj@fuuast.edu.pk

Central Asian Republics (CARs) constitute a huge and diverse geopolitical bloc where competing perceptions of cyberspace sovereignty interact. China's advocacy of cyber sovereignty, Russia's push for sovereign internet and the pragmatic digital policies of smaller member states demonstrate both convergence and divergence within this multilateral framework.

The most of the existing literature on SCO has focused on its security agenda such as counter terrorism operations, regional stability, or balancing against western influence (Ambrosio 2008; Biegon 2020). Similarly, scholarship on digital sovereignty has concentrated on greater power rivalry between the United States, China, and European Union (Mueller 2017; Pohle & Thiel 2020). Yet the SCO's role as a platform where alternative digital governance models are debated remains significantly underexplored. This gap is particularly important because the SCO provides a unique setting: it brings together states with divergent technological capacities and geopolitical priorities, but united by skepticism towards western dominated model of internet governance.

The problem this research addresses is the lack of academic inquiry into how the SCO mediates discourses on digital sovereignty and what this reveals about the emerging geopolitics of cyberspace. Without such analysis, international relations scholarship risks overlooking a critical arena where norms of digital governance are being articulated and contested outside western frameworks.

In this context, following questions guide this study. How does the SCO engage with and articulate digital sovereignty in its official discourse and policy framework? To what extent does member states particularly China, Russia, Pakistan, and Central Asian republics converge or diverge and their model of digital sovereignty, and does this about the SCO's role as a cohesive bloc or discursive arena in the broader geopolitical contest over cyberspace?

This study aims at examining SCO declarations, strategy, and statements relating to digital sovereignty and cyber space governance and analyzes the competing discursive framing of digital sovereignty advanced by China, Russia and other SCO members. It also tends to assess the extent to which the SCO contributes to shaping a regional or global digital governance framework. And to situate SCO digital sovereignty debates within the broader geopolitical shifts towards multi-polarity and resistance to western internet governance norms.

## **LITERATURE REVIEW**

### **Digital Sovereignty in International Relations**

Digital Sovereignty is a relatively new concept in International Relations scholarship. It refers to the authority of the states to control digital infrastructure, regulates data flows and secure cyber space within their jurisdiction (Pohle & Thiel 2020). Unlike traditional notions of sovereignty, which emphasizes territorial integrity, digital sovereignty extends sovereignty into virtual domain of information and communication technologies. Scholars such as DeNardis (2020) argues that digital sovereignty is inherently geopolitical, as it involves competing visions of internet governance whether decentralized, multi stakeholders led, or state centric. Western approaches, particularly those of United States and European Union, frame digital governance in terms of open internet principles and data protection regimes (Mueller 2017). By contrast, authoritarian states, such as China and Russia promotes state-centered models, emphasizing information control, surveillance

capacity, and protection against external interferences (Creemers 2017). These divergent models have fueled debates about a potential “splinternet” where global cyberspace fragments into distinct governance regimes (Hoffmann, Lazanski, & Taylor 2020).

SCO has been widely studied as a regional organization reflecting the multi-polarity of Eurasian politics. Initially focused on counter terrorism, and security cooperation, the SCO has gradually expanded its agenda to economic, energy, and digital domain (Aris 2009). Scholars debate whether the SCO functions as an effective organization or merely as diplomatic forum with limited institutional capacity (Ambrosio 2008). While China and Russia are seen as dominant players, the interests of Central Asian republics and new members like India and Pakistan complicates the SCO's cohesion (Krickovic & Pellicciari 2021). Although, SCO has included discussions on digital cooperation in its summit declarations since the mid-2010s academic attention to this dimension remains limited. Recent studies acknowledges that China uses the SCO platform to promote its cyber sovereignty model, while Russia leverages the organization to advance its sovereign internet law (Jia & Chen 2022). However, smaller states, like Uzbekistan, Kazakhstan and Pakistan remains underrepresented in this literature, despite their growing digital economies and dependence on external digital infrastructure (Kerr 2018).

### **Critical Geopolitics and Cyberspace**

Critical geopolitics provides an innovative theoretical lens to study digital sovereignty. Unlike realist and liberal approaches that view cyberspace primarily through material power or institutional cooperation, critical geopolitics emphasizes the discursive construction of space and power (Tuathail 1996). Applying this framework to digital sovereignty means examining how states imagine and articulate cyberspaces as a site of control, resistance, or identity. As Bratton (2016) argues digital infrastructure are not neutral technologies but spatial and political construct that reproduces power hierarchies. By examining SCO discourse, this study presents a perspective on critical geopolitics by analyzing how digital sovereignty is conceptualized as part of broader struggle against Western dominance and for multipolar digital order.

While existing literature SCO mostly in terms of security and energy, this study explores digital sovereignty globally, there is a limited intersection between two paradigms. Digital sovereignty is a less explored area specially in the context of SCO. Similarly, data on digital sovereignty in the context of critical geopolitics is also very limited. This study aims at addressing this gap by analyzing how SCO debates construct spatial imaginaries of cyber space and contribute to frame an alternate structure of digital governance.

### **RESEARCH METHODOLOGY**

This is a qualitative research study grounded in discourse analysis. The objective is to analyze how digital sovereignty is constructed within the Organization's official documents and strategies of member states. It uses both primary and secondary data. Primary data includes SCO Summit declarations and official communiques from 2021 to 2024, National cyber strategies of SCO member states, and speeches and statements by SCO leaders related to digital governance. Secondary sources include, academic writings on digital sovereignty, SCO and critical geopolitics, reports by think tanks, news and policy analysis on SCO digital initiatives. The research employs discourse analysis informed by critical geopolitics. Discourse analysis here focuses on how political

actors construct cyberspace through narratives of sovereignty, security, and resistance. Coding categories will include:

- Sovereignty Frame (autonomy, non-interference, control)
- Security Frame (Cyber security, terrorism, external threats)
- Geopolitical Frame (Multipolarity, western dominance, regional cooperation)

Discourse analysis is appropriate because the SCO is often criticized for being more of a discursive platform than an operational organization (Ambrosio 2008). Thus, analyzing official discourse provide insight into how digital sovereignty is constructed as a geopolitical issue, even if policy implementation is uneven.

### **THEORETICAL FRAMEWORK: CRITICAL GEOPOLITICS AND DIGITAL SOVEREIGNTY**

Critical Geopolitics emerged in the 1990s as a response to classical and structural geopolitics, which treated space as fixed and neutral and geopolitical power as a function of physical territory and resources (Ó Tuathail, 1996). Instead of viewing geopolitics as an objective science, critical geopolitics conceptualizes it as a discursive practice: the way in which political actors construct geopolitical space, identities, and threats through language, representation and narrative. In other words, geopolitics is only about military deployment and border disputes but also about how space is imagined and spoken about. Applied to cyberspace, this perspective means that the internet is not a neutral technological domain but a politically constructed space, where sovereignty, security, and autonomy are continuously negotiated. The notion of digital sovereignty is thus not simply a legal or technical category but a product of competing discourse that defines who controls data, infrastructure and flows of information.

One of the key contributions of critical geopolitics is to move beyond the fixation on territory. Traditional geopolitics assumes that sovereignty is tied to physical borders, yet cyber space challenges this assumption because digital infrastructures are both de-territorialized (information flows transcend borders) and re-territorialized (states try to impose borders through firewalls, data localization, and national regulations). Critical geopolitics allows us to study this paradox: cyberspace as simultaneously borderless and bordered. For example, China's discourse on cyber sovereignty frames the internet as a domain where state authority is paramount, emphasizing the right to regulate data flows, filter information and localize servers within territorial boundaries (Creemers, 2017). Russia, through its sovereign internet law, advances a narrative of defensive autonomy against western interference (Krickovic & Pellicciari 2021). Smaller states like Uzbekistan and Kazakhstan adopt hybrid narratives, balancing the benefits of global connectivity with desires of informational control (Kerr 2018). By treating these discourses as geopolitical practices, critical geopolitics the political imaginaries underlying SCO debates.

### **Discursive Dimensions of Cyberspace**

The discussion on discursive formation of cyber space demonstrates that how definitions, identities and power relations are constructed by narratives, languages, and political rhetoric. Critical geopolitics views cyberspace as not a purely technical arena, but a contested domain framed by competing discourses on security, sovereignty and governance. The articulation of cyberspace by states is a way to legitimized their specific policies base on their national interests and strategic

concerns. Whether as a secure sovereign domain, a vulnerable frontier, or an opportunity for modernization. Within the Organization, official declarations of SCO, summit speeches, and national strategies reflect how members of SCO engage with this discourse to articulate digital sovereignty as both a protective measure against western dominance and a route to alternate governance structures. This discursive framing is central to understanding how cyber space is politicized and how sovereignty becomes a rhetorical resource in the struggle over the emerging digital order.

### **SCO AS A GEOPOLITICAL ARENA**

From a critical geopolitical perspective, the SCO is best understood not primarily as a cohesive policy making bloc but as a discursive arena where different states articulate competing visions of digital sovereignty. The organization's summit communiqués frequently contain carefully negotiated language, phrases like "respect for national sovereignty in cyber space," "cooperation against the use of ICTs in terrorism and extremism," or "support for multipolar digital order." These terms reveal the contested imaginaries of cyberspace at play.

- China conceptualizes digital sovereignty as an extension of its developmental state paradigm, integrating ICT governance into broader initiatives such as "Digital Silkroad." China's 2017 cybersecurity law explicitly enshrine the principle of cyber sovereignty, linking it to the digital silk road under the Belt & Road initiative (KPMG China 2017). SCO declaration often echoes this framing by emphasizing "mutual respect for digital sovereignty"
- Russia underscores the need to protect itself from the cyber dominance of the west and legitimizes isolationist measures through security rhetoric. Russia's 2016 information security doctrine portrays cyberspace as a domain of western influence, legitimizing restrictive measures such as data localization laws (Legucka 2021). This aligns with its sovereignty rhetoric in its joint SCO Communiqués.
- Central Asian states reference digital sovereignty selectively, often prioritizing capacity building and modernization while discursively aligning with their stronger regional partners.
- Pakistan embeds digital sovereignty within its national security framework, demonstrating it as crucial for countering extremism and achieving digital modernization.

The theoretical lens of critical geopolitics is instrumental to examine how these narratives intersect and diverge within the SCO, revealing the symbolic contest of power that shape digital governance.

One of the most innovative aspects of applying critical geopolitics is the notion of spatial imaginaries. The actors envision cyberspace as geopolitical "space." For the SCO cyberspace is imagined not as a global common, but as a fragmented domain where national authority must prevail. This contrasts sharply with western multi stakeholders' models that conceptualizes the internet as a global borderless resource.

By analyzing SCO discourse, this research uncovers how member states construct cyberspace as:

- A Sovereign Domain: an extension of territorial control into digital space.
- A Contested Frontier: Vulnerable to western dominance, cyber-attacks, and ideological infiltrations.
- A Multipolar Space: Where alternatives governance models can coexist, resisting unipolar hegemony.

These imaginaries underscore how the SCO reflect broader geopolitical transformations towards multi-polarity and resistance to liberal internationalism norms.

### **Methodological Integration**

The methodology outlined earlier, qualitative discourse analysis of SCO documents and national strategies, align seamlessly with critical geopolitics. As O Tuathail (196) and Dodds (2017) argue, critical geopolitics relies on deconstructing texts to reveal how they construct space and power relations. By coding SCO declarations and state strategies into sovereignty, security, and geopolitical frames, this research operationalizes critical geopolitics in a systemic way. Moreover, by triangulating SCO documents with national cyber strategies, the study can compare the collective discourses of the organization with the national narratives of its most influential members. This approach ensures that analysis does not overstate SCO cohesion but instead highlights the discursive plurality within the organization.

### **Analysis**

The analysis focuses primarily on the major powers within the SCO, China, Russia, Pakistan and the collective framing of Central Asian states, given their central role in shaping the organization's discourse on digital sovereignty, while observer states, such as India and Iran as well as individual variations among Central Asian republics are acknowledged, they fall beyond the scope of this study. The objective is not to provide an exhaustive account of all members' cybersecurity laws, but to trace dominant narratives that define the SCO's collective positioning in global digital governance. This section employs the lens of critical geopolitics to analyze how member states of SCO frame digital sovereignty within their policies, strategies, organizational discourses. Instead of viewing the SCO as a cohesive bloc, the analysis shows how these core member states construct distinct yet intersecting narratives of cyber space. These narratives reveal that SCO is simultaneously a forum which is advancing the national agendas as well as symbolic arena for contesting western model digital governance.

This section applies the framework of critical geopolitics to examine how different SCO member states articulate their digital sovereignty in their policies, strategies, and SCO discourses. Rather than treating the SCO as a monolithic bloc, the analysis highlights how China, Russia, Pakistan, and Central Asian republics construct divergent yet overlapping narratives of cyberspace. These narratives reveal the dual role: a platform for projecting national vision and a symbolic arena where resistance to western digital governance norms is articulated.

### **China's Digital Sovereignty and Cyberspace**

China has been the most proactive SCO member in advancing a discourse on cyber sovereignty, defined as a right of each state to regulate its domestic internet without external interference (Creemers, 2017). Chinese leaders including President Xi Jinping, has repeatedly emphasized that cyber space is not a place beyond the rule of law (Xinhuanet, 2015) framing digital sovereignty as an extension of national sovereignty. Within the SCO, China promotes its cyber sovereignty agenda through official declaration. For example, the 2015 SCO summit in Ufa endorsed the principles of respecting state sovereignty in information space and combating the use ICTs for destabilization (Shanghai Cooperation Organization (SCO), 2015). China's narrative positions western model of



internet governance, based on openness and multi-stake holderism, as threat to national stability and cultural security.

China Also link digital sovereignty to its Digital Silkroad (DSR) initiative, part of the Belt & Road framework. Through the DSR, Beijing offers infrastructure investment, fiber optic cables, data centers, 5G networks to SCO members. Embedding its technological standards and norms (Triolo, 2020). This infrastructural power reinforces China's discursive authority: cyberspace is constructed as a domain where sovereignty is preserved not through isolation but through dependence on Chinese technology ecosystem. From a critical geopolitics' lens, China's discourse reflects a spatial imaginary of cyberspace as territorialized: a space where boundaries can be drawn and defended, much like physical frontiers. The SCO becomes a stage where China legitimizes this imaginary, portraying its digital model as a path toward, security, modernization, and resistance to western dominance.

### **Russia: Sovereign Internet and Defensive Autonomy**

Russia's approach to digital sovereignty emphasizes defensive autonomy against perceived western threats. The adoption of "Sovereign internet law" in 2019 institutionalized the Kremlin's power to isolate Russia's internet from global network during crises, reinforcing a discourse of securitization (Polyakova and Meserole, 2019). Within the SCO, Russia frames digital sovereignty primarily in terms of security. SCO joint communiques often stress the need to prevent the use of ICTs for interference in internal affairs or "terrorist purposes" (SCO, 2023). Unlike China, which promotes a proactive digital development agenda, Russia's discourse centers on protecting sovereignty from external manipulation, particularly, by the United States and Western tech corporation.

Critical geopolitics helps unpack Russia's spatial imaginary of cyberspaces as a contested frontier. Moscow visualizes its cyberspace as a battlefield where Western powers employ asymmetric power through monopoly in information, sanctions, and cyber operations. This framing justifies domestic controls such as surveillance of online platforms and restrictions on foreign digital services. However, Russia's influence within the SCO is not without constraints. While it aligns with China in challenging western norms, Moscow remains cautious of deepening dependence on Chinese technological infrastructure. This ambivalence highlights the SCO as a coalition of discursive convenience. Russia and China converge on the rhetoric of sovereignty yet diverge in their long-term digital ambitions.

### **Pakistan: Digital Sovereignty in Security and Development Discourse**

Pakistan's discourse on digital sovereignty is guided by dual lens of ensuring national security and advancing digital modernization. Lacking in robust and modern digital infrastructure and indigenous technology firms' over-dependence on external actors create more challenging scenario for Pakistan's digital sovereignty. And these challenges are crucial for addressing terrorism, extremism, and radicalization not only for national security but also aligning it with SCO framework (Ahmad, 2022). For instance, Pakistan in its SCO discourse, is concerned with the misuse of ICTs by terrorists and extremist elements and strongly advocates for strong regional cooperation, and collaboration in digital surveillance and counter extremism measures (SCO, 2021). This illustrates a securitization approach in which digital sovereignty is framed as a protective shield against instability. Simultaneously, Pakistan has started embedding digital sovereignty in its development

narrative. Digital Pakistan Initiative (started in 2019) emphasize e-governance, digital literacy and connectivity. Pakistan's collaboration with Chinese initiative of Digital Silk Road, it portrays digital sovereignty not only as safeguard but also as opportunity one that begins with participation in alternative digital infrastructure ecosystem beyond western dominance rather than on isolation (Jamil 2021). From a critical geopolitics' lens, Pakistan's discourse demonstrates a hybrid spatial imaginary in which cyberspace is constructed both as arena of vulnerability threatened by terrorists and as a way forward to modernization with the help of Chinese investment. The SCO supports this dual framing, allowing Pakistan to rhetorically align with sovereignty discourse while concurrently, seeking pragmatic digital partnership.

### **Central Asian Republics (CARs): Pragmatism & Selective Sovereignty**

The Central Asian republics (Kazakhstan, Kyrgyzstan, Tajikistan and Uzbekistan) holds an ambivalent position in SCO digital sovereignty debates. Given their limited technological capacities, these states rely significantly on Chinese investment and Russian security cooperation, while also promoting pragmatic digital modernization agendas. Kazakhstan, for instance, promotes "Digital Kazakhstan program" even as it enacts restrictive information laws consistent with sovereignty oriented rhetoric (Stryker, 2020). Uzbekistan has tested limited internet liberalization yet continues to invoke sovereignty when regulating online content, While Tajikistan and Kyrgyzstan with comparatively weaker infrastructure largely adopts sovereignty discourse shaped by Moscow and Beijing. In SCO summit declaration, Central Asian leaders continuously emphasized cooperation for capacity building, cyber security and ICT modernization (SCO, 2017). Their discourse reflects a balancing act: sovereignty is invoked rhetorically to align with great powers, but underlying priorities are to access investment, infrastructure, and training.

Critical geopolitics perspective sees Central Asian states constructing cyberspace as space of reliance, where sovereignty is framed less as full independence and more as negotiated autonomy within asymmetric power dynamics. SCO membership offers Central Asia republics a symbolic stage to endorse sovereignty discourse, even as they deepen material dependency on China's digital silk road and Russia's security architecture.

### **Synthesis: SCO as a Discursive Arena**

The analysis demonstrate that SCO debates on digital sovereignty are plural and contested.

- China projects cyberspace as territorialized and developmental, linking sovereignty to infrastructural power.
- Russia frames cyberspace as a security frontier, emphasizing autonomy through defensive measures.
- Pakistan blends security and development, constructing sovereignty as both protection and opportunity.
- Central Asian republics adopt sovereignty rhetoric selectively, prioritizing modernization and investment.

These findings demonstrate that the SCO does not act as a cohesive policy making bloc in the digital domain. Rather, it operates as a discursive space where sovereignty narratives align in resisting western models but diverge in their internal rationales. Looking from critical geopolitics



perspective, the SCO demonstrates how spatial imaginaries of cyberspace whether as territory, frontier opportunity or dependency inform the construction of multipolar order in digital governance. SCO narrative transforms cyberspace into a geopolitical space where sovereignty becomes both a protective shield and a developmental tool. This dual framing illustrates how sovereignty rhetoric legitimizes state control while simultaneously advancing modernization agenda. These discourses illustrate a symbolic struggle. Sovereignty is framed not merely as a legal right but as a spatial claim, situating cyberspace alongside territory and borders in geopolitical imagination.

### **The SCO and the Multipolar Digital Order**

The analysis reveals that the SCO functions as a discursive arena rather than a cohesive bloc. This has profound implications for how scholars and policy makers understand the evolving digital order. While China and Russia often present a common front in opposing Western models of internet governance, their underlying agendas diverge significantly. China's strategy is expansionist and infrastructural, using the Digital Silk Road to export technology, standards, and investment, thereby embedding its influence in SCO member states. Russia's approach is defensive and sovereigntist, seeking to insulate its domestic internet from western influence through legislations like the Sovereign Internet Law (2019). This duality highlights a multipolar digital order. The United States and its allies continue to promote multi-stakeholder governance model, where governments, civil society and corporations collaborate to shape norms (Mueller, 2017). In contrast, the SCO increasingly legitimizes a state-centric model, where governments retain ultimate authority over digital domains. The result is not a binary division but a pluralistic and fragmented order, where states aligned with different models depending on their interests, capacities, and vulnerabilities.

For Pakistan and Central Asian republics, the SCO provides both legitimacy and leverage. By endorsing sovereignty rhetoric, these states strengthen their bargaining power vis-à-vis western donors and institutions, while also securing Chinese and Russian support. Thus, the SCO demonstrates how regional organizations can serve as norm multipliers, amplifying sovereignty discourses that reshape global digital governance.

### **Critical Geopolitics and Spatial Imaginaries of Cyberspace**

A critical geopolitics lens reveals that digital sovereignty is not merely a legal or technological issue, it is about how states imagine and narrate cyber space as a space of power. Each SCO member state constructs cyberspace differently;

China territorializes cyberspace by equating it with sovereign borders Through policies like “great firewall” and “digital silk road”, Beijing presents cyber space as bounded as bounded and governable territory, where sovereignty is ensuring by controlling flows of data, platforms, and content (Creemers, 2017). This narrative legitimizes its global push to install Chinese hardware and software in partner states, normalizing the idea that digital infrastructure is an extension of state power. While on the other hand Russia constructs cyberspace as frontier of conflict. Moscow's discourse frames digital realm as under siege from western cyber operations, disinformation campaigns, and technological monopolies. Its sovereign internet law allows for isolating Russia's domestic internet infrastructure, embodying a vision of cyber space as a fortress that must be

defended (Polyakova & Meserole, 2019). When same theoretical lens is applied to smaller member states of the SCO, Pakistan envisions cyberspace as both vulnerable and aspirational. Vulnerable because of online extremism, disinformation, and weak cyber capacities; aspirational because digital development is tied to modernization and global competitiveness. Its reliance on Chinese digital projects situates sovereignty not in autonomy but in strategic partnerships that compensate for domestic capacity gaps (Ahmed et al. 2024). On the other hand, Central Asian states imagine cyber space as a dependent space, where sovereignty is rhetorically invoked but materially constrained. Kazakhstan, Uzbekistan, Kyrgyzstan, and Tajikistan rely on China for infrastructure and Russia for security frameworks, producing a form of borrowed sovereignty. Sovereignty here is less about independence and more about navigating asymmetric dependencies (Ugli & Radjabovich, 2025). By uncovering these imaginaries, critical geopolitics shows how sovereignty discourses are strategically malleable/. They allow states to frame their digital policies as legitimate, even when they reinforce dependency or authoritarian control.

A central implication of the SCO sovereignty discourse is its contribution to global internet fragmentation. While the internet was once idealized as a borderless global common, the sovereignty principle advanced within the SCO challenges this ideal. Instead, the internet is increasingly envisioned as a patch work of national jurisdiction, where data flows, content, and infrastructure are subject to state control (DeNardis, 2014). China's digital Silk Road has embedded its own new technical standard within the global technology competition and across the SCO states. This creates parallel ecosystem that may diverge from western standards reducing interoperability. The outcome is not uniform fragmentation but what can be termed as layered fragmentation. This layered fragmentation suggests that the "splinternet" is not a single phenomenon but a spectrum of sovereignty practices, with the SCO acting as a key site where these practices are legitimized and coordinated.

### **Implications for SCO Member States and Beyond**

China's sovereignty discourse reinforces its role as a norm setter in the global digital governance. By linking sovereignty to development, China positions itself not only as a defender of state control but as a provider of alternatives through infrastructure and technology. However, this strategy risk generating dependency backlash: smaller states may question whether reliance on Chinese digital ecosystems truly enhances sovereignty or substitute dependency for another. Russia uses sovereignty to justify securitization and control of the domestic internet. Within the SCO, Moscow's role is partly to balance China, ensuring that sovereignty discourse remain focus on resisting western dominance rather than Chinese expansion. However, Russia's weaker technological base may erode its long-term influence, raising the question whether it can sustain an independent digital ecosystem. Pakistan faces a dilemma and that is its weak digital infrastructure. China's Digital Silk Road advances connectivity and modernization on the one hand, but also risks locking it into Chinese standards. For Pakistan, sovereignty becomes relational rather than absolute secured through partnerships rather than independence. This suggests need for policy diversification, engaging not only with China but also with multilateral initiatives to avoid one sided dependency. For Central Asian states, sovereignty discourse provides symbolic capital. They can project themselves as defender of autonomy while deepening ties with Beijing and Moscow. Yet, this symbolic capital masks vulnerabilities. Without indigenous digital capacity, their sovereignty risks

becoming performative rather than substantive. Investments in local ICT sectors and legal frameworks will be crucial if they wish to translate rhetoric into practice. And as far as implications for the global governance are concerned, the SCO challenges the internet governance is converging towards universal norms. Instead, it demonstrates the pluralization of global digital governance model. For international institutions such as the UN, ITU, and ICANN, this creates a more fragmented negotiating environment, where western liberal models no longer enjoy uncontested legitimacy. The diffusion of SCO sovereignty discourses could weaken the western control over global digital infrastructure.

This research advances academic debate in three ways; by applying critical geopolitics to cyber space, this study shows how sovereignty is discursively constructed through spatial imaginaries. This adds nuance to IR theories that often treat sovereignty as a static legal principle. Rather than viewing SCO as a policy coordination bloc, the paper highlights its role as a discursive stage where competing sovereignties are legitimized. This reframing allows for a better understanding of how regional organizations influence global governance beyond formal policy making. Instead of treating internet fragmentation as binary, the paper introduces the idea of layered fragmentation, capturing the diversity of sovereignty practices across states. This concept guides the future empirical research into how states operationalize digital sovereignty in practice.

Like any discourse analysis, this study faces limitations. First, it focuses on representational practices, what states say in SCO declarations, speeches and strategies. This does not always correspond to material practices. For instance, while Pakistan emphasizes for digital sovereignty in security terms, its weak infrastructure means that sovereignty claims are aspirational rather than operational. Future studies could adopt mixed methods, combining discourse analysis with infrastructure mapping or interviews with policy makers.

Second the scope of analysis was limited to core SCO members, Observer states like Iran, Belarus, and Turkey also contribute to sovereignty discourse within the organization. Their inclusion can broaden the understanding of how sovereignty narrative could diffuse across Eurasia. Similarly, examining how external factors, such as European Union, United States or private tech companies respond to SCO sovereignty narratives could enrich the analysis of global contestation.

Third, while critical geopolitics uncovers the discursive dimension of sovereignty, it may understate the technological-material underpinnings of power. Future research could integrate political economy perspective to examine how infrastructure ownership, platform monopolies, and financial flows interact with sovereignty discourses.

## **CONCLUSION**

The SCO debates on digital sovereignty highlights emergence of a multipolar and fragmented digital order. By constructing cyberspace as territory (China), frontier (Russia), vulnerability opportunity (Pakistan), or dependency (Central Asia), member states articulate sovereignty in ways that both resist Western dominance and reinforce asymmetric dependencies.

From the perspective of geopolitics, the SCO demonstrates how sovereignty is not an objective fact, but a discursive practice. mobilized to legitimized policies, attract investment, or secure regime stability. The organization serves as a symbolic arena, amplifying sovereignty narratives that

reshape global governance. The implications are far reaching. SCO discourses normalize state centered internet governance, and embed sovereignty as a core principle of the international politics in the global age. While these discourses provide smaller states with symbolic legitimacy, they also risk entrenching dependencies, raising questions about the future of genuine autonomy in cyberspace.

In sum, the SCO is not forging a unified digital bloc but is shaping a discursive contour of the twenty-first century digital order. Its sovereignty narratives, diverse yet convergent in their opposition to Western norms, contribute to the construction of a multipolar cyberspace that will define global politics for decade to come.

### References:

- Ahmad, S. (2022). Cyber Security threat and Pakistan's preparedness: An analysis of National Cyber Security Policy 2021. *Pakistan Journal of Humanities and Social Sciences Research*, 5(1), 25-40. doi: 10.37605/pjhssr.v5i1.381.
- Ahmed, Z. S., Yilmaz, I., Akbarzadeh, S., & Bashirov, G. (2024). Contestations of internet governance and digital authoritarianism in Pakistan. *International Journal of Politics, Culture, and Society*, 38, 499-526. doi: 10.1007/s10767-024-09493-2.
- Ambrosio, T. (2008). Catching the Shanghai spirit: How the Shanghai Cooperation Organization promotes authoritarian norms in Central Asia. *Europe-Asia Studies*, 60(8), 1321-44. doi: 10.1080/09668130802292143.
- Aris, S. (2009). The Shanghai Cooperation Organisation: Tackling the three evils. A regional response to non-traditional security challenges or an anti-Western bloc? *Europe-Asia Studies* 61(3), 457-82. doi: 10.1080/09668130902753309.
- Biegon, R. (2020). US hegemony and the Trans-Pacific Partnership: Consensus, crisis, and common sense. *The Chinese Journal of International Politics* 13(1), 69-101. doi: 10.1093/cjip/poaa001.
- Creemers, R. (2017). Cyber China: Upgrading propaganda, public opinion work and social management for the twenty-first century. *Journal of Contemporary China* 26(103), 85-100. doi: 10.1080/10670564.2016.1206281.
- DeNardis, L. (2020). *The internet in everything: Freedom and security in a world with no off switch*. Yale University Press.
- Hoffmann, S., Lazanski, D., & Taylor, E. (2020). Standardising the splinternet: How China's technical standards could fragment the internet. *Journal of Cyber Policy*, 5(2), 239-64. doi: 10.1080/23738871.2020.1805482.
- Jamil, S. (2021). From digital divide to digital inclusion: Challenges for wide-ranging digitalization in Pakistan. *Telecommunications Policy*, 45(8), 102206. doi: 10.1016/j.telpol.2021.102206.
- Jia, K., & Chen, S. (2022). Global digital governance: Paradigm shift and an analytical framework. *Global Public Policy and Governance*, 2(3), 283-305. doi: 10.1007/s43508-022-00047-w.
- Kerr, J. A. (2018). Authoritarian practices in the digital age| information, security, and authoritarian stability: Internet policy diffusion and coordination in the former soviet region. *International Journal of Communication*, 12, 3814-34.
- KPMG China. (2017). *Overview of China's cybersecurity law*. Zhujiang.
- Krickovic, A., & Pellicciari, I. (2021). From 'Greater Europe' to 'Greater Eurasia': Status concerns and the evolution of Russia's approach to alignment and regional integration. *Journal of Eurasian Studies*, 12(1), 86-99. doi: 10.1177/1879366521998808.

- Legucka, A. (2021, Jun. 8). *Online warfare: Russian policy on international information security* (PISM Bulletin No. 111 (1807). The Polish Institute of International Affairs. [https://pism.pl/publications/Online\\_Warfare\\_Russian\\_Policy\\_on\\_International\\_Information\\_Security#:~:text=Russia in April this year,policy of the Russian Federation](https://pism.pl/publications/Online_Warfare_Russian_Policy_on_International_Information_Security#:~:text=Russia in April this year,policy of the Russian Federation).
- Mueller, M. (2017). *Will the internet fragment? Sovereignty, globalization and cyberspace*. Polity Press.
- Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, 9(4), 1-19. doi: 10.14763/2020.4.1532.
- Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models* (Policy Brief). Brookings.
- Shanghai Cooperation Organization (SCO). (2015, Ju. 3). Press Release of the Meeting of the Council of Ministers of Foreign Affairs of the Member States of the Shanghai Cooperation Organization. <https://eng.sectesco.org/documents/?offset=40>
- Shanghai Cooperation Organization (SCO). (2017). Astana Declaration of the Heads of State of the SCO. <http://eng.sectesco.org/documents>
- Shanghai Cooperation Organization (SCO). (2021). Dushanbe Declaration of the Heads of State of the SCO. <https://eng.sectesco.org/documents/>.
- Shanghai Cooperation Organization (SCO). (2023). *Astana Communique*. Astana.
- Stryker, C. (2020). Budding Digital Authoritarianism in Central Asia. <https://daviscenter.fas.harvard.edu/insights/budding-digital-authoritarianism-central-asia>
- Triolo, P. (2020, Apr. 29). The digital silk road: Expanding China's digital footprint. *Eurasia Group*. <https://www.eurasiagroup.net/live-post/digital-silk-road-expanding-china-digital-footprint>
- Tuathail, G. O. (1996). *Critical geopolitics: The politics of writing global space*. University of Minnesota Press.
- Ugli, N. K. T., & Radjabovich, M. I. (2025). The role of China's digital silk road in shaping the digital future of Central Asian economies. *Web of Discoveries: Journal of Analysis and Inventions*, 3(6), 4-9.
- Xinhuanet. (2015, Dec. 16). Highlights of Xi's internet speech. *Xinhuanet* [http://www.xinhuanet.com/english/2015-12/16/c\\_134923855.htm](http://www.xinhuanet.com/english/2015-12/16/c_134923855.htm)

Date of Publication	August 30, 2025
---------------------	-----------------