‘National Security’ and the Construction of Digital Governance Models: Content Regulation in the Pakistani ‘Digital Public Sphere’

Faruzan Anwer Butt¹, Muhammad Makki²*, Tughral Yamin³

¹National University of Sciences and Technology (NUST), Centre for International Peace and Stability (CIPS), Islamabad, Pakistan.

²National University of Sciences and Technology (NUST), Centre for International Peace and Stability (CIPS), Islamabad, Pakistan.

³National University of Sciences and Technology (NUST), Centre for International Peace and Stability (CIPS), Islamabad, Pakistan.

Received date: 10 January 2022
Acceptance date: 15 March 2022

Abstract
This paper situates the construction of ‘unlawful content’ in the Pakistani state’s design of legal frameworks under the Prevention of Electronic Crimes Act (PECA) 2016 and the Removal and Blocking of Unlawful Online Content Rules (RBUOC) 2021 in the broader context of state-centric ‘security’ argumentation. To this end, the processual nature of content regulation, embedded in the broader context of the country’s digitization drive, is used to examine the nature of state-citizen interaction in digital spaces. Thus, Pakistan’s nascent model of content regulation, embedded in a broader, overarching understanding of ‘digital governance,’ is problematized using the interplay between ‘national security’ and ‘human rights.’ The aim is to explore whether there is a disconnect in state-citizen perception of the primary referent object of security in the drive to structure the Pakistani digital public sphere, with state- versus human-centric approaches shaping policy priorities. Consequently, the paper engages with the idea of ‘situated meanings’ underlying policy design whereby social media platforms, as a phenomenon, hold different meanings for separate groups, and may give rise to divergent perspectives when it comes to prioritizing the objectives of public policy. In doing so, interpretive policy analysis (IPA), as a multidisciplinary approach, is adapted to explore the discursivity underlying policy design, with the language employed in PECA and RBUOC drafts seen as exercising a formative or generative influence in shaping the action of state and rights-based actors in digital content creation ‘spaces.’
Keywords: digital public spheres, national security, societal security, content regulation, DSR

1 Introduction

The proliferation of digital technologies continues to expand the domain of cyberspace as a ‘space of flows.’ Critical communication theory problematizes the nature of political participation occurring in the age of Social Networking Sites (SNS), with scholars such as Dahlgren exploring how ‘discourses can serve to impede the democratic potential of these media, particularly through the various ways by which they tend to deflect participation.’ (2014: 192) Participatory practices in Pakistani digital spaces have evolved in the context of ‘security discourses’ examining the socioeconomic potential of Information Communication Technologies (ICTs) against the ‘threat’ of fifth-generation warfare (Firdous 2020; Khan 2019).

As ICTs increasingly penetrate state management frameworks, the potential impact they may exercise on governance praxis remains underproblematized, especially in developing societies with a history of political unrest. In light of this, the normative baseline for the use of ICT enabled state-societal interaction is yet to be determined, with authors such as Jorgensen (2021) outlining the need for shared societal visions aiming for inclusive, equitable, and diverse public participation. In the context of SNS, various modes of expressing, encountering, and searching for information online may become subject to ‘securitization,’ as states attempt to interpret digital spaces through the lens of territoriality and ‘national security.’ The construction of select referent objects vis-à-vis security, as well as a normative framework aimed at securing the same, entail a process of multistakeholder interaction and negotiation, with implications for individual rights and freedoms.

In contrast to studies examining the mobilization potential of SNS for socioeconomic uplift, the concept of ‘fifth generation warfare’ problematizes the nature and scope of interaction enabled by SNS as a threat, particularly given the phenomenon of ‘alt-news’ (Turunen 2018). Thus, the very ‘permissionless innovation’ (Digital Citizenship in Pakistan 2015) valued in analyses focused on the user-centric potential of SNS, may be reframed as an unregulated, potential risk factor.

Considering the need to coordinate between divergent perceptions of the relation between SNS and ‘security,’ this paper engages with the idea of ‘situated meanings’ informing the design of the digital public policy. It is argued that SNS, as a phenomenon, holds different meanings for separate groups, and may give rise to divergent perspectives when prioritizing the objectives of public policy. These perspectives are subject to varied ‘lived experiences’ of actors in select contexts. Similarly, citizen groups concerned by the implications of restrictive digital governance praxis in select states may resist any perceived ‘spillover’ of such models into their home state. It follows that the language used in policy design exercises a formative or generative influence in shaping, and not merely representing, the action of state and rights-based groups interacting over digital spaces. To this end, critical approaches under Interpretive Policy Analysis (IPA) allow engaging with both the contexts and attendant situated meanings, underlying public policy instruments.
The present study problematizes the perspectives used to envisage a potential structure for Pakistan’s nascent digital ‘public sphere,’ with digital rights activists taken as championing a rights-based approach to SNS governance models, as opposed to state-centric understandings of national security. Both groups employ SNS for disseminating a wider message to domestic and transnational audiences, while engaged in attempts to structure these platforms through locally developed governance regimes. A key area of interest is the impact of inter-group interaction on the groups themselves, as representatives of both sides exhibit distinct threat orientations with regard to ‘security.’

In doing so, the paper examines how concepts essential to the area of inquiry identified, i.e., ‘public sphere,’ ‘space of flows,’ and ‘national security’ etc. have been addressed in contemporary literature, before presenting a brief overview of how these pertain to the Pakistani ‘digital public sphere.’ This is followed by introducing a three-tier conceptual framework for problematizing how identified policy instruments construct actors, processes, and mechanisms, in select contexts, for structuring this sphere. Relevant statutory provisions from these instruments form the basis for discussion in the subsequent section, coupled with an interpretive discourse analysis of categories used to construct ‘unlawful’ content as a key regulatory device. The discussion and analysis section maps identified provisions, and the context in which these were drafted, unto the three-tier conceptual model presented earlier. Following this, the concluding section further examines the context of policy design in light of the prospective impact of Digital Silk Road projects on Pakistan’s emerging digital governance model.

2 Cyberspace, Security and the State

The fragmented nature of digital spaces, alongside weak institutional and governance frameworks in transitionary settings, may prompt differing interpretations of their relevance for ‘security’. ‘Top-down’ state security agendas, particularly in the ‘threat-response framework’ typical of South Asia (Barthwal-Datta and Basu 2017), may be seen to prompt a predilection for deterrence-based strategies as key to safeguarding the primary referential agent of security i.e., the state. It may further color state interpretations of an emergent ‘digital public sphere’ as a threat to selectively defined security objectives. Liaropoulos (2015) examines how the militarization of ‘cybersecurity’ discourse presupposes the nature of cyberspace as a domain of conflict. The ‘digital public sphere’ may thus be taken as a key site for the evolution and implementation of such policy, embedded in the nature of the physical infrastructure underlying the spread of SNS access.

While national security by definition encompasses the protection of a state’s population, as well as its territory and sovereignty, it is argued that state understandings of security priorities may de-emphasize select human needs (Liaropoulos 2015). The absence of global governance regimes on human ‘rights’ in cyberspace allows the state to emerge as the key actor framing these rights in the context of select security interpretations (Smith 2010: 42-3). The

---

1 A key aspect of this has been examined in Tughral Yamin’s study on “Fake News as an Instrument of War” (2019) which cites the evolution of war as a ‘hybrid’ enterprise in which communication plays a central role.

2 This follows the inability of the UN Group of Governmental Experts (GGE), as well as the Open-Ended Working Group (OEWG), to establish broad-based consensus on norms for acceptable state behavior in...
fragmented nature of ‘publics’ in transnational digital spaces may predispose state actors to view the same with an excess of caution. A parallel concern, particularly in post-conflict spaces faced with a history of radicalization and extremist violence, is the use of SNS by militant actors for purposes such as recruitment (Borau and Wamba 2019; Droogan, Waldek and Blackhall 2018).

2.1 Space of Flows/Infrastructure/civic participation
User-Generated Content (UGC) offers a key site for modulating this interaction, as states attempt to categorize the nature and scope of UGC in line with policy objectives prioritizing distinct understandings of security. Thus, SNS platforms allow for UGC flows that generate parallel forms of data i.e., user information and usage statistics etc. Considering this, social media, conceptualized by theorists such as Sujon (2021) as being based on two key, albeit contrasting, themes of data/surveillance and community/connection, present a Castellsian ‘space of flows’. Castells’ understanding of the information society draws on McLuhan’s concepts of the effects of technology on space, time, and the structure of human activity (Kirtiklis 2017). ‘Space of flows,’ in the ensuing analysis, identifies how ‘space lost its dependence on time and vice versa (i.e., to overcome the spatial distance humans do not need a lot of time anymore) and this led to a transformation of scale and pace of human activities, and, eventually, changed their whole pattern.’ (Kirtiklis 2017, p. 72) Thus, as per Castell, ‘Space of flows is not a place in the traditional sense (a locale whose form, function, and meaning are self-contained within the boundaries of physical contiguity.’ (Castell 2010, p. 453)

Instead, it may best be understood through the dynamics of social practices taking place within it (Kirtiklis 2017; Stalder 2006).

Dahlgren (2005) explores the potential of the net as a ‘public sphere’ (2005). Similarly, Masip, Ruiz-Caballero, and Suau (2019) problematize the understanding of ‘publics’ in post-Habermas ‘digital’ spaces, using such concepts as UGC. Yet at the same time Papacharissi (2010) distinguishes between public ‘spaces’ and ‘spheres’ by highlighting that while the former enhance discussion, the latter enhance democracy.

2.2 State vs Societal Security
State actors may be inclined to view ‘security’ as a matter of hierarchy, with traditional state security prioritized as the sine qua non of any ‘non-traditional’ variants. Hoogensen and Rottem (2004) elaborate on ‘top-down’ security approaches emanating from the perspective of state elites, in contrast to alternatives based on individual and social group concerns. Chakma (2009) builds on such an understanding to comment on the power-oriented and competitive security orientation exhibited by states in South Asia, whereby a strong nation-state is conceived as key to addressing both internal and external threats. McDonald (2012) argues how security is a social construct, discursively produced through a process of intersubjective contestation and negotiation. In light of this, social media platforms may be contextualized as a broader platform for discursively (re)defining security, even as they themselves are subject to state securitization practices. Tickner (1997) outlines the need for multidimensional and multilevel definitions of

cyberspace: https://carnegieendowment.org/2021/05/19/un-struggles-to-make-progress-on-securing-cyberspace-pub-84491

8041 http://www.webology.org
security, broadly conceived as the diminution of all forms of violence (physical, structural, ecological; see also Browning & McDonald 2011).

The dual nature of digital spaces prompts increasing interpenetration between public and private spheres. As the administrative apparatus of states expand into the digital, increasing engagement between state and societal actors further blurs the line between public and private spheres. State intervention in ‘structuring’ these spaces may be compared with societal organization around ensuring any state-led transformation process does not infringe on citizen rights. As highlighted earlier, the absence of international treaties codifying a set of norms determining approaches to digital governance, leave the state as the primary actor possessed of the capacity, and the authority, to design tentative models.

In a similar vein, the role of societal groups in negotiating the processes, mechanisms, and procedures for the structural transformation of digital spaces, should not be overlooked. For instance, Farrell and Newman (2019) comment on the ‘internationalization’ of domestic security policies, as the “transatlantic politics of domestic security then shape the policies, practices and lived experience of security forces, firms and citizens across the globe” (2019: p.2). A similar theme may be glimpsed in the impact of China’s domestic digital security initiatives as cultivating shared understandings of the objects and means of security in partner DSR states – understandings which may spill over into the design of public policy. Such an analysis may also serve to reorient the debate on digital security along traditional, state-centric lines, particularly in states lacking effective democratic praxis.

Using Marichal’s (2012) analysis of SNS as ‘architectures of visibility’, Owen (2017) highlights how both state and societal actors capitalize on the capacity of these platforms to connect users around particular interests and causes. This visibility, while allowing users to circumvent information gatekeepers in the form of the mainstream media, simultaneously allow state agents to identify and label the emergent discourse under the rhetoric of ‘state security.’ (e.g., Papic and Noonan, 2011). An attendant element follows state attempts to ‘structure’ the nascent ‘public sphere’ represented by SNS, with authors such as Claessen (2020) exploring the securitization of internet infrastructure (both physical and virtual), alongside content generation. Kurowska (2019) elaborates on processes of ‘strategic norm contestation’, whereby political actors manipulate shared normative frames in order to attain certain political ends...

Van Veen (2007) elaborates on how ‘threats to sovereignty provide the state with an institutional interest to temporarily subordinate the interests of its citizens to its own, under the assumption that its functions are irreplaceable’ (quoted in Claessen 2020, p. 144) In the context of post-conflict spaces isolated from the mainstream, this may translate into a ‘securitization of dissent’ (Owen 2017) where rights-based discourse, premised on ‘human security’, appears to counteract, if not undermine, ‘national security.’ Thus, the discursive potential of UGC, in addition to the manner and scope of network formation and mobilization allowed by digital and physical infrastructure, form a key component informing state-citizen encounters in the digital public sphere.
Nonetheless, new technologies, and attendant platforms, do entail a paradigm shift in our conceptualization of politics and society. Such shifts may be said to inform the citizen objectives vis-à-vis encounters with state agents in digital spaces. As SNS reduce the cost of communication, increase the speed and dissemination of information, and fundamentally change the nature of the information available (Zeitzoff 2017), potential emerges for what Castells (2009) describes as mass self-communication. Thus, individual and state dimensions of ‘security’ are subject to (re)negotiation through the modes of interaction made possible by the affordances and attributes of SNS. The discursive environment presented by these platforms, in addition to deliberations of normative ideals informing their use, present a key component in alternative politics, whereby subaltern groups attempt to make use of the same for political purposes. ‘Political’, in this context, may be differentiated from ‘politics’, with Dahlgren defining the former as ‘the ever-present potential for collective antagonisms, conflicts of interest, in all social relations and settings’ (Dahlgren 2014, p. 192).

Given the increasing frequency of state-society encounters over ‘security,’3 there is a need for studies that problematize the language of policy in the context of material factors i.e., physical infrastructure, that underly the same. This has particular bearing on SNS, and the tendency in contemporary literature to focus on ‘cyberspace’ as a virtual construct without effective consideration of the infrastructure that shapes it through the language of state policy. Considering this, the study presents a model through which SNS regulation in Pakistan, underproblematic in the literature, may be analyzed using policy language, as informed by the underlying context of physical net infrastructure, and a select mode of state-society interaction in, and over, SNS.

3 Criminalizing SNS and Digital Rights in Pakistan

SNS, in the Pakistani ‘digital public sphere’, may be analyzed as a three-tier construct premised on the interplay between infrastructure, information, and interaction. The nature of both physical and virtual infrastructure i.e., broadband access, application design, device type, online platform layout etc. informs the mode and scope of the interaction between state and citizen users. The sporadic presence/absence of the state in the public sphere, i.e., in terms of service delivery, is a key characteristic of this setting, as is a tendency for the ‘securitization’ of the digital by state apparatus seeking to (re)assert control over virtual and physical spaces. This control reflects the ‘infrastructure-interaction’ model, whereby state policy and regulation informs both questions of access (infrastructure), as well as the nature of subsequent citizen participation (interaction). The Pakistani state’s attempts to regulate social media platforms through a focus on the removal of ‘unlawful’ content. To this may be added the abortive pace of digitization in different provincial zones, with only 5 percent of the population in erstwhile FATA having access to the internet (Diplomat July 2020), and the abrupt suspension of mobile data services in the event of ‘securitization’ of social media platforms. The prevalence of a rural-urban digital divide further complicates matters, as peripheral regions lacking access to basic net infrastructure are effectively cut off from the national ‘digital’ space.

---

In light of this, the amended Removal and Blocking of Unlawful Online Content Rules (RBUOC) 2021, may be analyzed as an attempt to control UGC flows in the Pakistani digital space. The Rules expand on provisions contained in the Prevention of Electronic Crimes Act (PECA), 2016; considered by local rights advocacy groups e.g., Bolo Bhi and Digital Rights Foundation, as setting a troubling precedent for top-down state control of Pakistan’s nascent digital public sphere. PECA’s statutory provisions have been analyzed by scholars such as Daudpota (2016, p. 2) as ‘being likely to offend Articles 4 and 9 (concerning due process guarantee as to liberty); Articles 8 and 9 (concerning freedom of speech); and Article 14 (concerning protection of privacy) under Pakistan’s Constitution’. This follows from the Rules being seen as excessively censorial in nature, with the potential to weaponize social media by criminalizing any criticism of state action or policy. A related concern is the May 2021 proposal to launch a centralized ‘Pakistan Media Development Authority’ (PMDA) with the overarching power to regulate films, electronic, print, and digital media.

Consequently, there emerges a need to ensure comprehensive multisectoral stakeholder input in order to capitalize on the full potential of digital public spaces for citizen welfare. From using hashtag trend data in otherwise data poor environments to determine necessary areas for state policy intervention (World Bank Group 2021), to employing Twitter as a platform for community-driven civic initiatives and poverty alleviation, there is a need to ensure policy aids, instead of impedes, the social, cultural, and economic potential of SNS. Groups such as the Asia Internet Coalition (AIC) argue that the precedent being set in Pakistan’s nascent digital governance regime is antithetical to progress and growth, with the potential to cause ‘immense social and economic harm.’ (DAWN July 2021) Local digital rights groups such as Bolo Bhi, Digital Rights Foundation, and Media Matters for Democracy, are increasingly alarmed by the broad-based blanket authorization granted to bodies such as the Pakistan Telecommunications Authority (PTA) for the defense of such abstract concepts as ‘national security/integrity,’ ‘morality,’ and the ‘glory of Islam.’ Given this analysis, state construction of ‘unlawful’ content in PECA 2016, and the RBUOC Rules 2021, may be said to reflect a state-centric ‘security’ perspective, rather than citizen-centric ‘rights’ based understanding, of digital governance.

4 Methodology
This paper problematizes select understandings of ‘security’ employed by the Pakistani state in its attempts to structure a nascent Pakistani digital ‘public sphere.’ Attendant public policy instruments, i.e., PECA 2016 and the amended RBUOC 2021, are taken as reflective of key normative assumptions that construct the actors, processes, and mechanisms that are the subject of state legislative action. Doing so necessitates adapting interpretive policy discourse analysis as an approach engaging with the discursivity underlying policy design (Yanow 2000; Roe 1994). Interpretive Policy Analysis (IPA) draws on the presupposition that issues addressed in policy have different meanings for different groups. These ‘situated’ meanings may be enacted in various, sometimes divergent ways, based on different perspectives that affect how people

see and respond to issues. An additional element is the impact of perspectives, and their associated actions, on others, thereby introducing a need to problematize the context underlying the construction of policy. Considering this, IPA challenges traditional positivist policy analysis (ref) and its emphasis on epistemic certainty, underscoring the generative role played by language in policy design whereby devices such as metaphors not only represent policy but also shape it (Roe, 1994).

Thus, this study is premised on the logic underlying Interpretive Policy Analysis (IPA) as concerned with the contexts, and situated meanings, underlying public policy instruments. IPA approaches situate such instruments in the context of interpretive communities, analyzing how language is deployed as a world-making exercise by actors through their daily practice. As such, it is recommended that ‘textwork’ i.e., an interpretive analysis of the language in public policy instruments as imbued with actor perceptions, be combined with ‘fieldwork,’ whereby the researcher directly engages with the daily practice of the actors concerned. Designed using inputs from contemporary literature on the theme of ‘digital public spheres’, the given framework addresses both the processes and context informing public policy design, in lieu of the self-reflexive praxis of concerned actors. In light of IPA as an evolving set of critical approaches concerned with transdisciplinary methodological flexibility, such a framework may constitute a useful contribution to assessing the nature of digital governance policies in developing states.

The ensuing inquiry examines the use of specific terms in policy texts with ‘structuring’ potential i.e., language that helps privilege a certain brand of thinking and doing over others and helps conceptualize the pre-assumptions shaping policy objectives. Such pre-assumptions do not take shape in a vacuum but are premised on existing social and political economic conditions which offer a basis for state intervention. It follows that textual analysis of a given policy document must be supplemented by a broader overview of the contextual conditions that inform its design. Thus, the ‘objects and reasons’ identified as warranting the need for PECA 2016; the discursive construction of ‘unlawful’ user-generated content in RBUOC 2021; and the legitimation devices used to outline the need for a centralized cyber governance model represented by the PMDA concept note, are all contextualized using the infrastructure-interaction-information framework identified earlier.

5 Three-Tier Conceptual Framework
The conceptual framework presented for this study focuses on the interplay between ‘infrastructure, information, and interaction’ as themes informing the analysis of state-societal encounters in the shaping of the digital public sphere. The processual nature of this exchange, whereby both state and societal actors may be said to act on distinct, if at times divergent, ‘security’ ideations, is combined with a focus on the context in which the exchange takes place. This context, in turn, is characterized by categories encompassing both the physical, and virtual, dimensions of the digital public sphere as a transnational ‘space of flows.’ Thus, of the three tiers outlined above, both information and infrastructure fall into the overarching context informing public policy design for regulating Pakistan’s expanding digital spaces through a content-focused approach. Under this context, information, as a category, emphasizes the
nomination of select content under a lawful/unlawful binary subject to top-down, state-led legitimization of the ‘objects and reasons’ underlying the same. The ensuing predilection toward state-centric ideation is further reflected in the ‘infrastructure’ category, whereby attempts at data-localization and state-controlled digitization initiatives in peripheral regions may be assessed as reasserting themes of state sovereignty in shaping transnational digital spaces. Consequently, public policy on the physical net infrastructure, as well as digital information flows, is colored by the question of territorialization and the question of state control over access to both. The context wherein the categorization of both information and infrastructure under state, versus societal, understandings of ‘security’ occurs is subject to broader geopolitical and geoeconomic trends, here seen through the lens of the ‘Digital Silk Road’ (DSR) of which the Pakistani state is a key member.

The state-centric nature of developmental projects under the DSR model, given the predominance of Chinese state-owned enterprises (SOEs) in concerning projects, has been addressed by scholars such as Patrick and Feng (2018). The role of Chinese companies in ‘digital’ developing economies may be analyzed through the increasing policy-relevance of state perceptions of ‘sharp power.’ Interpreted as a type of hard power, sharp power is grounded in a perception of information as a tool open to manipulation for hostile purposes (Patrick and Feng 2018). The advent of China as a lead innovator in physical ICT infrastructure may be studied alongside the tentative emergence of a ‘Chinese model’ of digital governance subject to state-centric interpretations of ‘securing’ digital spaces. Further, China’s DSR projects, under the BRI, stand to ‘export’ the policy implications of such a model to developing states possessed of weak legislative and judicial capacities. In light of this, attempts to structure the ‘digital public sphere’ in lead DSR states can be analyzed by problematizing both the categories used to sketch the margins of this sphere, as well as the processes informing state-societal interaction in and on the nature of digital spaces. ‘Interaction’ builds on the nature of information and infrastructure identified earlier to assess how the mechanisms, institutions, and procedures adopted for designing, implementing, and amending public policy, visualize the role of both state and societal actors. A top-down design lacking multistakeholder collaboration as well as effective feedback mechanisms is seen as impeding the agency of societal actors in ensuring a more multifaceted approach towards ‘security’ in state policy, especially as applied to an area as nebulous and broad-based as the digital public sphere. Thus, conceptual frameworks analyzing the nature of public policy as meaning laden texts subject to divergent interpretations by state and societal actors, enable critical readings of proposed policy with a view to addressing divergences in state-societal security approaches.

‘Infrastructure’ builds on how the nature of physical net infrastructure i.e., components for data storage, processing, and transfer such as data centers, fiber-optic cables etc., informs data governance models. Consequently, the manner in which physical components of digital spaces are sourced, and structured, ‘spills over’ into the design of digital regulation. Considering this, the Pakistani state’s predilection for centralized digital governance needs to be analyzed alongside infrastructural setups whereby the state-owned Pakistan Telecommunication Company Limited (PTCL) controls the Pakistan Internet Exchange (PIE). This is the country’s largest internet exchange point, having three main nodes in Karachi, Islamabad, and Lahore,
and an additional 42 nationwide. Until 2009, the PIE operated the nation’s only internet backbone. PTCL also controls access to 3 international undersea fiber-optic cables connecting Pakistan to the net. Thus, physical elements of cyber governance encompass questions of access and regulation, whereby inadequate or damaged components i.e., fiber-optic cables, coupled with geographic, gender, and socioeconomic inequalities, are indicative of disparate degrees of access to digital platforms. These disparities are particularly acute in ‘liminal’ spaces where state rehabilitation and reconstruction efforts are subject to slow progress. An attendant theme is how infrastructure debate informs questions of ‘cyber sovereignty’ vis-à-vis ‘cyber security’, particularly as data localization\(^6\) and protection laws gain prominence in domestic governance regimes.

Questions of ‘cyber security’ also inform how the second tier, interaction, is premised on state surveillance practices in the absence of democratic and judicial oversight. The uncertainty surrounding the nature and extent of existing cyber capabilities, with opacity adopted as a security tactic, coupled with lack of data protection laws in the Pakistani state, magnifies the potential for infringement of user privacy and freedom of expression. Track-and-trace measures adopted during the COVID19 pandemic were reflective of evolving surveillance capabilities combining call-monitoring and geo-fencing techniques, originally employed by intelligence bodies to address terrorism. Data collected is not subject to legal safeguards against state abuse, nor does the need for such safeguards feature prominently in state discourse on cyber governance. The primary focus of this discourse, especially in line with the role of digital spaces as public spheres, focuses on grading UGC with reference to such broadly defined objectives as ‘national security.’ To this end, legal instruments grant state authorities broad powers of censorship and punitive action against ‘unlawful’ content, as well as the ability to suspend internet services altogether in states of ‘emergency.’ The vagueness of statutory provisions identifying conditions warranting state intervention may be taken alongside the failure to incorporate judicial and legislative input for defining terms such as ‘national interest’ and ‘morality;’ despite these being repeatedly employed in constitutional articles cited in key instruments such as PECA 2016 and RBUOC 2021. The ensuing impact on state-citizen interaction in the ‘digital public sphere’ favors a top-down model of spatial structuring, decried by rights-based groups as endangering fundamental user, i.e., ‘human’ rights, at the behest of abstract, opaque iterations of ‘state’ or ‘national’ security. Additionally, an overt content-centric focus vis-à-vis security considerations is seen to sideline the vulnerability of critical infrastructure to cybercrime e.g., the discovery in 2020 that access to the state flag carrier’s, the Pakistan International Airlines’ (PIA) database, was being sold online on the dark web by Russian hackers. Added to this are concerns surrounding the role of the Pakistan Telecommunications Authority (PTA) as the body mandated to regulate the internet in Pakistan, and whether the nature and scope of its function serves to safeguard human rights.

The third tier, information, examines the discursive construction of the goals of state public policy, and how these reflect normative conceptualizations of society and social relations. Instruments for implementing state policy, such as the RBUOC 2021, draw on specific

\(^{6}\) Data localization is here taken to refer to a state mandating that select categories of data be housed on its own territory in order to ensure jurisdictional control over the same.
imaginings of state-society relations bounded by state perspectives of prevalent sociopolitical and economic contexts. The constitution, contestation, and containment of ‘crime’ or ‘unlawful content’ in digital spaces draws on a specific mode of argumentation and deliberation employed by policy actors using select legitimation techniques. Thus, states attempt to ensure institutional practices vis-à-vis content regulation resonate with wider social subjectivities i.e., beliefs, institutions, relations etc. Themes identified as warranting state intervention are constructed using language that allows a broad margin for state action. The use of expansive, referentially vague context identifiers such as ‘glory’ (i.e., action against content that violates the ‘glory of Islam’) risk state overreach, especially in the absence of stringent judicial safeguards. Further, discourses shaping the nature and scope of the digital public sphere privilege select perspectives on, and applications of, these spaces over others, drawing on particular interpretations of past state experiences with the same. Considering this, rules defining the ‘lawfulness’ of content emerging from online interaction aim to shape the function of ICT as a social structure, signifying usages which align with pre-suppositions of overarching state political imaginaries (i.e., Islamic welfare state). In light of this, state-societal interaction in, and on, the digital public sphere is based on a top-down model whereby legal, regulatory, and technical controls are the dominant strategies for cyber governance. Societal actors, including digital rights activist groups such as Digital Rights Foundation (DRF), have argued for the need for a more holistic, multistakeholder approach, incorporating economic models for ensuring the sustainability of independent media, as well as investment in media literacy programs and critical infrastructure.

6 Overview of Textual Data
The content regulatory landscape in Pakistan has been subject to a major shift in the form of the RBUOC Rules, notified in 2020 as an expansion of state powers identified in section 37 of PECA 2016. PECA itself was drafted under the overarching impact of the Army Public School (APS) terrorist attack in December 2014, when Tehrik-e-Taliban Pakistan (TTP) fighters stormed a school in Peshawar and massacred 150 people, an estimated 134 of whom were children. The incident prompted the launch of a 20-point agenda titled the ‘National Action Plan’ (NAP) for countering terrorism and extremism. Points 5, 11, and 14 broadly address the impact of content, disseminated through both print and electronic media, in propagating ‘hatred, extremism, sectarianism, and intolerance’ (Point 5), as well as ‘glorification of terrorists and terrorist organizations’ (Point 11). Point 14 identifies the need for ‘measures against abuse of internet and social media for terrorism.’ To this end, PECA presents an attempt to curb ‘unlawful content’ online, with Section 37 granting broad powers to the PTA for blocking and removing the same. Section 10, pertaining to cyber terrorism, is to be applied with reference to Sections 6 (unauthorized access to critical information infrastructure systems, 

7 In the lead-up to general elections in July 2018, the website of the leftist Awami Workers Party (AWP) was blocked, prompting the party to register a complaint with the Election Commission of Pakistan (ECP). The website was restored thereafter, though the PTA provided no explanation for having blocked it in the first place. In 2019–20, the body blocked 27,986 URLs that ‘contained hate speech, insulted the glory of Islam, were considered indecent or immoral, or threatened Pakistan’s national security.’ To date, no public database exists to list such sites, leading to a need to assess information on blocks on a case-by-case basis.
8 Pakistan Media Development Authority Ordinance, 2021 - Position Paper - (digitalrightsfoundation.pk)
9 https://nacta.gov.pk/nap-2014/
or data), 7 (unauthorized copying or transmission of critical infrastructure information data), 8 (interference with critical infrastructure information systems or data), and 9 (glorification of an offence). Daudpota (2016) comments on the need for criminal laws to explicitly state conduct amounting to a punishable act, with vagueness in relevant statutory provisions risking rendering sections of the law void. As per his analysis of PECA 2016, the blanket authorization empowering the PTA to block access to any online information, sans court orders; and the ability of the federal government to issue ‘directives’ to the owner of any information, with violation seen as a punishable with imprisonment and/or fines, potentially stand to violate due process of the law.

With regard to how digital spaces feature in national understandings of internal security policy design, the National Internal Security Policy II (2018-2023) engages with the theme of ‘cybercrime’ and how it pertains to violent extremism. NISP II’s emphasis on ‘securing’ cyberspaces may be analyzed alongside the National Counter Terrorism Authority’s (NACTA) release of the National Counter Extremist Policy Guidelines (NCEP) in 2018, and the importance accorded to designing an ‘online behavior code of ethics’ therein. NISP II’s 6Rs strategy identifies the threat of ‘cybercrime’ in conjunction with the use of cyberspaces as a domain for the rapid dissemination of extremist ideologies to wide audiences. Two of the Rs, ‘Reorient’ and ‘Reimagine,’ repeatedly cite the need to ‘secure’ cyberspaces, explicitly identifying their use by extremist groups to ‘influence the masses, gain sympathy, recruit, and obtain funding’ (NISP II 2018, p.9). One of the three areas highlighted for state action concerns the ‘ideational domain,’ based on which NISP II recommends modernizing state security apparatus. The focus on ‘securing’ cyberspace, as developed in the ensuing recommendations, relies predominantly on surveillance and censorship, with a key strategy under the ‘Reorient’ strand being to resource and empower the Federal Investigation Agency (FIA) to monitor social media sites for curbing unlawful activities. While there is mention of the need for campaigns to promote ‘public awareness,’ it remains underdeveloped in favor of an emphasis on improving the capacity of the PTA, as chief net regulator, to ‘secure’ online spaces and thereby curb provocative statements and hate speech. The ‘Reimagine’ strand cites a similar trajectory for media regulation, with the Pakistan Electronic Media Regulatory Authority (PEMRA) tasked with the strict enforcement of regulations pertaining to content containing hate speech, fake news, racial prejudice, and the glorification of terrorism/terrorist groups.

It may be argued that the overt focus on state censorship and top-down digital governance modes proposed in NISP II prompted an attempt for a more people-centric ‘inclusive’ approach in the form of NCEP 2018. The Guidelines identify the impact of media and communication as a key driver of extremism, citing the need to design an ‘online behavior code of ethics,’ both for the citizenry in general and for schools in particular. However, the precise nature of this code, and the processes and mechanisms underlying its design, are not defined, nor is any explicit mention made of how a general ‘code’ may be repurposed for training school children to better utilize cyberspaces. Paragraph 15 of the NCEP calls for a ‘campaign to develop capability to discern online good facts from bad facts’ as an essential accompaniment to computer literacy education. Paragraph 21, under ‘Education Reforms,’ reiterates this, arguing for an interactive learning model that educates young people ‘not to blindly follow the reality
presented online’ (NCEP 2018, p. 28) while serving to ‘enlighten them that all facts are not essentially correct and thus the rational application of mind is essential before venturing to associate with a certain opportunity given through online medium’ (ibid). It emerges that the binary between ‘good and bad facts’ is subject to state interpretation, with the citizenry afforded no recourse in negotiating the nature of the same. Similarly, the lack of feedback mechanisms premised on state-societal collaboration in designing the aforementioned ‘code’ serves to reassert the top-down nature of digital governance legislation outlined in NISP II. It may be argued that the themes presented in NISP II and the NCEP 2018 foreshadow the overt emphasis on state-centric ‘security’ ideation evidenced in attempts to ‘structure’ the digital public sphere in the RBUOC 2021.

The RBUOC Rules 2021, having recently been amended by the Ministry of Information Technology and Telecommunication (MOITT) following a severe backlash by civil rights groups10, seek to set out ‘safeguards, process and mechanisms’ for the exercise of the powers granted to the PTA under Section 37, PECA. In doing so, the Rules formalize the categories of ‘unlawful’ content identified as warranting state action, with the PTA granted ‘gatekeeping’ authority to determine the suitability of any and all content that may be allowed in the Pakistan digital space.11 Safeguards for freedom of speech and expression (Chapter II, RBUOC 2021, Section 4) merely reiterate the restrictions limiting freedom of speech in Article 19 of the 1973 Constitution; the same article having been quoted in Section 37, PECA. Further, the ensuing regulatory procedure grants the PTA the power to interpret and apply exceptions – the exercise of a judicial, if not legislative, function, which may be argued to go beyond the body’s original mandate.12 Given below is a page from the draft complaint form included in the RBUOC Rules for the reporting of unlawful content under identified categories:

---

Select Category
- Against Glory of Islam
- Against Integrity, Security or Defense of Pakistan
- Against Public Order
- Against Decency or Morality
- Contempt of Court
- Commission of an offence under PECA, 2016
- Offences against dignity of a natural person
- Offences against modesty of a natural person
- Child Pornography
- Cyber Stalking
- Others

Description of Social Media Platform/Application

Enter Social Media Platform/Application Name
Submit

Figure 1: Content Categories (Source: RBUOC Rules 2021)\(^{13}\)

Individuals, ministries, federal, provincial, or local government departments, as well as law enforcement and intelligence agencies may all file complaints to the PTA over any content deemed as ‘objectionable’ in light of the given categories\(^{14}\), with state officials having been incorporated under the broad qualifier of ‘natural persons.’ Further, the identity of the complainant shall be kept confidential by the PTA, though the body will not accommodate anonymous complaints. The language, and chronological sequencing, of the identified categories may be analyzed alongside the discursive construction of ‘security’ in the RBUOC Rules.

7 Discussion and Analysis
The text for the RBUOC 2021 features four prominent usages of ‘security’ in connection with the nomination of a referent object needing to be ‘secured.’ Nomination is here taken to imply a ‘discursive construction of social actors, objects, phenomena, events, processes, and actions,’ using devices such as membership categorization, nouns, and verbs. (Reisigl and Wodak 2015: 33). All four usages nominate the ‘nation’ or ‘Pakistan’ as the main referent, citing content that ‘threatens’ the same, with the potential to disturb ‘public order’ as being subject to

\(^{13}\text{https://moitt.gov.pk/SiteImage/Misc/files/Removal\%20Blocking\%20of\%20Unlawful\%20Online\%20Content\%20Rules\%202021.PDF}\)

removal/blocking. The statement of objects and reasons included in PECA 2016 makes explicit mention of the Act’s contribution to ‘the national security of the Nation,’ while identifying the need for ‘strengthening existing protections and establishing new safeguards especially against abuse of these new and intrusive powers.’ Statements by global, and domestic, bodies advocating for digital rights highlight the failure of the RBUOC to institute such safeguards, with bodies such as the Global Network Initiative (GNI) urging the Pakistani government to ‘rescind the Rules and undertake open, transparent, and multistakeholder deliberations to inform effective, fit-for-purpose, and rights-enhancing regulation.’ While the state initially withdrew the 2020 Rules for instituting such a deliberative process, the amended 2021 draft kept in place all of the provisions and processual requirements that had been flagged by rights activist groups and media houses. This study analyzes three of these ‘red flags,’ each of which is placed under the overarching three tier model of ‘infrastructure, interaction, and information.’ These may be respectively identified as data localization, regulator independence, and vague statutory provisions categorizing ‘unlawful’ content.

7.1 Tier I: Infrastructure (Data Localization)

Data localization may be problematized as a question of state access to the data collected by global ICT powerhouses; housed in physical storage centers. It further addresses the impact concepts such as ‘sovereignty’ portend to exert on the state’s right to this access. The Asia Internet Coalition (AIC), a body aiming for better understanding of Internet policy issues in the Asia-Pacific, cites the deleterious impact of data localization on user privacy as well the quality of digital service provision. The amended RBUOC 2021 require social media companies to register with the PTA within three months, in addition to appointing compliance, and grievance, officers within the same time-period. Platforms, including Twitter, Facebook, TikTok, Google, and YouTube are further instructed to establish offices in Pakistan (preferably Islamabad) ‘as and when feasible’ (previously set at nine months). These companies are to “provide to the Investigation Agency designated or established under section 29 of the Act, any information or data or content or sub-content contained in any Online Information System owned or managed or run by the respective Service Provider or Social Media Company, in decrypted, readable and comprehensible format or plain version in accordance with the provisions of the Act” (RBUOC 2021, Chapter IV, Section 8 (4)). The Act referred to is PECA, with Article 29 falling under Chapter III detailing the procedural powers for investigation of suspected offences. The GNI analyzes how the RBUOC Rules exert significant legal pressure on companies to ‘remove content and share access to data’ in the face of broad enforcement powers granted to the PTA; standing to undermine existing liability protections granted to companies under PECA’s Section 38. Data localization has been discussed alongside data-sovereignty, particularly in the context of China’s model of digital governance and its tentative ‘spillover’ effects along the Digital Silk Road (DSR). Pakistan is a key partner in the DSR, with work on the Pakistan and East Africa Connecting Europe (PEACE) subsea cable system having commenced in March 2021.

---

15 https://globalnetworkinitiative.org/pakistan-unlawful-online-content-rules/
16 https://globalnetworkinitiative.org/pakistan-unlawful-online-content-rules/
17 https://www.arabnews.pk/node/1805946/pakistan
Digital connectivity remains a core aspect of the China-Pakistan Economic Corridor (CPEC); a key highlight of which is the China-Pakistan Cross Border Fiber Optical Cable connecting China with Pakistan through Gilgit Baltistan (GB), Khyber Pakhtunkhwa (KP), and Punjab. Erie and Streinz (2021), writing on the political and economic impacts of the BRI, identify a ‘Beijing Effect’ whereby the installation of Chinese built infrastructure in developing states is accompanied by an emulation of the People’s Republic of China’s (PRC’s) approach to a sovereignty-centric mode of digital content regulation – a key aspect of which is centralization. The tendency towards centralization highlighted in the given policy instruments, in addition to proposals for a Pakistan Media Development Authority (PMDA) floated in May 2021, is predicated on the need to ensure ‘national security.’ Local activist groups such as ‘Bolo Bhi’ and the DRF have decried the broad-based authority granted to the PTA in assessing the nature and scope of all online content vis-à-vis ‘security,’ while bodies such as the AIC cite the deleterious impact this stands to have on the socioeconomic potential of ICTs in Pakistan.18

7.2 Tier II: Interaction (PTA’s role as Regulator)
The PTA has been granted broad powers for structuring the Pakistani digital public sphere, including the ability to unilaterally act against content without a court order. While reasonable restrictions on fundamental rights, such as that of freedom of speech, are interpreted by the superior judiciary in the light of constitutional provisos, the 2021 Rules effectively hand over this authority to the PTA. The body has also been authorized to protect ‘the glory of Islam’ with recourse to the blasphemy laws and secure ‘public order’ by acting against content deemed in violation of Chapter XIV of the Pakistan Penal Code 1860 i.e., ‘public health, safety, convenience, decency, and morals’19 as well as false information (sans definitions). Further, the rules outline a 48-hour period for social media companies to comply with the PTA’s instructions against objectionable content, barring which the body has the authority to impose blanket blocks on entire platforms. Non-compliance carries heavy fines of up to Rs 500 million. Complainants may include ‘include a Ministry, Division, attached department, sub-ordinate office, provincial or local, department or office, a law enforcement or intelligence agency of the Government, or a company owned or controlled by the Government’ (RBUOC 2021, Section 3 (1) (iii)). While the right to review has been provided in Chapter V, RBUOC 2021, the body tasked with carrying it out is the PTA itself, failing which, an appeal may be filed with the higher courts.

In light of this, the nature and composition of the PTA, as lead regulatory body, is essential in ensuring a free, independent, and fair environment for state-citizen interaction in the digital public sphere. The authority reports to the MOITT, and is comprised of three persons, a chair and two members, all appointed by the Prime Minister. As per Freedom House, ‘common government practice is to appoint retired military personnel as the heads of government departments, part of the military’s efforts to expand its regulatory capacity in most spheres of Pakistani governance’ (Freedom on the Net Report 2021)20 The current chairman is retired Major General Amir Azeem Bajwa. The Freedom House 2021 Report on the state of internet

18 https://perma.cc/B2WT-DVB5
20 https://freedomhouse.org/country/pakistan/freedom-net/2021#footnote1_woxsywy
freedom in Pakistan also highlights how the PTA, in violation of PECA’s legally mandated oversight mechanisms, seldom issues notices when restricting content, impeding the process of appeal or judicial review for those affected. Internet Service Providers (ISPs) must comply with blocking orders as a condition of their licenses, with blanket provisions in a 2015 telecommunications policy allowing the PTA to monitor and manage any content “in conflict with the principles of Islamic way of life as reflected in the Objectives Resolution and article 31 of the Constitution” (Freedom on the Net 2021). The RBUOC Rules place global social network sites (SNS) on par with local ISPs, establishing the same modus operandi for regulating the role played by both. In such a context, state-citizen interaction in the digital public sphere presents an increasingly top-down model of centralized control, with the potential to criminalize dissent or critique under overt securitization practices. In post-conflict zones lacking effective state presence in terms of service delivery, a punitive attitude towards criticism or rights-based mobilization risks jeopardizing much-needed trust in state institutions. Therefore, an emerging trend in state behavior to shut off internet connectivity altogether in times of social unrest or conflict makes for a troubling precedent.

In April 2021, the Ministry of Interior directed the PTA to block all major social media platforms, including Twitter, Telegram, WhatsApp, Facebook, and YouTube, in order to ‘maintain public order’ in the face of protests by Tehreek-i-Labbaik Pakistan (TLP). Suspension of mobile services for security measures on public events such as the Pakistan Day parade, and religious holidays such as the ninth and tenth days of the Islamic month of Muharram, is commonplace. In July 2020, the Ministry of Interior ordered the PTA to enact a network shutdown during protests in Chaman, Baluchistan, citing the upload of ‘anti-state’ materials online. Several districts in Baluchistan have lacked access to mobile data service since February 2017, while long-term shutdowns are also prevalent in restive border regions for ‘national security.’ Section 54 of the Pakistan Telecommunications Act authorizes the state to suspend internet services during emergencies, prompting the Islamabad High Court (IHC) to hold in a February 2018 ruling that routine shutdowns under the pretext of public safety infringed upon the citizenry’s fundamental rights and were illegal. This verdict was overruled by the Supreme Court in April 2020. Thus, the state’s authority to unilaterally suspend/ban both individual platforms, as well as access to the net as a whole, further impedes the structuring of a digital public sphere allowing multistakeholder involvement for rights-centric interaction and engagement.

7.3 Tier III: Information (Vague Statutory Provisions categorizing ‘Unlawful’ Content)

Unilateral action also features as a key concern in the light of the RBUOC 2021’s blanket authorization for the PTA to categorize any and all content under a lawful/unlawful binary premised on vague statutory provisions. These provisions are to be prioritized over SNS content guidelines developed by platforms such as Twitter and Facebook for transnational user communities, a move that, according to the GNI and AIC, risks isolating Pakistan from the global digital space. As per the RBUOC 2021 draft, “The direction, issued by the Authority under the Act and under these rules, shall prevail and take precedence over any contrary

---

Community Guidelines and such Community Guidelines shall be deemed to be of no legal effect.” (Ch. II Sec. 4 (2)) The direction identified extends to any and all content, with the PTA having the broad authority to ask ISPs and social media companies (SMCs) for information including “subscriber information, traffic data, content data and any other information or data” (RBUOC 2021, Ch. IV, Sec. 8 (4) Exp.) subject only to ‘justifiable technical limitations.’ Further, ISPs and SMCs must deploy mechanisms for the immediate blocking of live streaming content, “particularly related to terrorism, extremism, hate speech, pornographic, incitement to violence and detrimental to national security on receiving intimation from the Authority” (RBUOC 2021, Ch. IV, Sec. 8 (5)) Given the absence of any role for the judiciary in interpreting these restrictions, the PTA purportedly possesses the broad authority to do so, using such specific instruments as the criminal code. As per Usama Khilji, Director of Bolo Bhi, content in violation of the “integrity or defense of Pakistan” is to be processed using colonial clauses from the Pakistan Penal Code (PPC) including ‘sedition.’ Given how the digital public sphere presents a space for discussion on issues that may be censored from the mainstream media, the lack of effective oversight and transparency outlined above creates a precedent for criminalizing criticism of state policy in and of itself. Further, discussion and mobilization on societal issues deemed taboo under ‘prevalent standards of morality and decency’ may be subject to punitive action as has been witnessed in 2020-21.

Pakistan’s 2021 ‘Aurat March’ (Women’s March), held in commemoration of International Women’s Day (March 8th) was the target of a campaign of misinformation prompting accusations of blasphemy. Doctored photos of campaigners carrying purportedly blasphemous slogans were uploaded and shared widely online, with Twitter acting as a key site for dissemination. The proposed model for shaping the state’s ‘digital public sphere’, under PECA 2016, the RBUOC 2021, and the proposed PMDA, risks subverting much-needed debate on issues involving minority rights and gender inclusivity under such abstractions as ‘morality.’ The Freedom House 2021 Net Freedom Report identifies the potential of this sphere for community mobilization on issues barred from mainstream media, highlighting the example of the Pashtun Tahaffuz Movement (PTM), a group organized on the need to address human rights violations of Pakistan’s Pashtun ethnic minority. The PTMs online presence is key to circumventing a complete blackout in print and electronic media, in order to ensure a wider dissemination of its concerns and objectives. Nonetheless, its activists have been subject to arrest, including for ‘anti-state activity through social media’ under PECA Sections 9 and 10. As per Freedom House’s 2021 ‘Freedom on the Net’ Report for Pakistan, “Political speech, such as criticism of the government, judiciary, or the armed forces, has been subject to legal action.” While dis/misinformation remain key concerns vis-à-vis digital spaces, a regulatory approach premised on blanket censorship and content removal may obfuscate the state’s potential to capitalize on the potential of the digital public sphere to enable better governance, as well as socioeconomic uplift. Further, attempts at data localization, in lieu of ‘data sovereignty’, cannot sustain in the face of Pakistan’s reliance on global ICT powerhouses and

---

24 https://freedomhouse.org/country/pakistan/freedom-net/2021#footnoteref17_r65q4cf
the prevalence of digital technologies across social, political, and economic sectors. In the case of China, the PRC’s role as lead innovator in cutting-edge ICT enables it to sustain a digital media regime premised on cyber sovereignty. The ‘Made in China 2025’ plan aims for complete self-reliance in high-tech sectors, while allowing China to play an increasingly important role in standard-setting through bodies such as the International Telecommunication Union (ITU).

7.4 Context and Policy Design: Impact of the DSR

According to a January 2021 piece by Nikkei Asia, four of the seven submarine cables connecting Pakistan to the web come out of India.25 The piece cites a 2017 statement by Major General Amir Azeem Bajwa, then Director General (DG) of the Special Communications Organization (SCO), highlighting the security risk posed by routing much of Pakistan’s internet traffic through India.26 As part of CPEC and the DSR, Pakistan is among the first of the PRC’s partner states to shift to the Chinese dual-purpose navigation system, BeiDou, from the US-based Global Positioning System (GPS); allowing the state access to precise geospatial application for surveying and construction etc. Additionally, the PEACE fiber optic cable discussed earlier is being installed by the Hengtong Group, at the head of a tech consortium of companies from Africa, Hong Kong, and Pakistan. This is to be connected to a cable being laid by the SCO, in partnership with Huawei Technologies, connecting Rawalpindi to both Karachi and Gwadar. 850 km of cable already connect the Xinjiang Uyghur Autonomous Region with Rawalpindi, providing secure communications between Pakistan and China. Projects under the DSR are geared towards providing Pakistan’s Gwadar port with fiber optic connectivity in its quest to become a regional transit hub. As previously noted, digital ‘public spheres’ rely on non-digital infrastructures, making them a function of the physical infrastructure that gives rise to the digital domain. According to Tung-Hui Hu, “We may imagine the digital cloud as placeless, mute, ethereal, and unmediated. Yet the reality of the cloud is embodied in thousands of massive data centers, any of which can use as much electricity as a midsized town.” (Abstract, 2015)

Thus, Erie and Streinz (2021) highlight how China’s ‘Great Firewall’ (GFW) is in fact a compendium of technical and legal standards aimed at asserting a desired extent of control and draws on China’s ability to manufacture critical components informing both. In commenting on China’s assessment of the importance of transnational data flows for trade and development, the authors argue that the PRC, while cognizant of the same, maintains that such flows be subject to the precondition of security. In light of this, China has grown increasingly assertive in promoting its data governance concepts in international institutions such as the Internet Corporation for Assigned Names and Numbers (ICANN) and the International Engineering Task Force (IETF). It has also started to promote a ‘value-centric’ understanding of global governance by creating its own institutions for multilateral cooperation, in parallel to those established by the USA, such as the Silk Road Fund and the Shanghai Cooperation Organization (SCO) etc. Added to this is China’s launch of the ‘Wuzhen Summit’ in Zhejiang

26 Ibid.
Province, an annual conference seen as a means for China to popularize its vision for global data governance among representatives of both the developed and developing world. According to Erie and Streinz, “China’s discursive reshaping may further assume normative form, such as in the “International Strategy on Cooperation on Cyberspace” of 2017, which identifies “sovereignty” (zhuquan) as a cornerstone for international coordination on cyber issues.” (2021: 26). A comprehensive assessment of any such normative (re)structuring remains difficult, seeing as how core materials for DSR projects (memoranda of understanding etc.) remain inaccessible. Nevertheless, as states such as Pakistan look toward innovative digital technologies as a means of generating socioeconomic uplift, they must design governance models for regulating expanding digital spaces. In light of this, the impact of DSR and CPEC projects on the shaping of Pakistan’s nascent digital ‘public sphere’ forms a key avenue for further study.

8 Conclusion
This study aimed to problematize the impact of divergent state-citizen perspectives on the construction of public policy. Taking SNS as a key site of contestation for this divergence, it examined the instruments for structuring Pakistan’s nascent ‘digital public sphere’ through a state- versus human-centric conceptualization of ‘security.’ It follows that the choice of language in policy instruments, such as the RBUOC 2021, shapes, and does not simply represent, policy priorities. In light of this, the study explored the categories used to construct ‘unlawful’ content, and attendant legitimation devices warranting blanket authorization for unilateral action by the PTA as the chief regulator. Given Pakistan’s attempt to accelerate digitization under CPEC and the DSR, as well as the role digital technological innovation is poised to play in generating opportunities for socioeconomic uplift, the regulatory impact of infrastructure on governance is also discussed.

As the PRC’s DSR projects undertake the construction of data infrastructure in developing states around the world, these partner states are faced with the need to develop models for data governance including mechanisms for content regulation. China’s role as a leading technological innovator in ICT must be taken alongside its increasing assertiveness in promoting a ‘sovereignty-centric’ vision of the internet. While the Chinese state premises its indigenous cyber governance on a dynamic and complex combination of technical and legal standards, its DSR partners exhibit disparate capacities to emulate the same, based on a varied landscape of legal and political systems. In light of this, the portended impact of DSR projects on governance models in states faced with sociopolitical unrest and a history of violent conflict makes for a pertinent avenue of further study. The centralization inherent in a tentative ‘China model,’ coupled with the PRC launching parallel multilateral governance institutions to those established by the USA, risks the emergence of two, potentially non-interoperable models of global digital governance. In light of this, Pakistan’s participation in BeiDou, as well as major DSR fiber-optic projects, makes it a critical site for exploring the evolution of digital governance under the regulatory effects of infrastructure. Further, the state’s drive to design a centralized, security-centric model for content regulation affords a key opportunity for examining the governance potential of ‘digital public spheres.’
The paper aimed to engage with the nature of Pakistan’s digital policy as premised on a state-centric conceptualization of ‘security.’ It examined how the physical infrastructure underlying the internet serves to shape state policies on digital governance. This was followed by an analysis of how language used in policy design exercises a formative or generative influence in shaping, and not merely representing, the action of state and rights-based groups interacting over digital spaces. An attempt has been made to problematize the nature of this design through an infrastructure-interaction-information conceptual tier, using key statutory provisions drawn from PECA 2016 and the RBUOC Rules 2021. Potential areas for further inquiry may problematize the launch of local e-governance applications and their impact on policy reform, while also exploring additional devices, such as information manipulation, for shaping state-citizen interaction in digital spaces.

Reference List


Daudpota, Faisal. 2016. An examination of unconstitutional aspects of Pakistan’s cybercrime law. SSRN. https://dx.doi.org/10.2139/ssrn.2860954


