Authoritarian Diffusion and Cooperation within International Organisations: Legal Harmonisation of Internet Sovereignty Policies within the Countries of the Shanghai Cooperation Organisation

Thomas-Colquhoun, Ewan

Veröffentlichungsversion / Published Version
Arbeitspapier / working paper

Arbeitspapiere des Osteuropa-Instituts
Arbeitsbereich Politik

Ewan Thomas-Colquhoun

Authoritarian Diffusion and Cooperation within International Organisations

Legal Harmonisation of Internet Sovereignty Policies within the Countries of the Shanghai Cooperation Organisation

94/2024

Freie Universität Berlin

Authoritarian Diffusion and Cooperation within Regional Organisations: Legal Harmonisation of "Internet Sovereignty" Policies within the Countries of the Shanghai Cooperation Organisation

About the author:
Ewan Thomas-Colquhoun
Freie Universität Berlin
ewan.tc@hotmail.co.uk

Abstract:
This paper explores the concept of "internet sovereignty" as developed and endorsed by the member states of the Shanghai Cooperation Organisation (SCO). First, the concept is shown to have developed as a synthesis between the restrictive Chinese internet governance model based on the "Golden Shield" and Russian conceptions of national "information spheres". Research then shows how this "sovereignty" model serves to legitimise refocusing internet governance around the state, allowing for stricter controls on internet access, content, data, and infrastructure in authoritarian contexts. Using causal process tracing, this paper shows that the SCO supports the transfer of digital policy between members based on this normative "sovereignty" model, the alignment of states with the legalised form of this model in institutional documentation, and the transfer of the legitimising "Three Evils" narrative frame. This shows that regional organisations can provide a significant platform for authoritarian learning, which, when successful, helped the regimes of the SCO to find policies to expand and stabilise their control over the digital realm.

Keywords:
digital authoritarianism, internet sovereignty, norm diffusion, authoritarian learning

OSTEUROPA INSTITUT

Arbeitspapier 94/2024

Abteilung Politik am Osteuropa-Institut der Freien Universität Berlin

Ewan Thomas-Colquhoun

Authoritarian Diffusion and Cooperation within Regional Organisations

Legal Harmonisation of "Internet Sovereignty" Policies within the Countries of the Shanghai Cooperation Organisation

Freie Universität Berlin

Ewan Thomas-Colquhoun (2024) Authoritarian Diffusion and Cooperation within Regional Organisations: Legal Harmonisation of "Internet Sovereignty" Policies within the Countries of the Shanghai Cooperation Organisation. Arbeitspapiere des Osteuropa-Instituts (Abteilung Politik) 94/2024. Freie Universität Berlin 2024.

Impressum

Arbeitspapiere des Osteuropa-Instituts, Freie Universität Berlin
Abteilung Politik

Garystraße 55
14195 Berlin

Redaktion: Alexander Libman
alexander.libman@fu-berlin.de
Lektorat/Layout: Alexander Libman

Table of Contents

Abbreviations, Tables and Figures

China: The People's Republic of China
CCP: The Chinese Communist Party
DPI: Deep Packet Inspection
DSR: Digital Silk Road
FDI: Foreign Direct Investment
India: Republic of India
ICANN: Internet Corporation for Assigned Names and Numbers
ISP: Internet Service Provider
ITU: International Telecommunication Union
Kazakhstan: Republic of Kazakhstan

Kyrgyzstan: Kyrgyz Republic
Pakistan: Islamic Republic of Pakistan
QCA: Qualitative Content Analysis
RATS: Regional Anti-Terrorist Structure (of the SCO)
RO: Regional Organisation
Roskomnadzor: Russian Federal Service for Supervision of Communications, Information Technology and Mass Media
Russia: Russian Federation
SCO: Shanghai Cooperation Organisation
SORM: System for Operative Investigative Activities
Tajikistan: Republic of Tajikistan
TCP: Transmission Control Protocol
UN: United Nations
USSR: Union of Soviet Socialist Republics
Uzbekistan: Republic of Uzbekistan
WIC: World Internet Conference

1 Introduction

In recent years, a growing amount of academic and public attention has been paid to the "Rise of Digital Authoritarianism" (Shahbaz, 2018) and the persecution of the established methods of authoritarian control within the relatively new and, certainly evolving, cyber landscape. Having moved on from an early focus on the democratising effect of the internet, particularly during discussions on the "third wave" (see Ferdinand, 2000; Shane, 2004; Best & Wade, 2009; Laidlaw, 2015), scholars have come to explore the ways in which illiberal internet governance can strengthen authoritarian regimes. Indeed, scholarship on hybrid regimes has led to the proposition of a new regime understood as "informational autocracy", which primarily uses controls on information to maintain stability, rather than violent coercion (Guriev & Treisman, 2019). Whilst the debate continues on the validity of such a typology, focus has rightfully come to settle on the unique advantages digital technologies give regimes to control their populaces, from propaganda through surveillance to overt cyber-attacks.

Within recent discussions of these authoritarian practices in cyberspace (see Michaelsen and Glasius, 2018), the concept of internet sovereignty[1] has often been evoked to grapple with the normative aspects of authoritarian internet governance. Academic discussion has generally focused on the idea of internet sovereignty as a set of norms or policies (Budnitsky & Jia, 2018; Flonk, 2021; Litvinenko, 2021) employed, although not exclusively, by the authoritarian regimes of China and Russia to exert control over digital data flows (Flonk, 2021; Litvinenko, 2021; Shcherbovich, 2021) and digital infrastructure (Stadnik, 2021; De Nardi & Musiani, 2016; Kolozaridi & Muravyov 2021). Budnitsky and Jia's (2018) study, which was the starting point for the analysis of this thesis, describes these norms as the brand of "internet sovereignty", a means of marketing an alternative model of internet governance and promoting the "national brands" of China and Russia as "rising digital powers".

This thesis extrapolates from this marketing terminology and questions whether other authoritarian states are a receptive "target audience" for internet sovereignty. This assertion is built from the field of research looking into authoritarian learning, which applied earlier ideas from studies of policy transfer in democratic states to authoritarian contexts (Hall & Ambrosio, 2017). This theory contends that authoritarian regimes, with their primary concern staying in power (von Soest, 2015), "adopt survival strategies based upon the prior successes and failures of other governments" (Hall & Ambrosio, 2017). Within this field, focus has been paid to the concept of "authoritarian diffusion", a subsection of the learning literature, which focuses on the networks through which policies transfer between regimes and facilitate future adoption (ibid. pg. 148). This theory has been used to suggest that authoritarian regimes seek to maintain internal stability by bolstering the capacity of neighbouring states to resist democratisation through repressive practices (Hall, 2023). As such, policy transfer between authoritarian states becomes a means to maintain domestic control. Within this paradigm, the "legal harmonisation" from this thesis' title is the methodology used to test to which extent separate legal regimes agree and, therefore, measure how much policy transfer has taken place (Lemon & Antonov, 2018). Assuming high degrees of legal harmonisation are present, researchers can begin to analyse the processes of diffusion between states.

As with any discussion on processes, however, it is important to consider the mechanisms through which this policy transfer could take place. Early studies in democratic

[1] This dissertation uses "internet sovereignty" as a catch all term for the application of traditional sovereignty practices to the digital sphere, informed by the Russian term "suverrenyi internet". "Cyber sovereignty", as preferred by the Chinese, as well as "digital" and "network" sovereignty should all be understood as interchangeable with this term.

states showed that regional organisations (ROs) are a significant institution for facilitating policy transfer (Peevehouse, 2005; Börzel & Risse, 2014). As such, scholars on authoritarianism have also come to look at ROs as possible institutions for promoting transfer (Lemon & Antonov, 2020; Debre, 2021; Hall, 2023). Taking the earlier assumption, therefore, that Russia and China are actively promoting the concept of internet sovereignty, it is logical to assume that a RO of which they are both members could be a fertile ground to test these theories. As such, building on this previous research, this study is intended to test the impact of this "brand" on the diffusion of internet sovereignty policies within this "League of Authoritarian Gentlemen" (Cooley, 2012) which according to the literature would seem receptive to such norms (Lewis, 2012; Karmazin, 2023; Hall, 2023), namely the Shanghai Cooperation Organisation (SCO).

Founded as the successor to the Shanghai Five, this organisation comprises China, India, Iran[2], Kazakhstan, Kyrgyzstan, Pakistan, Russia, Tajikistan, and Uzbekistan, and was ostensibly established as a mechanism to resolve security issues in the post-1990 environment in Central (and now Southern) Asia. With time, this organisation has taken a more active stance at integration, providing mechanisms for greater security and economic cooperation between members. Importantly for this thesis, it has been shown in this more advanced role to provide a platform for the transmission of authoritarianism to member states (Ambrosio, 2008, 2018; Aris, 2008; Hall, 2023). At the same time, whilst digital policy has been often mentioned as an area in which these states could be making use of this platform for diffusion (Budnitsky & Jia, 2018; Hall, 2023), there are yet very few empirical studies testing these assumptions. Therefore, the SCO is a strong case study to test the assertations of the literature on internet sovereignty as a concept, as well as interrogate the role of ROs in authoritarian learning. These key issues directed research and lead to the formation of the following questions, which follow logically and guided the analytical process. Q1: To what extent are internet sovereignty laws harmonised within the SCO? Q2: What evidence is there of the SCO having created a framework for diffusion to cause this harmonisation? Q3: What possible mechanisms could cause diffusion to be taking place?

As well as being a logical means to expand on these questions and test these previous ideas, this paper also fills a significant research gap. Some scholars (Stadnik, 2021; McKune and Shazeda, 2018) have called for further comparative research on the impact of Russia's

[2] The Islamic Republic of Iran; having joined the SCO on the 04.07.2023, was excluded from research as there was not enough data to involve the country in this study.

cyber norms, with a particular focus on the countries of the former Soviet Union and Central Asia (Litvinenko, 2021). Simultaneously, this case can expand the scientific understanding of authoritarian ROs, as discussed above, which, whilst remaining a small field, has attracted increased scrutiny in recent years (Söderbaum, 2004; Acharya & Johnston, 2007; Cooley, 2015; Obydenkova & Libman, 2019; Debre, 2021). Specifically, this study focuses on the ability of such organisations to institutionalise information exchange between autocrats by providing a regular forum for dialogue between policymakers (Obydenkova & Libman, 2018), or a "learning room" as described by Hall (2023). This focus on norm and policy transfer within an authoritarian organisation, and "authoritarian diffusion", is discussed in detail in Chapter 2.1 "Authoritarian Learning, Diffusion and the Logic of Authoritarian Regional Organisations".

Alongside these contributions to the scientific literature, this thesis also has the potential to produce insights relevant to the current geopolitical landscape. This arises from the frequent opposition cast between the authoritarian "internet sovereignty brand" and the prevailing democratic model of internet governance – multistakeholderism. Often portrayed as a natural opposition, the models place different actors at their centre and are promoted by states in open competition. Multistakeholderism involves multiple groups influencing the dialogues around, decision making for, and implementation of governance regimes, while the norms of internet sovereignty place the state at the centre of decision making (Van der Spuy, 2013). With proponents of multistakeholderism predominantly in the democratic West, and those of internet sovereignty in the non-democratic East, some scholars have intimated the formation of "blocs" around competing models of internet governance (McKune, 2015; Kolozaridi & Muravyov, 2021; Budnitsky and Jia, 2018), particularly inside international institutions such as ICANN, the WCIT and ITU (Glen, 2014; Flonk, Jachtenfuchs & Obendiek, 2020; Nanni, 2022). Indeed, in the latter, the sovereignty model has been shown in some cases to outcompete liberalism for votes internationally (Hulvey, 2022). There is, therefore, a practical requirement to understand the nature of this concept, if, as is argued, it is to draw such significant geopolitical battle lines going forward. Any conclusion drawn on the effectiveness of the SCO at spreading these norms could, therefore, have significant implications for responses to the organisation's expansion, an aim discussed in both Russian and Chinese doctrine (Kaleji, 2023; Wong, 2023), and could be applied to other organisations such as BRICS (see Polatin-Reuben and Wright, 2014; Belli, 2021).

To address these issues, the theoretical section of this thesis, Chapter 2.2 "Internet Sovereignty – Cyberspace, the Nation State and Authoritarian Responses", reviews the literature on the concept in the members' national contexts to synthesise a precise definition of

internet sovereignty for analysis. The Chinese model is analysed with reference to norm analysis (Zeng et al. 2017; Dragu & Lupu, 2021; Moore, 2022) from the concept's first introduction at the Wuzhen Internet Conference (2014). Russia and Central Asia are analysed concerning the earlier concept of "information security", with India's "digital sovereignty" discussed with reference to post-colonial narratives (Prasad, 2021). Pakistan, meanwhile, was the outlier of this group in being the only member state without a developed internet sovereignty concept. Ultimately, this section defines internet sovereignty as a collection of authoritarian internet governance norms, in which the state has control over its own delineated digital territory, a segregated "information space", to be protected in the interests of the state itself and which justifies digital authoritarian practices. From these norms, this section and the subsequent Chapter 3.1 looking at "Cyber Norm Development in the SCO and the Mechanisms of their Diffusion" describe four types of policies ratified by member states that contribute to regimes being able to control cyberspace, namely (1) access, (2) content, (3) data, and (4) infrastructure.

In this framework, the harmonisation of legal regimes between members is revealed and, with specific reference to contextual events, the overarching hypothesis of this study, that the SCO provides a platform for diffusion, is tested. Building on the authoritarian diffusion literature, this section also develops several possible internal and external mechanisms for diffusion, namely "direct exchange", "state-organisational alignment", "international legitimation" and "diffusion through practice", which form the analytical hypotheses. As problematised by Ambrosio and Tolstrup (2019), diffusion is "inherently causal", with the convergence of practices, isomorphism, remaining possible without any interference from external players and in the absence of learning processes. As such, evidence of these mechanisms is sought in the wider context of the SCO and related to the timelines of legal ratification, assessing whether institutional cooperation causes policy transfer. The discussion tests these assertions against alternative explanations for legal harmonisation, including, but not limited to: legal culture, similar domestic circumstances, technological factors, and the influence of the multistakeholder governance model. This focus on both internal and external mechanisms reduces the chance that claims to "spurious diffusion" are made, as it actively tests for the existence of alternative mechanisms not considered in the hypothesis, rather than cherry-picking evidence to support claims.

Based on these limitations and the theoretical framework discussed above, several hypotheses were produced to be tested in the analysis of the empirical findings, which explore the mechanism for diffusion: the harmonisation hypothesis (H1), the direct exchange

hypothesis (H2), state-organisational alignment hypothesis (H3), the international legitimation hypothesis (H4) and the diffusion through practice hypothesis (H5). The confirmation of both H1 and then any one of H2, H3, H4 or H5, as well as in combination, would contribute to resolving the main research question of this study, namely, H6: that the SCO provides a significant platform for the diffusion of authoritarian internet sovereignty practices.

The focus from these hypotheses on the causal mechanisms driving legal harmonisation informed the methodology chosen for the empirical analysis of this study, as described in Chapter 3.2. First, data for each member were collected in a three-step expansive process pertaining to the four categories of internet sovereignty policy, derived from empirical research: access, content, data, and infrastructure control. 100 laws were collected[3], with (11) for China, India (6), Kazakhstan (18), Kyrgyzstan (6), Pakistan (11), Russia (32), Tajikistan (7), and Uzbekistan (9). These laws were then analysed using QCA with sub-categories of specific provisions further dividing the four main categories (Schreier, 2012). Amongst others, these included: for access control, internet shutdowns, and licencing; for content control, defamation, "false information" and censorship laws; for data control, data localisation and surveillance, and for infrastructure, state network ownership and the mandatory installation of technical equipment. Having been analysed according to this coding frame, timelines of ratification of these laws were produced to be able to identify the policy innovators in these subcategories, as well as instances of later adoption. In situations where there were significant textual similarities between the laws of countries X and Y, where Y could be shown to have enough knowledge of X's law to evaluate and adopt it, a case for possible diffusion was identified and H1, the harmonisation hypothesis, confirmed (Ambrosio & Tolstrup, 2019). These cases were then tested against the hypothetical mechanisms described above, as well as against alternative explanations to qualitatively ascertain causality and test the final hypothesis, H6. These findings are then analysed in the discussion to reflect on their implications for studies on authoritarian diffusion, ROs, and the literature on internet sovereignty.

The subsequent concluding remarks of this study confirm the diffusion hypothesis for specific instances within the data, including the "Three Evils" which drove state-organisational alignment and rhetorical harmonisation. Similarly, cooperation in cybersecurity drills had a significant effect by driving diffusion through practice, whereby data retention and user identification strategies were transferred to allow "best practice" in surveillance. Limitations were also found, with reference to the role of the SCO in supporting alignment of legitimation

[3] For a full list see Appendix F.

narratives based on internet sovereignty norms, which stopped short of being a cause for diffusion. Directions for future research are then proposed, including a tighter focus on the role of data-rich tech companies in authoritarian regimes and the implications of the diffusion of authoritarian practices into democracy, taking the example of India from analysis. With a mind on international internet governance narratives, further organisations are suggested, including ASEAN and BRICS, research on which could provide insight into the potency of internet sovereignty norms going forward.

2 Theoretical Discussion and Literature Review

2.1 Authoritarian Learning, Diffusion, and the Logic of Authoritarian Regional Organisations

The key logic of authoritarian leaders is primarily that of regime survival (Olson, 1993; Levitsky & Way, 2002; Gallagher and Hanson, 2013; von Soest, 2015). In an economic sense, the ability of rulers to enrich themselves and allies has been shown to be a key motivation for gaining and remaining in power, with Olson's (1993) "stationary bandit" the prototypical autocrat. Stronger than the draw of this potential reward, however, is the risk associated with failure; as shown by history, deposed autocrats do not typically outlive their regimes by a significant length of time. As such, the consolidation and maintenance of power is their goal, with elections, if present, mostly a means to legitimise the existing government, rather than for the transition of power (Levitsky & Way, 2002; Gandhi & Lust-Okar, 2009; Pepinsky, 2013; Schedler, 2014). From these key tenets, theories have developed which describe the toolset authoritarian leaders have to maintain their control.

Gerschewski (2013) argues that autocrats rely on the "Three Pillars" of legitimation, co-optation, and repression, an assertion which forms the theoretical basis for this thesis. According to this theory, authoritarian leaders first try to persuade their citizens that they are the "right man[4] for the job" through legitimising narratives, whilst also "co-opting" the support of key political forces by offering a share of rents or other incentives. Then, should these strategies be unsuccessful, repression raises the cost of dissent to levels significant enough to dissuade mass mobilisation. As high-level categories, these "pillars" describe sets of tools which are used for regime stability, described by Glasius (2018) as "authoritarian practices". These are wide ranging, from law enforcement strategies, to propaganda, but are often

[4] Such leaders are almost exclusively male.

formalised through policymaking. Assuming, therefore, that these practices aid survival, it is logical for authoritarian leaders to implement as many as possible to consolidate control. With the cost of failure so high, however, internal trial and error of different practices is risky for developing the correct set of policies for control. As such, the idea developed that authoritarian leaders implement lessons from the successes and failures of other polities in a process described as "authoritarian learning", whereby authoritarian "best practice" transfers between states and rulers (Hall & Ambrosio, 2017).

After all, learning processes have been described in depth within democratic states (Dolowitz & Marsh, 1996; Dolowitz & Marsh, 2002; Evans & Davies, 2002; Marsh & Sharman, 2009), often concerning democratisation, which describes how policies transfer to bolster democratic processes (Börzel & Risse, 2014). This has often been combined with the concept of a "democratic peace", which argues democracies are more likely to peacefully coexist and cooperate with other democracies (Hegre, 2014). It follows that cooperation is easier with rulers that share your values. The logic behind this in autocracies, however, is subtly different. Democratic rulers do not face the same existential threat upon losing power as authoritarian leaders – there is always the next election. As such, whilst the theory from earlier research into democracies can provide a basis for understanding the learning processes of autocracies, separate ideas have been developed to describe "authoritarian learning".

As described in Ambrosio and Hall's (2017) literature review, this begins at regime survival and describes a process whereby autocrats apply the strategies of other states based on their assessment of successes and failures. Hall (2023) delineates two arenas for the process of learning in authoritarian states. The first is "internal learning", which describes how authoritarian rulers apply lessons learned from previous rulers of the same state. This thesis, however, focuses on the second of these processes, "external learning", where lessons from the successes and failures of autocrats from third countries are applied in a new setting – a process more widely focused on in the literature of authoritarian learning (Hall, 2023). A myriad of phenomena have been covered, including the transfer of policies, institutions, administrative arrangements, rhetorical frames, and practices, amongst others (Yom, 2014; Tolstrup, 2015; Ziegler, 2016; de la Torre, 2017; Darwich, 2017; Weyland, 2019).

As described by Lemon and Antonov (2020), this literature then subdivides into theories of diffusion, which describes "any process where prior adoption of a trait or practice in a population alters the probability of adoption for remaining non-adopters" (Strang, 1991) and policy transfer, described by Dolowitz and Marsh (2002) as:

"the process by which knowledge about politics, administrative arrangements, institutions, and ideas in one political system (past or present) is used in the development of policies, administrative arrangements, and ideas in another political system".

In practice, however, these terms have been used largely interchangeably, with the divisions between them often blurred (Ambrosio & Tolstrup, 2019). As such, whilst strictly covering policy transfer, this thesis uses "diffusion" to describe the *processes* of transfer, aiming to capture how wider structures promote the movement of authoritarian practices.

There exist, however, any multitude of theorised mechanisms that cause diffusion. Levitsky and Way (2006) describe, for instance, the "linkages and leverages" of authoritarian regimes with foreign governments as a means through which ideas spread between countries. Here "linkage" describes the "economic, social, communication, intergovernmental and transnational civil society relationships that tie countries to the West", but subsequent studies apply this theory to the connections between authoritarians. Hall (2023) draws convincing conclusions as to the linkage between the Belarusian and Russian security services, for instance, which credibly describes diffusion. Leverage, on the other hand, concerns the "hard" processes of foreign policy, whereby decisions are made based on the power countries have to influence other states' decisions, with the USSR's ability to force cooperation with the countries of the Eastern Bloc a strong example (Applebaum, 2012). Studies of Eurasia have looked at Russia's "teaching" of authoritarian electoral systems (Tolstrup, 2015) or at the effect of regional hegemons (Kneuer & Demmelhuber, 2016). Further afield, studies of South America have looked at how constitutional arrangements diffuse through perceptions of outside success (de la Torre, 2017). Finally, more recently, studies have looked at the role of regional institutions for the diffusion of policies, with Lemon and Antonov (2020) looking at the CIS and Hall (2023) describing the "learning rooms" of the CIS, SCO, and CSTO. Here the prevailing logic is that ROs provide a platform for learning and policy exchange between states (Obydenkova & Libman, 2018). After all, democratic organisations, such as the EU, have been frequently shown to provide a platform for the diffusion of democratic practice and institutions, whilst studies on their authoritarian mirror images were still thin on the ground. This thesis, therefore, takes up the call of these previous works to interrogate the role of ROs in diffusion. The SCO was chosen because, as the following section describes in detail, China and Russia have both been prominent proponents of "internet sovereignty" norms and feature within this organisation, alongside other authoritarian states understood as potential targets for diffusion (Litvinenko, 2021; Shcherbovich, 2021).

This case selection also makes sense when the goals of the organisation are considered. The founding convention, for instance, explicitly describes policy transfer as a key goal:

"In accordance with this convention the central competent authorities of the Parties shall cooperate and assist each other through: ... 7) exchange of regulatory legal acts and information concerning practical implementation" (Shanghai Convention on Combating Terrorism, Separatism and Extremism, 2002, Article 6).

What's more, it provides multiple platforms for potential diffusion, which correlate with the mechanisms described above. The first of these are the conventions of the organisation, the "memorandum of obligations"[5] which members must sign before joining and which could potentially serve as a repository for policies. Second are the joint exercises undertaken by members in the framework of the RATS, which provide the opportunity for linkages to develop between security services and authorised bodies for cyberspace. Likewise, thirdly, linkages could conceivably develop through the yearly meetings between these countries' representatives of for cyber-policy, constituting a "learning room" as envisaged by Hall (2023).

Using this theoretical groundwork, paired with this evidence from the institution, this thesis, therefore, hypothesises (H6): that the SCO provides a platform for the diffusion of authoritarian internet sovereignty practices.

As the literature describes, however, diffusion is, fundamentally, a "causal process" (Ambrosio and Tolstrup, 2019) placing the research burden on producing evidence beyond doubt that transfer is taking place. To prove this causal link, it must be shown that "prior to adoption, the adopter knew of the policy innovation, evaluated its merits and adopted it based on this evaluation" (Lemon and Antonov, 2020). As they argue, policy convergence can occur independently of processes causing coalescence in a concept understood as "spurious diffusion". What's more, the "traditional approach", as described by Ambrosio and Tolstrup (2019), which takes convergent outcomes, finds evidence for relations between policymakers, and concludes with mechanisms, can often fall short in proving diffusion. This is because the choice in case study is often predicated on known convergence, a selection bias which ignores cases where diffusion mechanisms are present, but diffusion fails to occur. Other studies evolve what Ambrosio and Tolstrup (2019) describe as either a "smoking gun" approach, which sees

[5] Listed in Appendix F.

a particular piece of overwhelming evidence as a proof, or a "jumping through hoops" approach, which, through solving multiple hypotheses, proves a causal link.

This thesis attempts to overcome the limitations of this field in a manner similar to Lemon and Antonov (2020), which is why methodology is based on their approach analysing "legal harmonisation". This approach compares legal texts and qualitatively identifies salient similarities, before analysing for innovators and later adopters. By focusing on publicly available legal text, this thesis' data is objective and the findings reproducible, strengthening the conclusions drawn.

The case selection also reduces limitations. The SCO was chosen to test the assumptions of other researchers and *not* because a case of convergence is clear and sought to be proven. Secondly, the range of regimes contained within the organisation provides room for divergent results, showing contexts where diffusion is less likely to occur. This allows for analysis of factors both *causing* and *preventing* diffusion, rather than focusing purely on confirming facilitating factors. Furthermore, looking at legal harmonisation through causal process tracing allows analysis to focus on "smoking gun tests" – the burden of proof for this work. These tests must show that policymakers in adopting states were aware of the innovations of others and had time to evaluate them, done by proving linkages and putting policymakers "in the same room" at events organised by the SCO. Simultaneously, this work looks for outside mechanisms that could explain policy convergence, to challenge the SCO's institutions as the causal explanation.

Ultimately, there will always be limitations to this approach. In an authoritarian environment, the non-transparency of regimes leads to situations where information proving or disproving diffusion is unavailable and without access to policymakers definitive conclusions cannot be drawn. As such, the conclusions of this thesis must be understood based on their relevance for future research. In the absence of other empirical studies in this area of digital policy, this contribution is important enough for expanding theories of diffusion in the SCO to justify this method, despite its limitations. Furthermore, as a qualitative work, the descriptive value of research in revealing the structures of the SCO and member states is very relevant for future researchers, even if causal links cannot be proven beyond doubt. Indeed, the volume of data collected, covering the provisions of eight countries over thirty years as well as the SCO itself, creates a useful database for future scholars in this area to generate findings.

2.2 Internet Sovereignty – Cyberspace, the Nation State and Authoritarian Responses

2.21 Cyberspace, A New Home?

"Internet sovereignty" as a concept has come under increasing scrutiny over the past two decades from ever expanding academic fields, but still creates theoretical difficulties. As has been problematised, there exist multiple variants of this term including digital, cyber, technology, information, and data sovereignty (Couture & Toupin, 2019). These terms, despite having been developed in different contexts, are often used interchangeably within the literature. This has created such significant problems in finding a suitable definition for this term and those related, that a separate discussion has evolved which scrutinises their uses in different contexts (Couture & Toupin, 2019; Mueller, 2010, 2017; Pohle, 2020; Pohle & Thiel, 2020; Litvinenko, 2021). Conceptually, it also is difficult to pin down, with studies using this same terminology to focus on a wide range of issues. Articles have discussed, among other things, the European Union's GDPR laws (Celeste, 2021; Moerel & Timmers, 2021; Roberts et al. 2021; Vardanyan et al. 2023), China's concept of "cyber-sovereignty" (Kolton, 2017; Parasol, 2018; McKune & Ahmed, 2018; Fung, 2022), Brazil's LDPR and wider data sovereignty goals (Polatin-Reuben & Wright, 2014), the rights of indigenous peoples (Kukutai & Taylor, 2016; Duarte, 2017), and Russia's draconian internet reforms of 2019 (Stadnik, 2021; Litvinenko, 2021). This is, however, not surprising – these situations all describe political entities' attempts to regulate the expansion of the internet in the modern world in their sovereign interests. This chapter, therefore, describes the separate norms surrounding internet sovereignty in the SCO member states, as well as coming to propose a definition. This provides the theoretical groundwork describing the norms which are to transfer in line with the primary hypothesis of this thesis (H6), that the SCO is a platform for authoritarian diffusion.

Importantly, "norms" are discussed within this thesis when referring to the concepts of internet sovereignty as endorsed by the separate states and are theoretically understood as "ideational phenomena" as described by Finnemore and Sikkink (1999). This theory states that norms define standards of behaviour for actors with a given identity. For the SCO member states studied, this identity is that of sovereign non-Western states, who have the right to define their own rules for internet governance. In this sense, "norms" are understood as informing the decision making of these states to define these rules, with legal provisions an *expression* of deeper normative understandings. As such, actions can be analysed with reference to their ideational underpinnings and vice versa. The later analysis, therefore, whilst tied to the provisions themselves, nevertheless can reflect on the norms which underpin and justify policymaking.

A further core issue to address with terminology, however, is in understanding the nature of "sovereignty" itself, which has had differing definitions across time and geographies (Bartelson, 2006). Taking these difficulties, this thesis deliberately sets a wide definition, as has been the trend in the research into its application to the digital, which can be applied across member states. Therefore, this thesis recognises sovereignty in a Westphalian sense, as the supreme authority of a political entity to rule over a given territory, which, in accordance with Hollis (2012) is not limited to landmass but also to resources. This is both "internal sovereignty" within the borders of the state, and the "external sovereignty" through recognition from other state entities (Pohle and Thiel, 2021). Importantly, this definition recognises sovereignty as belonging to the power vested in rulers, the state, and its constituent organs, as in the early conception of Bodin, rather than concerning citizenry as in theories from thinkers such as Rousseau (Bartelson, 2006). The benefit of this approach is that it does not contravene the separate doctrines of sovereignty amongst members[6], and is in accordance with the SCO charter (2002, Article 2).

The question remains, however, of how to apply this concept to the decentralised network of the internet, which defies traditional understandings of the nation state. By way of an answer, in the early 1990s a notion developed which described the interconnections of networks which made up the internet as "cyberspace". This geographical metaphor for digital information exchange contributed to a conceptualisation of the internet as informational "territory" (Deibert, 2008; Graham, 2013). Suddenly, concepts of sovereignty could be applied these virgin lands, which, due to network privatisation, belonged not to nations but private companies and, to a lesser extent, the users, or "netizens". The internet became a public space, a kind of Foucauldian heterotopia (Wark, 1993; Lee & Wei, 2020), where different places and times were unified in the flow of information between them. This ownership structure and focus on unrestricted information flows initially led some to conceive of this "territory" as autonomous, existing outside of states' control:

"Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us

[6] China: Five Principles of Peaceful Coexistence (1954); India: Constitution of India Preamble (2023); Kazakhstan: Constitution of the Republic of Kazakhstan, Article 2 (1995); Kyrgyzstan: Constitution of the Kyrgyz Republic, Article 1 (2020); Pakistan: Russia: Constitution of the Russian Federation, Article 4 (1993);Tajikistan: Constitution of the Republic of Tajikistan, Articles 1 & 6; Pakistan: Constitution of the Republic of Pakistan Preamble (1975); Uzbekistan: Constitution of the Republic of Uzbekistan, Chapter One (1992).

alone. You are not welcome among us. You have no sovereignty where we gather (Barlow, 1996, as quoted by Couture and Toupin, 2019).

As described by Couture and Toupin (2019), this set the internet's freedom in opposition to state sovereignty. In their article, the authors point out, however, that this autonomy could not exist in the face of states' capacity to control the infrastructure on which the internet relies and coerce private companies in this space to act in state interest (Wu, 1997). As such, the idea of an internet unfettered by state control soon faded, but the idea of it as controllable territory remained, with many states introducing laws to govern online activities by the beginning of the early 2000s.

In the early period of internet development, however, as described by April Mara Major (2000), the norms which governed digital policymaking converged with those of the United States, as the society with the fastest development and largest user base. This meant the early global internet became a space defined by the values of private property and free speech, mirroring rights enshrined in the US Constitution. This, coupled with the relative anonymity provided by encrypted internet protocols, meant cyberspace could potentially become a significant danger for autocracies, whose citizens could suddenly communicate freely both with each other and the outside world.

2.22 The Golden Shield and Great Firewall of China

Whilst Western scholars took the liberal governance norms of the early internet as an indication that it could become a driver for democratisation (Ferdinand, 2000; Shane, 2004; Best & Wade, 2009; Laidlaw, 2015), authoritarian states further east had long been looking at ways to assert control over the territories created in cyberspace. Most successful was China's "Great Firewall", a set of legal and technological frameworks using TCP inspection to filter cross-border traffic and effectively segregate Chinese networks from the internet (Clayton, Murdoch & Watson, 2006). This system, as part of the larger "Golden Shield" project, was designed to prevent internet users in China from accessing IP addresses deemed undesirable to the CCP. These included foreign websites, as well as domestic sites belonging to forces deemed oppositional, such as the China Democracy Party or the Falun Gong religious movement (Goldsmith & Wu, 2006; Zittrain & Edelman, 2003). This project developed along with the initial expansion of the network in the 1990s and was supported by the nationalised structure of the country's network infrastructure with the main ISP, China Telecom, state-owned and

other companies limited to renting bandwidth from them (Herold, 2012). The internet in China was segregated *by design,* therefore, meaning a practical form of sovereignty had been achieved, whilst the initial internet sovereignty debates in other states were only beginning to take place. Therefore, the Chinese concept of "cyber-sovereignty" logically must have developed as a means to describe and justify existing capabilities, rather than as a challenge to narratives further afield.

In this regard, scholars argue that this system came as a result of China's long-standing conception of sovereignty, based on the Five Principles of Peaceful Coexistence, first signed with India in 1954 (Creemers, 2020). This, coupled with the experience of the Soviet Union's stagnation, led to the development under Deng Xiaoping of a "Socialist Market Economy" allowing market reforms to the economy whilst maintaining effective state control (Sigley, 2007). Chinese sovereignty theories in the 1990s, therefore, into which the internet was born, were based on the concept of non-interference and the primacy of the state on Chinese territory and in the market. As such, the internet's development followed the same path, not to be interfered with by foreign states, but allowed to expand in line with the aims of market growth.

The full cyber-sovereignty concept borne out of these ideas first appeared in the White Paper "On the Internet in China" (2010, Chapter V), which states:

"Within Chinese territory the Internet is under the jurisdiction of Chinese sovereignty. The Internet sovereignty of China should be respected and protected. Citizens of the People's Republic of China and foreign citizens, legal persons and other organizations within Chinese territory have the right and freedom to use the Internet; at the same time, they must obey the laws and regulations of China and conscientiously protect Internet security".

This conceptually solidified that which had been achieved technically, an internet controlled by the government, through policymaking and the nationalised network infrastructure.

Importantly, it was only later, after President Xi's rise to power, that this concept began to take on an international element (Zeng et al. 2017). As described by Moore (2022), this happened most visibly at the first WIC in Wuzhen in 2014 and was orchestrated by China's Cyberspace Administration. The term described a model which was anonymously distributed to participants' hotel rooms in the early hours of the conference's final day in the form of the Wuzhen Declaration (2014; Areddy, 2014). This document saw internet sovereignty as the right of states to develop their own governance regimes for the internet and "work for a cyberspace

shared and governed by all" (ibid.). Moore (2022) argues that this really was promoting an internet with Chinese characteristics, with the "border controls and immigration standards they see fit" (Griffiths, 2019). Following this narrative to its logical conclusion, Griffiths argues spreading these norms throughout the world would create a fragmented internet, "turning the entire world into China, where people use a mirror image of the internet, resembling that outside the Great Firewall, but skewed and misshapen." For other countries to develop their own internet sovereignty, authors have shown how China exports technologies build up friendly states' digital capacities with a negative effect on human rights (Moore, 2022; Yau, 2022).

Taking the logics of authoritarian stability, the internal benefits of the Chinese internet governance model are relatively straightforward. The control of online content prevents oppositional forces from challenging the CCP's legitimacy claims, with digital surveillance allowing for rapid repression. State ownership of the infrastructure and largest companies in the digital space, meanwhile, allows for rent seeking and distribution to co-opt key elites to the CCP's regime.

The question remains, however, as to the motivation of the CCP to promote such a narrative internationally, especially since it already was so successful in controlling its domestic internet. For McKune (2015) and Flonk (2021), this successful control was a key cause for the export of these norms. They argue that international adoption of similar measures legitimises existing practices for domestic audiences – making people even less likely to question their draconian nature. Zeng et al. (2017) take this further, arguing that these norms when seen as legitimate domestically, could allow for the government to socially manage the Chinese population, perhaps even allowing for "complete control" (McKune and Shazeda, 2018). Whilst others don't go this far, there is a clear understanding of legitimation as an important goal of the Chinese government. Budnitsky and Jia (2018) propose a further legitimatising aspect of this promotion in their description of "internet sovereignty" as a brand. They argue that the acceptance of these norms abroad contributes to the projection of China as a "Great Power". This conceivably both improves domestic citizens' perception of the capabilities of their state to wield power abroad, driving legitimation, and strengthens the image of China internationally, increasing customer interest in the country's digital solutions. The "brand" described by Budnitsky and Jia (2018), therefore, strengthens domestic legitimacy, as well as increasing the rents collected by the regime through international trade – both strengthening the CCP's position. This, in turn, also reflects the ideals of the "Socialist Market

Economy" described above – international promotion of cyber-sovereignty norms positively contributes both to the control of the CCP and the growth of the Chinese economy.

In sum, the Chinese concept of "cyber sovereignty" claims the state alone has the right to govern the internet on its territory. It was inspired by the concept of sovereignty laid out in the "Five Principles of Peaceful Coexistence" and justified the existing design of the state-controlled internet in China. This benefited the CCP through allowing repression of dissenting voices, as well as co-optation through distributing rents collected through state-ownership of internet companies. The international promotion of this brand of Chinese "cyber-sovereignty" serves to further strengthen the CCP by increasing rents collected through the international trade of technologies used for internet controls and domestic legitimacy through claims to "Great Power".

2.23 The "Information Spheres" of Central Asia

Discussions of sovereignty in cyberspace developed in Central Asia along with the expansion of the network. Rather than following the technical "Chinese approach", these states developed legal regimes to control cyberspace, but also placed the state in the centre (Ibragimova, 2013). The first legal frameworks applied laws "On the Mass Media" to the online space[7], which each to varying degrees controlled the registration of media outlets online and limited the dissemination of certain information, including state secrets, sedition, calls inciting religious or ethnic violence, pornography, and defamation. These laws were harmonised due to the shared inherited legal culture from the Soviet Union, having been adapted from Law No. 1552-1 "On the Press and Other Mass Media" adopted by the Supreme Soviet of the USSR on 12 June 1990. At the same, these countries developed relatively open regimes for network development, due to the lack of domestic expertise in this area and requirement for FDI to modernise Soviet legacy networks (McGlinchey & Johnson, 2007; Ibragimova, 2013). Indeed, the CIS introduced an agreement for these states to cooperate in network expansion, with connections established beginning in the same year (Commonwealth of Independent States, 1996), with input from the United Nations and the European Union. As such, the internet in these states developed in a largely unfiltered connection with the worldwide web, rather than in the relative isolation of the Chinese system (McGlinchey & Johnson, 2007).

[7] Russia (as the USSR) 1990, Tajikistan 1990, Kyrgyzstan 1992, Uzbekistan 1997, Kazakhstan 1999.

At the same time, state ownership of internet infrastructure gave governments greater control over content than in Western democracies with privatised networks. Indeed, state-owned telecommunication companies[8] and the Soviet-built infrastructure gave them the necessary levers to control the online space. As such, online censorship was a significant problem across the region from the internet's development, with each country applying practices based on their states' differing digital capacities (Ibragimova, 2013). The theoretical justification for these measures was the concept of "information security", which saw Central Asian states defining segregated "information spheres", where state authorised bodies used legal tools to control information flows in the interests of national security. Significantly, from their promulgation, these laws were justified with the concept of sovereignty, with Tajikistan the first to crystallise a concept of "information sovereignty" through its law "On Information" (2002, Article 43). Unsurprisingly, these national security interests mostly served regime stabilising purposes. In Kazakhstan, web filtering through Kazakhtelekom blocked access to government criticism (Ibragimova, 2013); Kyrgyzstan under Bakiyev saw similar techniques on oppositional media (Melvin & Umaraliev, 2011); Uzbekistan has used website filtering since at least the Andijan massacre of 2005 to quell protest (Stroehlein, 2008) and Tajikstan has blocked Facebook and other social media for their role in disseminating criticism (Shafiev & Miles, 2015). As such, whilst not as capable as China to segregate a national internet segment, the countries of Central Asia have been effective in prosecuting a regime-stability focused system of internet governance, based on a defined concept of "information security" which, significantly for this thesis, was justified through the sovereignty concept.

Indeed, one of the earliest uses of the term was Nursultan Nazarbayev's opening speech at the 2011 SCO summit, in which he stated:

"The time has come to introduce new concepts of "electronic boundaries" and "electronic sovereignty" into international law. We have to support the important work of our Russian and Chinese colleagues and work out an integrated consolidated position of the SCO in this direction. At the same time, we have to be open for all positive sides of the Internet that bring constructive ideas and new technologies. We may consider creating a special SCO authority working as cyber-police against Internet aggression," (Tashkinbayev, 2011)

[8] Kazakhstan - Kazakhtelekom, Kyrgyzstan - Kyrgyztelekom, Uzbekistan - Uztelekom, and Tajikistan – Tajiktelekom.

This call indicates, firstly, that the Russians and Chinese were seen as the innovators of the internet sovereignty model. This also indicates the readiness, on the Kazakh behalf at least, for deeper alignment within the SCO and, as such, this organisation's potential to diffuse such a model. Finally, the logic of creating a unified Central Asian concept is revealed. "Cyber policemen" should be created to control the new territory of cyberspace, extending the repressive capacity of the state, with support, presumably technical, coming from the fellow member states of the SCO. This, in theory, would consolidate the autocrats of Central Asia, isolating them from the perceived elevated mobilising effect of the global internet and buttressing them against democratisation and possible regime change.

2.24 RuNet: An Internet with Russian Characteristics

As Borogan and Soldatov (2017) indicate, however, the Central Asian internet governance concept likely first developed in the region's neighbour to the north, the Russian Federation. In Putin's first months in office, security concerns about the internet led to a Russian "Doctrine of Information Security" (2000). This crystallised the concept of a "information sphere", which was understood as:

"an assemblage of information, information infrastructure, entities engaged in the collection, formation, dissemination and use of information, and a system governing public relations arising out of these conditions. The information sphere as a system-forming factor of societal life actively influences the state of the political, economic, defence, and other components of Russian Federation security. The national security of the Russian Federation substantially depends on the level of information security, and with technical progress this dependence is bound to increase."

Crucially, the Russian constitution was to apply to this newly established space, for "national interest … the rights and freedoms of man and the citizen to receive and use information, the assurance of a spiritual renewal of Russia, and the preservation and reinforcement of the moral values of society, traditions of patriotism and humanism and the cultural and scientific potential of the country" (Doctrine of Information Security, 2000, pg. 2). This established a precedent for the state to claim control over both the infrastructure of the internet and the information (content) contained within, by evoking the supremacy of the constitution and sovereignty. Crucially, this doctrine also establishes the perceived threat to

Russia's information interests, with foreign states' interference seen as endangering normative "Russian" moral, spiritual and patriotic values, and the Russian language. This is significant, as it set a normative basis for how information spheres should take on national characteristics; the RuNet envisaged was not only internet activity on Russian territory but applied to all internet activity in the Russian language – ostensibly for its conservation. As such, this doctrine established a normative basis for how the internet in Russian *should be,* in line with moral and spiritual values, *as defined by the Russian state.* This had a regime stability benefit, as non-conforming content deemed "un-Russian", was delegitimised. Secondly, the theoretical application of constitutional powers to content in the Russian language expanded attempted control into the diaspora and Russian-speaking populations abroad, theoretically allowing for transnational influence.

This concept of "information spheres" has been understood as a culmination of former KGB and FAPSI general Vladislav Sherstyuk's crusade along with the Security Services to develop their control over network infrastructure through technological methods such as SORM and SORM 2[9]. Importantly, this concept, its exact wording ("information spheres", "information security") and SORM practices were emulated in the securitisation of narratives around the internet throughout Central Asia (Soldatov & Borogan, 2015; Ibragimova, 2013). This provides further evidence for the legal harmonisation between Russia and Central Asia, creating a strong case for the value of the analysis of this thesis – to be explored in the empirical section.

The concept of "internet sovereignty" in Russia further evolved by blending this earlier notion of "information security" with broader discussions on sovereignty during Putin's second term. Codified in the ideas of Surkov (2006) concerning "sovereign democracy", *Russian sovereignty* was discursively defined in opposition to Western understandings of a self-governing democracy and was based on Russian "cultural criteria" (Putin, 2007). Discourse analysis (Morosov, 2008) describes this as the process of maximising the autonomy of the Russian state "to control all significant domestic and transnational processes". Morosov argues this is in opposition to Western liberalism, which is portrayed by the Kremlin as promoting democracy without regard for states' rights, with sovereignty "a rudiment of the past that impedes the spread of democracy" (ibid.). Whilst the theory of "sovereign democracy" fell away in the subsequent years, discussions of sovereignty expanded, with the term

[9] From the Russian "Sistema tekhnicheskykh sredstv dlya obespecheniya funktsii operativno-rozysknykh meropriyatii" (System for technical means for the functioning of operative search activities), in practice systems for monitoring network communications.

accompanying a securitisation of many areas, including the economy (Conolly & Hanson, 2016), morality (Sharafutdinova, 2014) and the internet (Budnitsky, 2018; Epifanova, 2020, Flonk, 2021).

The debate around internet sovereignty developed alongside Dmitri Medvedev's tighter focus on digital technology. Founded in 2008, Roskomnadzor began to surveil and censor information, which accompanied an attempted "Russification" of the internet (Nocetti, 2011). A state search-engine was to be produced, a Cyrillic upper-level domain (.рф) was procured from ICANN in 2009, and a Russian-only operating system was slated for 2014. Whilst doomed to fail, these projects displayed the intent to create an internet with Russian characteristics.

As in the Chinese case, the literature describes both external and internal authoritarian logic for creating this sovereign internet. Both Russian (Kolozaridi & Muravyov, 2021; Kovrigin, 2022) and international (Litvinenko, 2021; Nocetti, 2015) scholars describe the external threat posed to the Russian "information space" from foreign cyberattacks. The United States was the focus of this narrative following the Snowden revelations, with the idea that it and allied powers use cyberattacks to destabilise the Russian regime. This idea is often purported by the state itself and was immortalised by Putin's assertion that the internet is a "CIA project" (Rayman, 2014). This generates legitimacy for the regime as both a perceived guardian of citizens in cyberspace and through limiting the power of foreign narratives through their delegitimisation as "potential threats".

The internal benefit of a "national internet" is in its limitation of the reach of oppositional voices both through overt censorship and surveillance, which often culminates in the arrest or harassment of critics[10]. As in the Chinese case, a further aspect is the financial benefit which can be gained though the control of data. Zuboff's (2019) theories of "surveillance capitalism", when applied to state-owned and aligned tech companies, can describe how the Russian state's internet sovereignty laws help generate income from citizens' data (Ostbo, 2021). As such, Russia's large and successful tech firms, such as VK, Yandex, and Sber, provide the government with streams of both revenue and data – allowing for greater surveillance and increased rents.

Taking these aspects together, the Russian internet sovereignty concept can be deconstructed: tightening state control of the internet helps censor and surveil oppositional forces, limit foreign cyber threats, and increase rents collected through state-aligned

[10] OVD Info lists 61 cases from 2022: https://data.ovd.info/repressii-v-rossii-v-2022-godu#4

companies. As such, control over the digital sphere, in the form of "internet sovereignty" becomes a tool of the autocrat, in this case Vladimir Putin, to consolidate his regime.

2.25 Post-Colonialism and the Internet in India and Pakistan

In the final geographical area of this study, South Asia, a similar network model initially developed to the northern peers in Central Asia. Both India and Pakistan expanded their networks through state-owned corporations[11] which relied on state subsidies and FDI. This was coupled with the application of established legal statutes to the evolving media, with Pakistan, as an Islamic Republic, criminalising internet users for blasphemy under Section 295(c) of its 1898 Criminal Code. Both India and Pakistan also controlled seditious or defamatory content under the Penal Code (1870) inherited from British colonial rule over the Indian subcontinent. Both jurisdictions saw significant use of these laws to control internet users, particularly following the explosion of social media use towards the turn of the decade (Cali, 2012; Freedom House, 2012). What's more, evidence suggests Pakistan used these control structures to implement internet shutdowns in the Balochistan region in 2005 (El-Khawas, 2009), and as a result has been understood as an early adopter of such authoritarian internet practice (Wagner, 2018). As such, despite liberalisation seeing state-owned telecoms companies move into private hands, it is difficult to argue that either state followed the typical "liberal model" of internet development, despite both benefitting from the commercialisation of the internet through providing IT and E-Commerce services.

The commercial aspect of the internet feeds into India's internet sovereignty[12] narrative which focuses on data as a resource. As with the Chinese and Russian narratives, this concept developed in opposition to the claimed American hegemony in the digital sphere (Gupta & Sony, 2021). As described by Prasad (2021) this narrative opposes the perceived imperialism of American tech companies. He describes data as both belonging to the individual, as well as being an extractable resource, through his metaphor of "people as data, data as oil". Within this argument, India's E-Commerce Act and Data Localisation Law are methods for transferring data from exploitative foreign companies to be "equitably accessed by all Indians" (Draft National e-Commerce Policy: India's Data for India's Development, 2019). In keeping with the post-colonial narratives of the world's largest democracy, data should be "of the people, by

[11] VSNL in India and PTCL in Pakistan.
[12] More commonly discussed as "data sovereignty".

the people, for the people" (Kovacs & Ranganathan, 2019). Critical perspectives, however, have questioned the ultimate benefactor of this redistribution of wealth created from the largest national data supply on the planet (Kovacs & Ranganathan, 2019). Some argue that programmes such as the Aadhar digital ID have given data extraction rights over India's citizens to the government, making those not engaging with the system "un-people" (Vidyut, 2018). As such, they argue, it is the state itself that benefits from India's concept of "digital sovereignty", in that the financial benefits gained from access to citizens' data is gatekept by the government and can be distributed in the tender process. In this sense, the Indian concept bears resemblance to other member states' – legal internet sovereignty provisions support the state's ability to distribute rents to key allies in the tech space. Indeed, there is evidence of tech companies, such as Twitter, agreeing to restrict accounts critical of the regime in return for maintained market access (Singh, 2021). From a political perspective, therefore, the digital sovereignty practices of India somewhat reflect the co-optation strategies employed by the autocratic states discussed above, whereby allies loyalties are "bought" through allowing them to profit on citizens' data.

Critically, however, discussions of "data sovereignty" in India are a new phenomenon, with academic discussion having only begun since 2019 – the time of SCO ascension. There exists a chance, therefore, that official use of this term, first seen in a government document in 2019, comes as a result of the influence of the organisation's narratives, a concept discussed further in the findings of this work.

This is mirrored in Pakistan, which does not have a developed domestic debate on "internet sovereignty", with academics describing the phenomenon as foreign, or developed in China (Shahid, 2023; Nizamani & Firdous, 2020). As such, both countries become a key focus for the analysis of diffusion, being states where internet sovereignty narratives are externally influenced. At the same time, the focus on the state as decision maker for internet policy, and the application of laws to limit information flow existed in these countries before conceptual discussions, showing that a normative basis is not always necessary for restrictive policies. Conversely, therefore, as argued by Kumar and Thussu (2023), there can be no specific "internet sovereignty" policies as such. Instead, as discussed in the case of China, the term internet sovereignty is a normative justification for policies which place the state at the centre of internet governance regimes, rather than citizens or business.

To conclude, this chapter described the issues in coming to define a term which, whilst endorsed by the SCO, has significant ideational variations based on the member state applying it. The ideational underpinning of applying "sovereignty" theory to the internet was discussed,

with the network described as digital territory, a "cyberspace" where state borders can be drawn. The norms of this cyberspace, the "ideational phenomena" which influenced its early development were shown to initially mirror liberal ideas of free information flow and private property, which could potentially threaten authoritarian regime stability. As such, the states of the SCO developed internet control concepts and practices to limit this threat.

In China, this took the form of the Golden Shield and the "cyber security" concept which was influenced by the "Socialist Market Economy" goals of the state and began to be externally promoted in 2014. Russia's concept of "information security" influenced digital controls across Central Asia and later crystallised into the idea of "internet sovereignty", before later merging with the Chinese concept, as will be discussed in the next section. The key idea overall was the centrality of the state in controlling a territorialised segment of the internet, with normative national characteristics. This was applied to multiple facets of the network, including infrastructure and data. The logic behind this control is regime survival, with technical and legal controls strengthening the state's capacity to legitimate, co-opt, and repress in the digital sphere. In this paradigm, the international promotion of these norms serves to further legitimise domestic practices, bolster neighbouring autocracies against democratisation, and oppose a perceived American hegemony in the digital sphere. The so-called "Balkanisation" of the internet within this logic, therefore, becomes a side-effect of rulers' attempts to expand their domestic control in cyberspace, rather than being an end goal in and of itself.

3 Empirical Research and Methodology

3.1 Cyber Norm Development in the SCO and the Mechanisms of their Diffusion

The Shanghai Cooperation Organisation was founded through the promulgation of China, Kazakhstan, Kyrgyzstan, Russia, Tajikistan, and Uzbekistan of the "Shanghai Convention on Combating Terrorism, Separatism, and Extremism" (2001). As the successor to the Shanghai Five, the RO had the aim of inducing cooperation to eradicate the "three evils of terrorism, separatism and extremism" which faced member states in the post-Soviet Asian geopolitical landscape (Aris, 2009). Whilst not a formal alliance, according to this convention, cooperation was to include information sharing, joint operational search activities, the exchange of experience and training, and the establishment of a regional counter-terrorist structure, later realised through the Regional Anti-Terrorist Structure (RATS).

This chapter examines the development of cyber norms within this organisation, details their key principles with relation to the concepts of internet sovereignty from the previous chapter, and indicates the relevant deductive categories for the qualitative analysis of legal harmonisation. Four possible organisational mechanisms of diffusion are also defined based on primary sources. Analysis chronologically traces the developments within the organisation, for which an accompanying timeline can be found in Appendix A.

From the first moment, the SCO was explicitly envisaged as a forum to promote legal harmonisation. The establishing convention describes the "exchange of regulatory legal acts and information concerning practical implementation" (ibid. Art. 6, Par. 7) as key to members' cooperation. This provides a framework through which internet governance norms could diffuse by creating a platform for interstate dialogue and is the first mechanism to be tested for in later analysis, the "direct exchange hypothesis" (H2). Analysis, therefore, also takes the signing of the Shanghai Convention as the starting point for the possible impact of the SCO on the diffusion of internet sovereignty policies.

The first explicit discussion of cooperation on cybersecurity took place later, however, following the expansion of multilateral coordination and confidence through the joint military exercises "Coalition 2003" and "Peace Mission: 2005", as well as successive summits in Moscow, Tashkent, Astana, and Shanghai. This was codified in the "Action Plan on Ensuring International Information Security" (Ministry of Foreign Affairs of the People's Republic of China, 2007) formulated at the Bishkek summit, a key shift of focus to the digital sphere as an area affecting members' security. Whilst rapid internet expansion was the global driver of this refocusing, the lessons learned from the Colour Revolutions in Georgia, Kyrgyzstan, and Ukraine about the internet's mobilising potential were likely a key secondary trigger. Indeed, Titus Chen (2010) recognises this as leading to the strengthening of the Chinese regime's "coercive capacity" and McKune and Ahmed (2018) identify Russia's fingerprints on the plan through the securitised "Information Security" concept, as described in the previous section.

The action plan was followed by the publication of the "Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organisation" (2009) at the Ekaterinburg summit, which establishes the perceived threats to be countered through information security policy, and the norms which were to inform their contravention. Identified are: "information weapons (warfare) […] cybercrime, the use of a dominant position in the information space to the detriment of the interests and security of other States, […] threats to […] infrastructure, and the dissemination of information prejudicial to the socio-political and socio-economic systems, spiritual, moral and cultural

environment of other States" as the major threats to members' information security (Shanghai Cooperation Organisation, 2009). Whilst at first glance these aspects don't seem dissimilar to United Nations' resolution: "Developments in the field of information and telecommunications in the context of international security" (A/RES/53/70, 1999), they establish several important norms, which have come to shape the organisation's approach.

Firstly, by tacitly denouncing the American dominant position in the online space, they advocate in this agreement for a breakdown of the country's hegemony in online governance and in favour of decentralisation. This, coupled with this document's framing of the sovereign state as the key player in governance, reimages a multilateral system of internet governance, breaking from the Western ideal of "multistakeholderism". This reflects the Russian concept of "information security", which identified foreign nations as a key threat, and blends it with the Chinese sovereignty idea endorsing non-interference. These states had, therefore, taken the leading role in the SCO and had begun the process of norm promotion.

Secondly, this document justifies the requirement for content controls in national segments of cyber space, to crackdown on the threatening influence of "prejudicial information" to the interests of the state, both in terms of material well-being, and the undefined metaphysical "cultural and spiritual" aspects specific to each state (ibid. annex 2, para. 5). Finally, this document securitises the internet's physical infrastructure, which is "threatened" and, logically therefore, to be protected and controlled by the state in the interests of national security. Overall, this introduces key aspects of the SCO's narrative for information security, the basis for internet sovereignty, in applying the Chinese concept of multilateralism and justifying content and infrastructure controls in state interest and for abstract normative trappings, including states' spiritual and moral characteristics. As such, these aspects are the basis for the cyber norms agreed to by the member states which define the organisation's approach and proceed from the national concepts described in the previous chapter.

As the first such agreement of its kind within this institution, this moment also established a further mechanism for the potential diffusion of norms within this organisation, through the legal alignment of a member states laws with the organisation's frameworks, which this thesis describes as the "state-organisation alignment hypothesis" (H3). This establishes a reciprocity between the members and the organisation – not only has the SCO been shaped by the concepts of the member states, but the member states legal regimes can also be informed by the organisation's conventions.

The topic of cybersecurity was a central focus of the organisation's June 2011 summit in Astana, which coincided with the entry into force of the 2009 agreement. In his opening

statement to assembled leaders, Nazarbayev called for a "an alliance-wide cyber police force" and promoted the concepts of "e-sovereignty" and "electronic borders" as potential tenets of international law (Kerr, 2016). It is unsurprising, therefore, that in September later the same year the normative aspects of the organisation's approach to regulating the internet in the interests of "information security" were developed in the countries' proposal to the UN (A/66/359, 2011) for a new draft on the "International Code of Conduct for Information Security". In this document, the member states advocate that "the state should lead all elements of society, including its information and communication private sectors, to understand their roles and responsibilities with regard to information security", echoing an earlier submission of the Russian Federation in 1999. Importantly, as Eichensehr (2015) argues, this proposal goes further than before, in that it denies the "applicability of existing international law to cyberspace, advocated increased government control over the internet, and legitimized limitations on freedom of expression" by arguing for multilateral state primacy in domestic digital policy making. A logical continuation of the arguments of the 2009 document, the submission of this document to the United Nations is significant as it represents a collective act of norm promotion at the international level. Using Finnemore and Sikkink's (1998) definition of the "stages of norms", it appears, therefore, that the cyber norms within this organisation had become internalised, with the sought institutionalisation within the UN the next logical step of a "norm cascade". The proposal, however, was met with opposition and, due to a coalition of Western states voting against, was redrafted in 2015. In this later version, the Chinese delegation claimed to have "taken into account the reasonable suggestions of the international community" (Eichensehr, 2015) and devised more liberal suggestions.

Whilst this new draft code took on the language of "transparency and democracy", however, McKune's (2015) analysis reveals how it attempted to redefine how international human rights law was to be applied, leaving countries to control their own "information space". She argues the "new consensus" was capitalising on the Snowden leaks, in challenging the legitimacy of American primacy in internet governance. Most importantly, these documents indicated how cyber norm promotion had become an explicit aim, with their implementation continuously sought at an international level through to 2015. This creates a third potential mechanism for the diffusion of norms, the "international legitimation hypothesis" (H4), through which a potential wider international consensus on promoted norms could push reticent members into harmonising their policy with the SCO.

Beyond this, 2015 became key for the implementation of internet sovereignty norms on the institutional level of the SCO: joint cyber security simulation exercises took place in

Xiamen within the RATS framework, anti-extremism draft laws were drawn up with articles on internet controls, and Russia and China signed a cooperation agreement on cybersecurity. Equally important, this year saw the beginning of India and Pakistan's ascension, with both parties agreeing to the "memorandum of obligations" a year later, taken in analysis as the start point of these countries' potential capacity to receive the SCO's cyber norms through diffusion via organisation-internal mechanisms. Of these developments, two key moments stand out. Firstly, the text of the Chinese-Russian joint agreement (2015) reiterates the respect of one-another's sovereignty as regards the information space and, in Article 3 Paragraph 3, calls for "co-operation in the development and promotion of norms of international law to ensure national and international information security". Both countries had an agenda for influencing international internet governance and were expressing intent to lead together in this area. Secondly, at the "Joint Exercise on the Use of the Internet for Terrorism, Separatism, and Extremism" in Xiamen, authoritarian practices were taught within the organisation, with visiting specialists learning how to identify "information inciting terrorism" and reveal users' identities and locations allowing for swift arrest (Wood, 2015). This laid the groundwork for a further possible mechanism for norm diffusion, with drills promoting a certain "authoritarian best practice", which would require similar domestic legal frameworks to be developed for local emulation. This framework would presumably be based on a Chinese model, with them hosting the exercises in Xiamen, and is described as the "diffusion through practice hypothesis" (H4). These drills were repeated in 2017 and 2019, each constituting moments when policy harmonisation could have been enhanced through this diffusion mechanism. Crucially, these later drills included Chinese digital forensics company Meiya Pico's technology, translated for training in each of the member states which, as described by McKune & Ahmed (2018), "amounts to diffusion by practice of priorities, capabilities, and techniques, SCO member states are normalizing their cooperation regarding targeted online content and discovery of those responsible for that content". This also strengthens the assertion that China financially benefits through norm promotion, with this Chinese company profiting from the spread of their technology into other SCO member states.

The next significant moment in the SCO's development and promotion of cyber norms was the ratification of the "Convention of the Shanghai Cooperation Organisation on Combating Extremism" (2017). Article 7 calls explicitly for the introduction of content restrictions, along with the proactive "development of counter narratives to suppress the spread of extremist ideology". This "enhanced outreach" approach can be viewed as a legitimation of online propagandising against ideas understood by the states as dangerous. This strengthens

the established norm of state internet content control, both in removing certain voices and now in disseminating their own. Article 9 of this convention also calls for internet monitoring, to identify and criminalise "non-compliant persons" and restrict their access to the internet. This constitutes a further key cyber norm for the SCO, namely that restricting individuals' or organisations' access to the internet is valid in the interests of state security.

More recently, SCO members have sought to further institutionalise explicit "internet sovereignty" norms. The Samarkand Declaration (2022), within Articles 23-27, reiterates the concepts of state primacy in internet governance and sovereignty within cyberspace. Article 56 also provides evidence for the existence of the direct exchange mechanism (H2) within the SCO stating: "member states have supported the establishment of legislative linkages and the sharing of experiences in governance and development". As before, this indicates legal harmonisation is a conscious goal of the organisation.

Harmonisation was provided a further platform in 2023 with the first meeting of the Heads of Ministries and Agencies of SCO members responsible for the development of information and communication technology (Shanghai Cooperation Organisation, 2023a). This most recent summit in New Delhi saw the further development of a unified list of "terrorist, separatist and extremist organisations whose activities are prohibited on the territories of the SCO Member states" (Shanghai Cooperation Organisation, 2023b). It is too early to divine the significance of this register, but it does reflect the legal institutions of the member states, with Russia and the Central Asian states having implemented such registers for domestic internet governance. Finally, this same declaration reaffirms members' intention to use the UN as a platform to promote the organisation's concept of the "sovereign right of states to manage it [the internet] in their national segment" (ibid). As such, on a global level, these states will continue to push for acceptance of the norms described in this chapter.

To conclude, this chapter has hypothesised four possible diffusion mechanisms for legal practices related to the "linkages" between members within the SCO framework. The first mechanism (H2), "direct exchange", was established with the organisation's founding and describes policy transfer as an active exchange, with SCO summits and meetings between ministers responsible for information technology the most probable platforms. The second mechanism is that of "state-organisational alignment" (H3), whereby member states adopt legal norms taken from conventions signed within the organisational framework. H4 describes a diffusion mechanism through the "international legitimation" of cyber norms, where international institutions legitimise proposed norms through their acceptance into international codes of conduct and result in a norm cascade. The final mechanism, "diffusion through

practice" (H5), describes how member states adopt laws learned through cooperation in cyber security simulation drills, with law enforcement "best practice" predicating the establishment of similar legal frameworks to allow for their use. Whilst there are certain to be further diffusion mechanisms not borne out through this primary source analysis, these four mechanisms, as the most explicitly apparent, form the basis of analysis to identify the role the SCO as an RO plays in the legal harmonisation of members' internet sovereignty laws.

This chapter also established the origins of the normative basis of the SCO's internet sovereignty concept, shown to represent a combination of the Chinese and Russian ideas discussed in the previous chapter. The first of these norms was the shift from "multistakeholderism" to "multilateralism" with the state to become the central agent in controlling a "national segment" of the internet, with borders drawn based on the concept of sovereignty. Crucially, this underpins the following norms, in legitimising the state's right to act within the information space, and in reducing the agency of non-state stakeholders. The second established norm is that of content control, whereby the state and its agencies exercise control over the information available to users within these national segments. This takes the form of punitive and preventative censorship controls, or proactive dissemination of information favourable to the regime (propaganda). The next norm is infrastructure control, whereby the state controls the digital or physical infrastructure of the internet and, in so doing, reduces the ability of non-state domestic or foreign actors from disrupting critical systems. This provides a means for enforcing the final norm described by this chapter, "access control", whereby state actors prevent types of users from accessing or disseminating information through their segment of the information space, through direct bans, licencing laws, internet shutdowns or, indeed, cyberattacks against sites deemed a danger to national security.

As a final word, the use of primary sources in this chapter creates a risk of misrepresentation through omission, both of activities not publicly revealed and of external factors which could limit the effectiveness of diffusion mechanisms. Not least the fact that the SCO does not constitute a formal alliance such as NATO or have a binding legal charter such as belonging to the European Union. What's more, conflict continues between members, with border issues between India and China, India and Pakistan, and Kyrgyzstan, Uzbekistan, and Tajikistan. Indeed, the digital space has remained a point of contention, with China, Russia, and India, all actively engaged in cyber espionage against fellow members – despite SCO agreements claiming respect of each other's sovereign internet segments (Mirza et al. 2021). As such, whilst not described in detail here, these external limiting factors are considered at length in the discussion section's analysis of the SCO's role in diffusing these legal norms.

3.2 Research Methods

This dissertation adapts the causal process tracing methodology of Lemon and Antonov (2020) to assess the role of the SCO as an RO in the legal harmonisation of internet sovereignty laws. In this method, timelines of policy adaptation are created across states of interest and compared with external factors to ascertain diffusion mechanisms. This study's timelines were built on the deductive reasoning from the previous section according to the "theoretical sampling" method, whereby data collection is iterative, oriented towards the research question, and dependent on emerging theoretical considerations (Glaser & Strauss, 1967).

As such, the number of laws analysed for each member state varied, with Russia (32) the highest and Tajikistan (6) with the lowest. Important is that the number of laws collected for each state does not reflect the focus taken, with the same expansive process for data collection used for each, as displayed in Figure 1, to ensure each country was treated with the same attention. First, internet governance laws common across jurisdictions were collected via keyword search, relating to *data protection*, *telecommunications*, *cybersecurity*, *mass media*, and *information technology*. Then secondary sources were used to identify missing laws, including academic papers, reports from Freedom House's "Freedom on the Net" project (2023), NGO data, and documents submitted to the ITU. Finally, keywords from the laws already collected were used inductively, for cases where the same wording was employed in different national contexts. The variation in the sample sizes comes, therefore, as the result of national differences, including: the quantity of internet laws a country has, the degree of formalisation of internet sovereignty practice, the legal transparency of a country's regime, and its legal culture. This latter point partly describes, for instance, the difference between Russia (32) and China (11) in terms of sample size. Both have long-established and recently introduced laws for internet governance. Russia, however, sees many more amendments, whereas the Chinese legal regime, once established, tended in the data to remain unamended. Whilst not a central focus of this study, these differences could provide an interesting basis for future scholarship on comparative law.

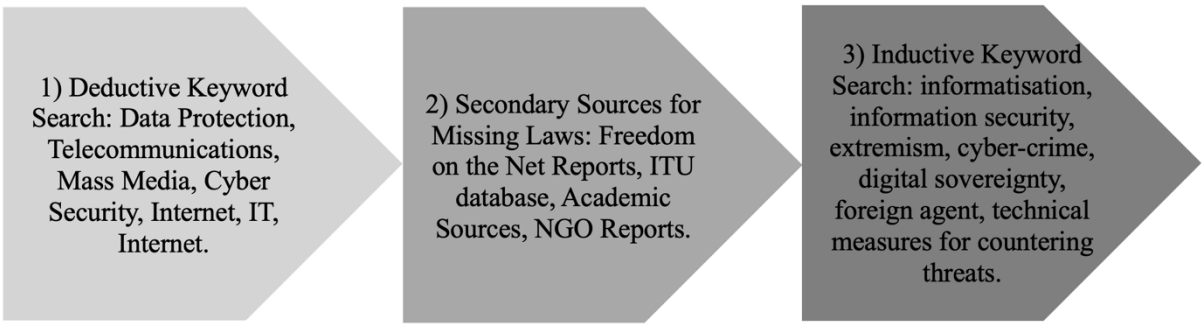

Figure 1- Data Collection Method

Once identified, relevant laws were compiled and downloaded. They were collected, where possible, in English[13], with those unavailable subjected to machine translation. Whilst this loses a certain amount of nuance from the original text, it was the fairest way to perform analysis and compare the texts one to one considering none of the languages are the author's native.

After collection, the texts were analysed by hand using the qualitative analysis software MaxQDA according to the method of qualitative content analysis (QCA). As described by Dey (1993), QCA requires the formation of qualitative main and sub-categories, which are used as a "coding frame" to analyse text. The formation of sub-categories allows for close analysis, whilst maintaining a systematic approach and allowed for the comparison of laws differently worded but providing for the same practice.

The main categories used in this study were derived from the empirical research of the previous section which described the SCO's internet sovereignty laws, namely: access, content, data, and infrastructure control[14]. As the only category not deduced from the previous section, "data control" was included due to the central focus on data as a resource in the Indian concept of "digital sovereignty", as discussed in the theoretical chapter.

In keeping with this coding frame, relevant sections of the collected laws were identified and compared with those of other states to create timelines of legal harmonisation. Carrying out this process by hand was far more inefficient than the original machine-assisted methodology proposed by Lemon and Antonov (2020). The benefit was in thoroughness, I can be confident to have caught as many of the relevant laws for each state as could be found with the tools at hand. Crucially, this analysis was not focused on the semantic level, which would likely be lost in translation, but rather on the concrete provisions of these laws for internet governance practice. Machine tools using keywords for analysis could have missed moments

[13] Relevant versions coming from the UN's database, China Law Translate from Stanford, the ITU Database.

[14] Appendices B, C, D, and E.

where different wording creates the same provision for the same basic practice across states with different legal culture.

Having created timelines from these main categories, qualitative analysis systematically described the data collected through division into subcategories, through which, according again to QCA, larger conclusions can be drawn (Schreier, 2012). These subcategories were devised in a deductive process driven by the theoretical research in Chapter 2 of this thesis. The inductive categories derived from the empirical data themselves, as well as theses deductive categories are displayed in Figure 2.

Main Category - Deductive	**Subcategories - Inductive**
Access Control	**Internet Shutdowns:** State directed restrictions of network access, which can be directed at a regional level, or towards certain sections of society. **Licencing:** State controls access to networks by restricting access to only those organisations granted licences after screening through authorised government body. **User Restriction:** The state directly, or more commonly through aligned tech companies, controls individual users' access to the internet through requiring, for example, government IDs to be verified before rendering services. **Foreign Business Restriction:** The state restricts foreign businesses' access to the national internet segment, above and beyond that of domestic companies.
Content Control	**Defamation/slander:** restrictions on online content legally deemed to be untrue and insulting in nature. **Sedition:** restrictions on actions calling for subversion of a constitution and an incitement to insurrection. **False Information:** The State uses technical or legal means to restrict access to information deemed to be "false". **Extremism:** Restriction of access to content which is legally defined as extremist.

	Indecency: Restriction of access to content considered from the moral legal perspective of the state to be indecent. **Blasphemy:** Restriction of access to content considered to insult a religion or religion(s) of a state. **Three Evils:** Restriction of access to content containing the "three evils" of terrorism, separatism, and extremism. **Propaganda:** Promoting a positive image of the state through information dissemination. **Anti-Protest:** Restriction of disseminating information calling for protest. **Hate Speech:** Speech acts inciting violence to a specific group based on differentiating factors such as race, religion, sex, orientation etc. **Foreign Agents:** Laws labelling organisations or individuals as "foreign agents" with the intention of de-legitimising their voice **Foreign Businesses:** Laws restricting the content of foreign businesses and the information they are allowed to disseminate on the country's territory. **Discreditation of Armed Forces:** Laws preventing content considered to "discredit" the armed forces of the country.
Data Control	**Data Localisation:** Mandating the storage of information on the territory of a given state, or defined group of territories. **Surveillance:** Provisions providing for the state's ability to monitor, gather and interpret users' data, typically in the interests of state security, law enforcement. **Data Retention:** Provisions mandating the storage of user data for extended periods to allow for state search activities.

	User Identification: Mandated storage of data used to identify users.
Infrastructure Control	**Technical Equipment:** Mandated installation of government software on the network allowing for operational search. **National DNS:** The extension of state control over the national domain naming system, either through state ownership of companies or through establishing a state DNS separate to the global ICANN system. **Critical Infrastructure Registers:** The creation of national registers of critical network infrastructure. **State Exchange Points:** State control of the network exchange points on the country's borders.

Figure 2- Analytical Sub-Categories

Taking the similarities between laws providing for these sub-categories and the first adopter of certain provisions, policy innovators and later adopters in certain areas can be identified. Testing these theses against the wider context of developments in the organisation and between the member states, conclusions can be drawn as to the mechanisms by which policies had come to be harmonised, thereby testing the devised hypotheses.

As such, the process for this testing is as follows: if SCO member X introduces a provision, which is then subsequently adopted by country Y, the harmonisation hypothesis H1 is confirmed. Evidence for the hypothetical mechanisms is then collected, to confirm or disprove each of, H2, H3, H4, and H5. If convincing evidence for these hypotheses are found, external factors were then sought, to test for alternative explanations. The evidence of external factors was taken as either entirely or partly disproving these hypotheses as they conceivably have an influence on the transfer of practices reducing the hypotheses' claims to causality.

Finally, whilst this process tracing of plausible causality can provide useful insights into interactions within the SCO, it is important to recognise the limitations of this approach as described in Section 2.1. Firstly, as a qualitative study, this thesis provides no means to statistically verify the causality behind events it describes. Whilst in some cases the evidence of harmonisation seems undeniable, for example in the case of the identical wording of Article 15 of Tajikistan's 2003 counterextremism law and Article 12 of the Kyrgyz 2005

counterextremism law, in others, connections could be spurious. Nevertheless, the findings remain a valuable contribution to the understanding of the role of the SCO in authoritarian learning and can provide a useful basis for future quantitative research.

4 Research Findings and Discussion

4.1 Access Control Laws

The first main category was that of "access control" which examines states' ability to restrict or approve access to the internet based on criteria they themselves define. In keeping with the internet sovereignty concept, such provisions are the "border controls" for countries' digital territory, deciding which individuals or organisations can enter, and which are turned away. As such, provisions in this area are valuable for autocrats. Limiting network access to those disloyal to the regime creates an information space which reciprocates the state's legitimising narrative and closes out dissenting voices, limiting the ability of oppositional forces to mobilise online.

In this area, 48 provisions were highlighted and assigned the category "access control". These provisions were then organised chronologically[15], and subsequently coded into the four sub-categories of laws identified from the theoretical and empirical analysis and described in Figure 2. These four subcategories included: *internet shutdowns* (10), *licencing* (15), *user restriction* (18) and *foreign business restrictions* (5). From these subcategories, (6) specific legal provisions were identified as providing for harmonised practice between these states including mass media laws, network shutdown laws, foreign business restrictions, user restrictions on "extremist" individuals, website restrictions for hosting prohibited content, and user restrictions based on providing real identity data. The data in their final analysed form are displayed within Figure 3, a timeline of their implementation by member states[16]. Above the line are provisions not considered harmonised between states, either for their uniqueness or, more commonly, because they were worded differently enough that harmonisation seemed implausible. Provisions below the line had enough textual similarity to be considered harmonised, with colours denoting the relationships between them. The following discussion breaks down each of these provision types, divining the identities of innovators and adopters,

[15] Found in Appendix B
[16] Created using the time.graphics tool, available at: https://time.graphics/line/851543.

describing the causes behind their implementation, and interrogating whether the SCO plays a role in their diffusion.

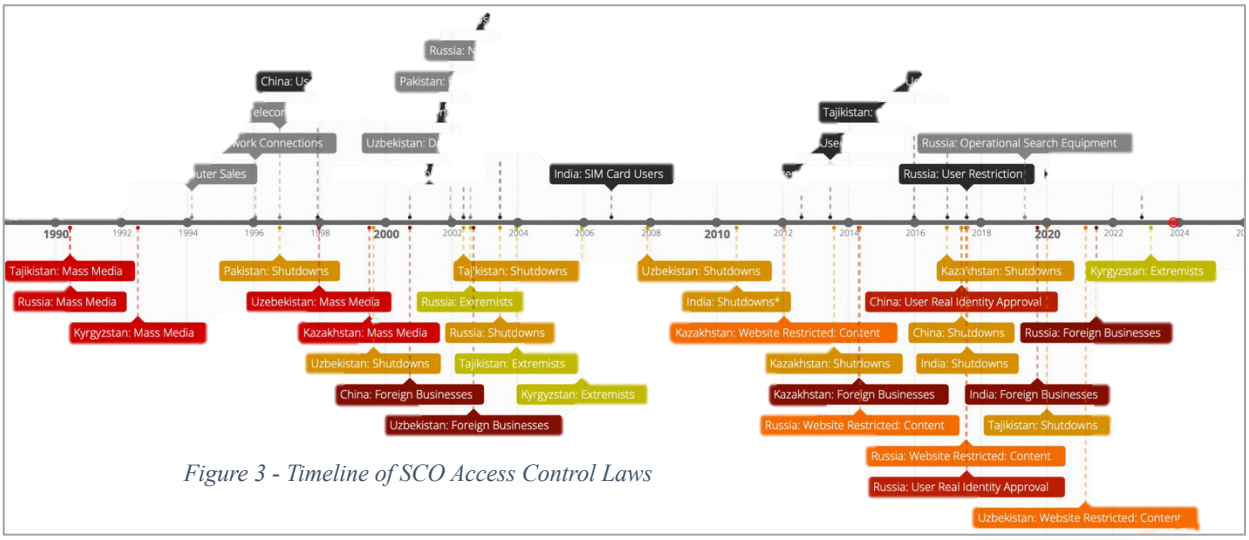

Figure 3 - Timeline of SCO Access Control Laws

4.12 Laws on the Licencing of Mass Media Outlets on the Internet

In the absence of a legal regime for managing the developing internet, Tajikistan, Russia, Kyrgyzstan, and Uzbekistan applied their mass media laws to the digital space[17]. This meant online publishers, at this time largely blog hosting sites or the websites of existing media, would be required to apply for a licence to provide services. Significantly, these laws all carried the name "On Mass Media" and the same provision for controlling the "dissemination of mass media". The benefit of these laws to the regimes introducing them was in gatekeeping the voices that could be heard in the online space, in the same way as print media had traditionally been controlled. Carrying the same text, and creating the same provisions for distributing digital media, these laws are "harmonised" according to the test for H1.

Importantly, however, as their promulgation pre-dates the establishment of the SCO, this harmonisation could not come about through organisational diffusion. As described previously, harmonisation came from the Soviet Mass Media Law[18] as its text served as the basis for these later laws as they appeared, with few changes made. The inclusion of this example in analysis serves as an example of the outside factors affecting harmonisation. Legal culture, alongside possible diffusion processes, influences the implementation of later laws and is an important external factor included in later analysis. This case serves, therefore, to

[17] Excluding Kazakhstan, which explicitly disqualifies websites from the law.
[18] Law No. 1552-1 "On the Press and Other Mass Media" adopted by the Supreme Soviet of the USSR on 12 June 1990.

challenge the assumption of diffusion (H6), as outside processes had more significance for transfer than the SCO.

4.13 "Extremist" Access Control and the "Three Evils" of Content Control

The second type of harmonised laws provided for restricting "extremist" individuals' internet use and removing content produced of an "extremist" nature. Whilst these aspects were coded separately, the discussion is enhanced by bringing these subcategories from access and content control together for analysis here, due to the significant thematic overlap. These laws[19], which appeared in a near identical form across Russia and Central Asia, loosely apply the term "extremist" to individuals performing actions loosely defined by the respective regimes as a danger to the "constitutional order". As has been previously discussed (Goldsmith, 2005; Aris, 2009; Ziegler, 2016), these laws are deliberately vague, describing a range of actions as extremist, including calling for the incitement of "social or class discord", without providing a definition for what "discord" entails (Kazakhstan, "On Countering Extremism", 2005). As a tool for autocrats, therefore, these laws are effective in limiting internet access to individuals calling for change to the existing system, whether violent or otherwise, thereby controlling the narrative in this "national" online segment.

On the surface, such provisions seem to have first been adopted by Russia with their law "On Countering Extremism" (2002), with the Central Asian states following over subsequent years. The descriptions of "extremist actions" in this law, however, require a different interpretation:

"1) extremist activity (extremism): forcible change of the foundations of the constitutional order and violation of the integrity of the Russian Federation; public justification of terrorism and other terrorist activities ..."(ibid)

[19] Russia "On Countering Extremism" (2002), Tajikistan "On the Struggle with Terrorism" (2003), Kyrgyzstan "On Countering Extremism" (2005), Kazakhstan "On Countering Extremism" (2005), Uzbekistan "On Countering Extremism" (2018).

Here the definition clearly takes on the "Three Evils" (2001) of terrorism, extremism, and separatism from the SCO charter, ratified a year previous to the publication of the Russian version. As described previously, these tenets originated with the adoption of the Chinese Computer Information Network and Internet Security, Protection and Management Regulations (1997), making China the innovator of these norms. As studies have shown, the concept of the "Three Evils" originated from "counter-terror" operations in Xinjiang in the 1990s (Li, 2019), with the name itself seemingly originating from a Chinese folk tale (Wilhelm, 1921). As such, the convention's wording can be viewed as an application of Chinese counter-terror strategies with policy transfer formalised through the SCO. In this sense, authoritarian learning has taken place, with members taking lessons on digital governance as developed by China in Xinjiang. Correspondingly, Figure 4 displays the content control laws which explicitly describe the "Three Evils" alongside the access control laws for "extremists".

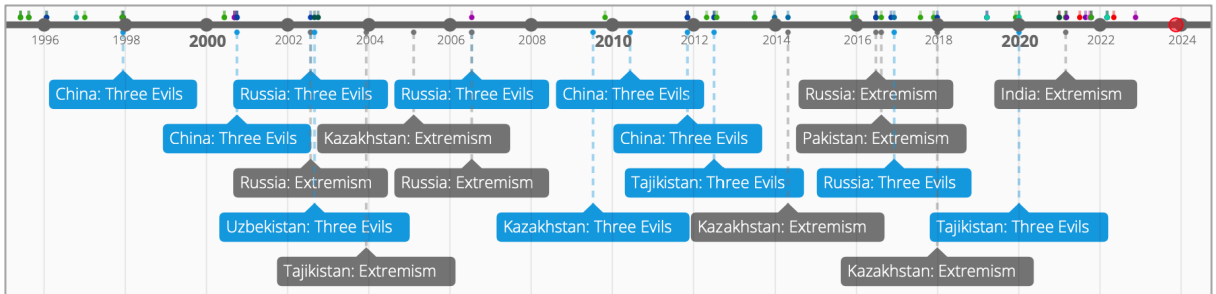

Figure 4 - "Extremism" Access Control Laws and Restrictions on "Terroristic, Separatist or Extremist" Content

This case provides evidence for the "state-organisational alignment" hypothesis (H3), as the Russians, and then later the Central Asian members, had knowledge of previous adoption from ratifying the convention in 2001, and then implemented the same definitions as laid down in that document. What's more, India and Pakistan adopted similar extremist access laws after joining the RO[20] evidencing a further transfer of this rhetorical frame. Whilst in a democratic organisation such an alignment would seem natural, SCO membership does not mandate passing domestic laws to mirror organisational norms. This means that members actively chose to align their legal regimes with the organisation, confirming H3 for these access and content control provisions.

The later adoption by Kyrgyzstan and Kazakhstan, however, limit the argument that "state-organisational alignment" is the only cause for policy transfer. Here, the contextual events of the Colour Revolutions of 2005 help rationalise later adoption. The signing of the

[20] India: Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021; Pakistan: Prevention of Electronic Crimes Act 2016.

Kazakh law in February 2005 coincided with the protests in neighbouring Kyrgyzstan around the disputed Presidential election, with Akayev later fleeing through Kazakhstan into Russia (Al Jazeera, 2005). In Kyrgyzstan, the law came after the transition of power in August and was the first to be signed by Bakiyev, ostensibly to stabilise a country in turmoil (Rotar, 2005). The adoption of these laws, therefore, was driven by the necessities of the developing acute situation on the ground in Central Asia, rather than purely through policy alignment with the SCO.

The establishment of the RATS register of extremist organisations in 2006 also seems a significant mechanism. This mandated restricting the activity of designated organisations across the territory of all member states according to the "mutual recognition" principle from the "Concept of Cooperation of SCO Member States" (2005). This aligned practice and created a vast area, both physical and digital, which could not be accessed by designated "extremists", and on which content they created would be restricted. In this regard, cooperative practice also contributes to the diffusion of "extremist" policies, partially confirming H5, the hypothesis of "diffusion through practice".

This policy transfer, therefore, constitutes a diffusion of a rhetorical frame, which allowed for the criminalisation of activity based on the definitions decided on by the separate regimes. In this regard, content produced by all manner of organisations, from feminist activists in Russia (Lokshina, 2017), to journalists in Uzbekistan (Stroehlein, 2008), Sikhs in India (Pundir, 2023) and Muslim religious figures in China (Human Rights Watch, 2021) were restricted.

In this case of access and content control for extremists, therefore, harmonisation (H1) is confirmed, with state-organisational alignment (H3) confirmed for Russia and Tajikistan. The transfer driven by acute regime stability requirements in Kazakhstan and Kyrgyzstan caused only a partial confirmation of state-organisational alignment (H3) for their context. The practice mechanism (H5) also was a partial player for diffusion, with coordinated practice a cause for regulatory alignment of rhetorical frames. Conclusions can be drawn, therefore, as to the role of the SCO in authoritarian diffusion. It has served as a vehicle for China to institutionalise norm promotion and provide a template for legal provisions to be later implemented by fellow members. In turn, these authoritarian states gather effective strategies for suppressing the voices of targeted groups and reduce their capacity to challenge authority across the vast territory of the SCO. As such, this is a perfect situation for diffusion to take place within a RO. The members' motivations aligned with the original adopter and ready-made provisions were provided in the form of the SCO convention. Crucially, this diffusion

concerned practices with a proven track record in the innovating country, China, showing that authoritarian learning accompanied the transfer process.

4.14 Provisions for Internet Shutdowns

Internet shutdowns, as the least technically advanced internet control method, are a blunt tool for authoritarian regimes in the digital sphere. Disconnecting troubled regions from the internet helps autocrats cover the excesses of their repressive measures and prevents protestors from massing by disrupting communication. As such, each of the member states implemented laws providing for the cessation of internet services in times of crisis and in the interests of national security[21]. Whilst widely distributed chronologically, these laws are harmonised, as they refer to the same measures – the temporary suspension of networks, in the same emergency situations for the same justifications of national security.

The role of the SCO in this harmonisation is, however, harder to define. The laws covering shutdowns in Pakistan and Uzbekistan, for instance, came about before the ratification of the charter and seem influenced by practical considerations, with both nations sporadically using shutdowns in areas of unrest, such as Balochistan (El-Khawas, 2009) and Andijan (Stroehlein, 2008). Russia's communications law is similarly difficult to tie to SCO processes, as it was passed before the commitments to increased cooperation in cybersecurity brought about by the establishment of information sharing in 2013 (Quingsheng, 2019). As such, the harmonisation of these laws seems more driven by internal processes, where facing the same challenges of increased mobilisation from digital technologies were met by the blunt tool of internet shutdowns, meaning that for these first cases the diffusion hypothesis H6 cannot be supported.

In Kazakhstan, India and China, however, there is evidence that the SCO played a role in policy transfer. Kazakhstan's law, for instance, was passed following the Astana summit of 2011, where Nazarbayev publicly called for greater cooperation in cyberspace. At the same time, the RATS had been headed by Kazakh former Security Officer Evgeny Syosev, who made it his target to "further harmonisation of national legislation in the field of countering terrorism" (Sysoev, 2017) and had been lobbying for this process with the governments of SCO members.

[21] Pakistan: Telecommunications Act 1996; Uzbekistan: Law No. 822-1 of 1999; Tajikistan: the Legal Regime of the State of Emergency" 2000; Russia: On Communications 2003; Kazakhstan: Law No. 121-V, 2013; China: Cybersecurity Law 2017; India: Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules, 2017.

Furthermore, the adoption of harmonised shutdown laws in India and China in 2017, following the second SCO cyber-security exercises in Xiamen, presents a case for the role of the organisation in supporting harmonisation. The exercises coincided with the passing of China's Cybersecurity Law (2017) as well as shortly preceding India's "Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules" (2017). India's promulgation of this law is particularly significant – having been introduced at the country's entrance into the organisation, alignment through practice has driven the adoption of authoritarian legal provisions. Importantly, the leaders of these states met and discussed cybersecurity during the Astana summit of the same year (Xinhua, 2017), as well as having had security personnel trained by the Chinese Cyber Authority (State Council Information Office of the People's Republic of China, 2022). In this regard, harmonisation is driven through H5, the "practice hypothesis" in which the adoption of authoritarian "best practice" requires introducing the same legal provisions as previously tested by other states. Furthermore, whilst there is not significant evidence to make a claim to causality, the statements promoting legal harmonisation and proliferation of visits of Sysoev to member states in this period would indicate that the direct transfer hypothesis (H2) could have played a role in this process – a topic requiring organisation-internal documents to be proved, which are not publicly available.

In sum, the provisions for internet shutdowns in the SCO partially confirm the diffusion hypothesis (H6), driven by the process of diffusion through practice, with some important caveats. As a low-tech solution for access control, authoritarian states had been informally implementing such practices long before policy transfer, indicating that internal conditions drove isomorphic adoption of practices. The passing of shutdown laws was not necessary for the use of such measures, with evidence from both China in Xinjiang (Wong, 2010) and India in Manipur (Software Freedom Law Centre India, 2023), of them being used before ratification. In this sense, these legal provisions are a *formalisation*, rather than *introduction* of practice influenced by the structures of the SCO. Importantly, these considerations were not limited to the authoritarian states of this research, with India, an established but flawed democracy, showing itself to be open to the adoption of authoritarian digital practice in the interests of national security, to the extent that it became the "world leader" in using such strategies (Ellis-Petersen & Hassan, 2023).

4.14 Real-Identity Requirements for Internet Services

Further harmonised access control laws mandated real identity user verification before internet service provision. The initial adopter of such practice was China, which had already mandated prior approval of network connections for users by 1997[22]. Subsequently, however, there has been a spate of laws requiring biometric identification for establishing internet connections for users across the countries of the SCO, including, for example, India's restrictions on SIM card purchasing following the Mumbai attacks of 2008. Harmonised, however, are Russia and China's laws[23] requiring the use of government ID for online identity verification and the use of native social media products such as VKontakte in Russia and WeChat and Sina Weibo in China. As with national borders, online access borders are becoming controlled by biometric verification.

The ramifications of these laws are felt hardest amongst the civil societies of both nations. The number of individuals arrested in Russia for their activities in social media, for instance, has been steadily growing since at least 2016, with the largest increase since the tightening of censorship following Russia's full-scale invasion of Ukraine (OVD Info, 2023). Meanwhile in China, such methods have been used for the suppression of opposition in Hong Kong (Leung, 2023) and have caused the development of online euphemisms, with "tea invitations" referring to law enforcement raids tied to online behaviour and "human flesh search" describing doxing (Wang et al. 2010). Thus, the benefit of such practice for these authoritarian regimes is clear, tying the real identities of users to their posts can deter the use of the internet for activism, with law enforcement authorities having an easier job of locating dissenting users.

In terms of the causes for adoption, China, as the innovator, can be shown to have taught Russia strategies for access control through leaked documents obtained by Radio Free Europe, with Russian adoption of the same provisions taking place only a month later than the Chinese (Belvodeyev et al. 2023). These sources document high-level meetings taking place between the Chinese Cyber Agency and Roskomnadzor through 2017, and most importantly at Xi's visit to Moscow following the SCO conference in the same year and immediately preceding the cybersecurity exercises in Xiamen. As such, the harmonisation seems likely a result of H2, the "direct exchange" mechanism through bilateral relations between member states. This,

[22] "Computer Information Network and Internet Security, Protection and Management Regulations" (1997).

[23] China: Cybersecurity Law of the People's Republic of China 2017; Russia: Federal Law No. 241 FZ "On Amending Articles 10.1 and 15.4 of the Federal Law "On Information, Information Technologies and Information Protection".

however, cannot represent a confirmation of the diffusion hypothesis (H6), as, whilst the organisation provided a relevant platform for diffusion in providing a learning room for the leaders and a platform for communication, the ultimate transfer took place outside of the formal institutional framework of the organisation. Instead, the formal organisation seems to have provided a platform to support the informal linkages between states, supporting transfer, but not causing it.

4.15 Foreign Business Restrictions

The final access control aspect harmonised were the restrictions on foreign-owned and operated digital businesses with interests on member states' territories. These took numerous forms, from the limitation of shares of foreign ownership in media companies, such as in Uzbekistan and India[24], through the requirement for the registration and inspection of foreign online companies before market access in China, Russia and Kazakhstan[25], to mandating companies establish a domestic legal entity for doing business on their territory in China, Kazakhstan, Russia, Pakistan[26]. This latter set of laws is striking for the investigation of access control harmonisation. First introduced by Kazakhstan in 2014, this is the first example in analysis for policy innovation to have occurred outside Russia and China. The almost identical wording across these laws and the same requirement for websites with over 500,000 users would indicate that the later adoptions adapted Kazakhstan's innovation, but all happened 7 years later within six months of each other in 2021. Importantly, these adoptions followed the release of the organisation's "Joint Statement on Information Security" after the Moscow summit of 2020, which had also seen discussions on the digital economy and had been led by the Kazakh delegation, with India the only country not signing the final formulation (SCO, 2020). As such, whilst the text does not mention these specific measures and so cannot qualify for state-organisational alignment (H3), the direct exchange hypothesis (H2) is a plausible mechanism for exchange, with all leaders having been in the same (albeit digital) room to discuss the topic of the harmonised laws. At best, however, this policy transfer can be

[24] Uzbekistan: Law of the Republic of Uzbekistan No. 405-II 30.08.2002; India: Press Note 4 Amending FDI Policy 18.09.2019.

[25] China: Internet Information Service Management Measures Law No. 292 25.09.2000; Russia: Federal Law No. 236 FZ 01.07.2021; Kazakhstan: Law of the Republic of Kazakhstan No. 118-VII 03.05.2022.

[26] China: Personal Information Protection Law of the People's Republic of China 01.11.2021; Kazakhstan: Law of the Republic of Kazakhstan No. 128-VI; amending 'On Informatization' 23.04.2014; Russia: Federal Law No. 236-FZ 01.07.2021; Pakistan: Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 12.10.2021.

understood as a case of likely diffusion, rather than proven – the lack of transparency of the organisation precludes making a definite statement, with the content of information security talks unpublished.

What's more, the refusal of India to sign up for this agreement is an expression of the country's dissatisfaction with China in the digital realm, with the banning of Chinese platforms, such as TikTok, having occurred in 2020 for "security concerns" due to skirmishes along the Galwan River (Perper, 2020). This shows the limitations of the "diffusionary" effects of the SCO, with distrust between members reducing the potential for cooperation. Indeed, the numerous border disputes between members and the resulting distrust must be seen as a key limiting factor for cooperation and a key focus of analysis.

4.16 Conclusions on Access Control

The evidence of this section confirms the diffusion hypothesis (H6) for the SCO as causing legal harmonisation with some significant limitations. The extremism laws introduced by the Central Asian members and Russia following their ratification of the SCO convention in 2001 are a clear case confirming the "state-organisation alignment" hypothesis (H3), as their wordings recreate the text of the agreement almost exactly. In this case, however, alignment was not immediate, with adoption proceeding later in Kazakhstan and Kyrgyzstan sparked as a response to domestic pressures. The provisions for internet shutdowns showed a partial effect of the SCO for helping alignment through practice (H5), in this case driving the formalisation of shutdown laws, with practice pre-existing. The evidence for this hypothesis is strengthened through the harmonisation of laws on extremism following the establishment of the RATS unified register of extremist organisations in 2005 – which required cooperation in restricting users, driving a convergence in practice and policy. As the licencing laws discussed at the opening of this chapter indicate, however, the adoption of authoritarian practices was not singly caused by the SCO, having developed according to domestic pressures. Furthermore, real identity verification laws in Russia and China were shown to harmonise through bilateral cooperation between the countries' digital authorities, in the background of SCO forums, but not as a direct result of agreements reached in the organisation's framework. Finally, the harmonisation of laws controlling the access of foreign businesses to domestic digital markets challenged the perception that China and Russia dominate the norm setting of the SCO. As has been previously discussed for regime succession (Lemon, 2021), fellow member Kazakhstan

in this case played the role of policy innovator for the organisation and region with respect to such businesses restrictions.

As such, the SCO plays an important role in bringing policymakers of the region together and has relevance in the legal formalisation of authoritarian digital practice through the transfer of rhetorical frames. Evidence suggests that earlier adoption of practices, such as Russia's laws on identity verification or Chinese definitions of extremism as first applied in Xinjiang, drives the later adoption of similar provisions in other member states. This analysis, therefore, presently agrees with previous studies which suggest that the benefit of ROs is in providing platforms for regimes to learn from one another. In this case, however, the "learning rooms" causing policy transfer were largely informal, rather than being driven by the institutional structures. Finally, there is some evidence from India's alignment with the organisation that this effect expands beyond authoritarian states and can lead to restrictive internet management in a democracy – a topic recently discussed (Cottiero & Haggard, 2023), but worthy of greater focus in the literature. At the same time, the country's disputes with China were a key limiting factor in closer alignment with the organisation.

4.2 Content Control Laws

Provisions for controlling internet content have become a staple means for authoritarian regimes to regulate their online space. As described by Guriev and Treisman (2019), modern autocrats have become particularly adept at controlling information flows. Most often, information is restricted when it damages a leader's legitimacy or otherwise leads to dissatisfaction with the regime. In this sense, the most stringent regimes can attempt to curate a country's narratives by removing the oxygen supply for oppositional discourse to form.

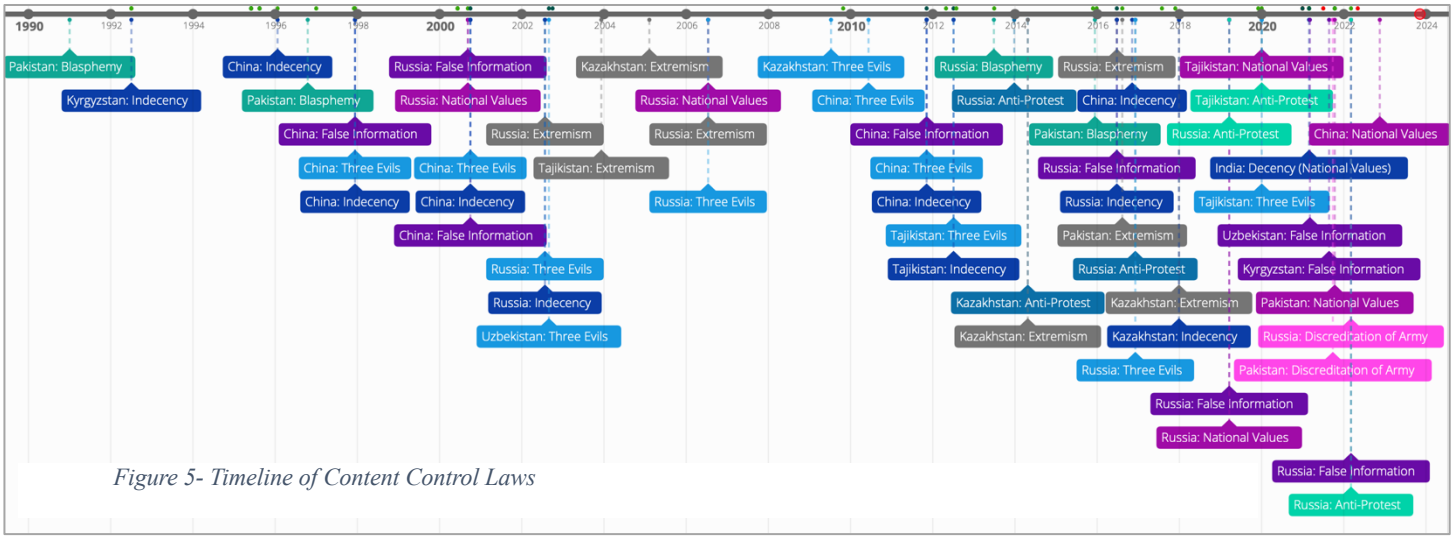

Figure 5- Timeline of Content Control Laws

Digital content restrictions are, therefore, a modern continuation of censorship practices, which have long been a critical aspect of authoritarian control. As could be predicted, these provisions were the most frequent in the data collected (58). To make sense of this large volume of data, this main category was divided into the (14) subcategories described in Figure 2 and then coded according to the specific analytical categories used in this discussion of: *indecency* (11), *false information* (9), *three evils*[27] (11), *national values* (10), *anti-protest* (7), and *army discreditation* (2). As before, a timeline was created to display the adoption of these types of laws chronologically and is displayed in Figure 5; this time, however, only laws considered harmonised were included, with the full graph available online[28]. In this discussion these laws have been grouped to aid in analysis and brevity.

4.21 Indecency and "National Values" Laws

The most seemingly innocuous of legal provisions in this section were those concerned with controlling content deemed indecent or in some way harmful to a "national morality". Common also to democracies, such laws are designed to protect citizens from content deemed inappropriate or otherwise disturbing, with those in the data mostly covering content of a sexual, verbally explicit, or violent nature. "National Values", meanwhile, described laws which defined certain moral, spiritual, or cultural values as defining characteristics of the state, which were to be protected through content controls. For ease of analysis, these categories are analysed together here but it should be borne in mind that each were internally harmonised, rather than between categories.

As can be seen in Figure 5, both China and Pakistan were the earliest nations to apply some form of "national values" to the internet, which tracks with the ideological underpinnings of these Socialist and Islamic nations. Indeed, the significant differences in the aims of these laws precludes their coding as harmonised and their introduction in the developmental period of the internet indicates they were a continuation of existing ideological policy. Russia's (2000) "Doctrine of Information Security", however, is the first legal text in the secular, non-ideological states to carry protections for normative understandings of the country's values in the "preservation of the cultural and historical values of the peoples and nationalities of the Russian Federation and rational utilization of the information resources amassed by society

[27] Discussed in the previous chapter.
[28] https://time.graphics/line/852194

that constitute national property". This moment marked the shift to content control laws which applied prescriptive values to the online space, which began in earnest following Russia's adoption of Federal Law No. 30 FZ (2019), the "internet sovereignty law" and saw the protection of "national dignity" enshrined in law. What followed was a spate of similar legal projects in China, Tajikistan, Kazakhstan, Pakistan, and Kyrgyzstan[29], which each adopted similar formulations. Whereas before content had been removed that was a threat in its criticism of government, this content control focused on the cultural and moral aspects of peoples' lives. This represents a shift in the aims of authoritarian governance in Asia, therefore, from the *preventative* management of discontent to the *prescriptive* imposition of norms onto their native populations, a transition from nationalism as a narrative tool, to a practical aim.

Relevant to this thesis is that these laws adopted the language of the Ekaterinburg "Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization" (2009) which called for a prohibition on the "dissemination of information prejudicial to the socio-political and socio-economic systems, spiritual, moral and cultural environment of other States". This formulation is almost certainly influenced by China and Russia's previous provisions for "national values" but came ten years before the adoption of these later laws. As such, it is difficult to intimate that "state-organisational" alignment (H3) is the cause for this harmonisation. Instead, narratives of national exceptionalism seemed to develop in member states outside of the influence of the organisation across the 2010s. The significant similarity in text between these provisions, however, indicates that the SCO agreements were a repository for legal norms, which were adopted by authoritarians when the need arose. In this regard, diffusion (H6) is disproved for this case. As before with the case of access laws, however, it seems likely that the SCO does play a role in the standardisation of provisions across member states, again allowing the harmonised formalisation of existing practices. In this sense, SCO conventions are a repository and justification for the adoption of nationalist authoritarian internet governance norms, which are used by member states at times of their choosing relating to domestic concerns but are, nevertheless, rhetorically unified from due to the RO's normative basis.

4.22 False Information Laws

[29] China: Management of Internet Comment Post Services 2022; Pakistan: Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules 2021; Tajikistan: Law of the Republic of Tajikistan "On Countering Extremism" No. 1655 2020.

As can be seen in Figure 5, laws restricting the dissemination of "false information" have increased over the past few years, particularly since the Covid-19 pandemic[30]. Such provisions are useful for the SCO's authoritarian rulers, who typically appointed authorised digital media bodies to decide on which content is "false"[31]. The proliferation of such bodies can be seen as more pernicious than the diffusion of laws of the Three Evils as described in the previous section. These laws allow regimes to define and enforce acceptable narratives within cyberspace, manipulating society into obedience by only allowing voices in agreement to be heard.

Provisions of this sort have been seen in Russia, Uzbekistan, and Kyrgyzstan, with China again the initial adopter. These laws were considered harmonised, as they contain similar texts and each rely on the same institution, some form of an authorised body of digital media, to decide on "the truth" and censor content, rather than on receipt of a court order. With harmonisation confirmed, however, it is difficult to isolate a mechanism through which these legal provisions could conceivably have diffused through the SCO. Whilst the legal texts are very similar, particularly between Kyrgyzstan, Russia, and Uzbekistan, there is no official agreement from the SCO which could serve as the basis for these laws. Similarly, there is no public evidence of meetings concerning false information within the SCO. In this case, therefore, it is impossible to propose an organisational mechanism for causing harmonisation.

Instead, this represents a transition within these authoritarian states towards tighter information control in general, concentrating on widening categories of content and accompanying general autocratization processes. Looking outside the organisation, there could be several causes for this, which warrant future scholastic focus. The first is almost certainly the wider thematization of "fake news" brought about by the Covid pandemic, which has brought content controls to the attention of many leaders also outside the RO. Secondly, the proliferation of technologies which can better filter information, particularly those offered by the Chinese through the Digital Silk Road Initiative, allows states to tighten controls by expanding their censorship capacity. Finally, leaders may have become emboldened to apply such processes as the perceived influence of the liberal democratising narrative wanes. Whilst

[30] China: Cybersecurity Law 2011; Russia: Federal Law 208 FZ: amending Federal Law 149-FZ 2016; Kyrgyzstan: Law of the Kyrgyz Republic No. 101 "On Protection from False and Inaccurate Information" 2021; Uzbekistan: Law of the Republic of Uzbekistan No. 3RU-679.

[31] China: Cyberspace Administration; Russia: Roskomnadzor; Uzbekistan: Uzkomnazorat; Kyrgyzstan: State Communications Agency under the Ministry of Digital Development of the Kyrgyz Republic.

H6 for diffusion inside the SCO has been disproved in this case, false information laws could provide an interesting case study for future academia, to understand if other diffusion processes are taking place in Asia – or whether external factors are causing an isomorphic conversion of practice.

4.23 Anti-Protest Laws

A further type of content control provision found to be harmonised was the restriction of calls for protest on the internet. Common across China, Russia, Kazakhstan, and Tajikistan, these laws carried the same wording of restricting "calls for mass events/protests" (Law of the Republic of Kazakhstan No. 200-V, 2014) and carry significant benefits for authoritarian rulers in criminalising social mobilisation[32]. Russia was the first adopter of such a law in 2013, which has been linked the waves of protests seen in the country from 2011 (Gorbunova, 2017). The subsequent lack of mass protest in the country since the adoption indicates that such laws controlling content, in combination with other methods, can positively contribute to regime stability.

Research has shown Russian and Chinese bilateral cooperation on techniques for limiting protest in SCO external settings (Belvodeyev et al. 2023), which limits the claims which can be made as to the direct influence of the SCO on diffusing these provisions. Nevertheless, the first cyber-security drills in 2015, carried out in the auspices of the organisation focused heavily on identifying "extremist calls for mobilisation" (Quingsheng, 2019), a euphemistic description of calls for protest. As such, member states had been trained on how to control content calling for protest prior to the introduction of these legal provisions. What's more, the establishment of the internet expert group, as part of the 2013–2015 outline of SCO Cooperation, and the resulting collaboration between law enforcement provided a further platform for the best practices learnt from Russia's experience of protest to diffuse through the organisation (Wood, 2015). As such, these provisions for countering the dissemination of calls for protest confirm H5, the hypothesis referring to diffusion through practice.

This confirmation of the diffusion hypothesis is different, however, as it sees Russia rather than China as the initial adopter of anti-protest content control laws. In this regard, and

[32] Kazakhstan: Law of the Republic of Kazakhstan No. 200-V, 2014; Russia: Federal Law No. 398 FZ: amending Federal Law 149-FZ of July 27, 2006; Tajikistan: Law of the Republic of Tajikistan "On Countering Extremism" No. 1655, 2020; Cybersecurity Law of the People's Republic of China, 2016.

mindful of the backroom meetings between the countries at this time, it seems logical to suggest that the policies were initially transferred bilaterally between these states in direct exchange, before being "taught" under the auspices of the organisation at Xiamen and, therefore, further diffused through member states. Nevertheless, content controls on calls for protests again indicate how the SCO as an RO provides situations were autocrats have the opportunity to learn from one another, and subsequently better control their civil societies.

4.24 Conclusions on Content Control

Content control laws, as the most prolific area of harmonisation between member states, provide evidence for the SCO as an organisation which can promote policy transfer. At its least influential, in the case of laws restricting content against "national values", the organisation served as a repository of provisions which were later adopted by members to control their online segment – playing a role in the standardisation and rhetorical justification of internet governance laws, rather than as the cause for diffusion. On the other hand, the rapid proliferation of content control laws concerning calls for protest is a clear case for the organisation as having been significant for diffusion, through the practice mechanism. "False information" laws were the only area where harmonisation occurred in the absence of the SCO's influence and could conceivably have been caused by external factors. Nevertheless, as a trend going forward in both Chinese and Russian internet governance practices, who have been shown to be key innovators of digital policy for the SCO, it would be unsurprising if future agreements cover the dissemination of false information, once again formalising and standardising existing practice as described here.

4.3 Data Control Laws

Laws covering the storage and transfer of data have become a focus of governments across the globe in recent years, with the European Union's GDPR laws seen as something of a "gold standard" (Schünemann & Windwehr, 2021). Such laws establish users' rights to privacy as well as organising the rules for businesses to generate profit through data. The power afforded by possessing sensitive information over citizens as well as to collect rents by creating regulations for business have made such laws a valuable tool for authoritarian leaders. At its core, digital data control in an authoritarian sense is also surveillance, a modern incarnation of established practices. The subcategories of provisions for data control defined in analysis were:

(wide) surveillance (8), *data retention* (9), *cross border restrictions* (8), *data localisation* (7), *user identification* (13), and *operational search/backdoor access* (8). Analysis once again thematically groups these aspects to better describe the processes at work.

4.31 Surveillance, Data Retention and User Identification laws

Surveillance has long been a staple of authoritarianism, with access to compromising information on citizens being a means to coerce obedience or detect and punish transgression. Access to large amounts of citizens' data also can help authoritarian structures overcome the "dictator's dilemma", which argues that there are significant incentives within an authoritarian system to provide leaders with inaccurate information, particularly when the truth endangers those reporting (Wintrobe, 1998). It is, therefore, unsurprising that the data contained laws for each country[33] allowing some form of surveillance for operational search activities or mandated backdoor decryption for security services. Underpinning these laws are requirements for companies' "data retention", which sees them storing data for a mandated minimum period and "user identification laws", which tie these data to real people. Whilst first introduced through China's Internet Information Service Management Measures (2000), a spate of such laws was seen within SCO member states beginning with Russia in 2014, as displayed in Figure 6. These laws are harmonised in that they contained the same provisions for "storing on the territory […] information on the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds or other electronic messages of Internet users and information about these users within six months from the date of completion of such actions, as well as provide this information to authorized state bodies, carrying out operational-investigative activities or ensuring the security [..]", with slight variations.

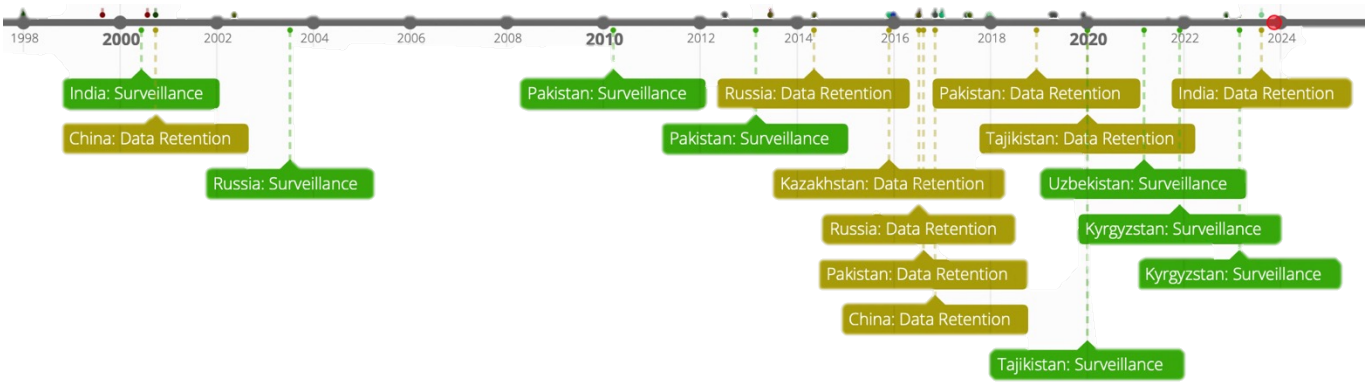

Figure 6- Timeline of Surveillance and Data Retention Laws

[33] Figure 6 and Appendix D.

The rapid uptake of such laws and their harmonised text can be correlated to the increased focus on information security and cyber cooperation in the period following the 2015 Xiamen cybersecurity drills, which saw joint statements from the organisation as well as China and Russia's bilateral agreement on cooperation in cyberspace (2015). What's more, the Strategy for the Development of the Shanghai Cooperation Organisation until 2025 agreed on in 2015, laid a basis to "improve the mechanism of co-operation in combating the use of ICTs for terrorist purposes" which was to increase information sharing within the RATS. This practice related cooperation indicates that "diffusion through practice" remains the most-likely mechanism for these laws to have transferred between members, with the lack of a policy document recommending data retention limiting other conclusions.

This fits with the rapid expansion of laws requiring the identification of users as can be seen in Figure 7. The increase of these measures following the cybersecurity drills of 2015, which focused on "identifying extremist users" (Quingsheng, 2019) and their locations in real time, must be linked with security services' needs to have the correct data on users to make this practice viable.

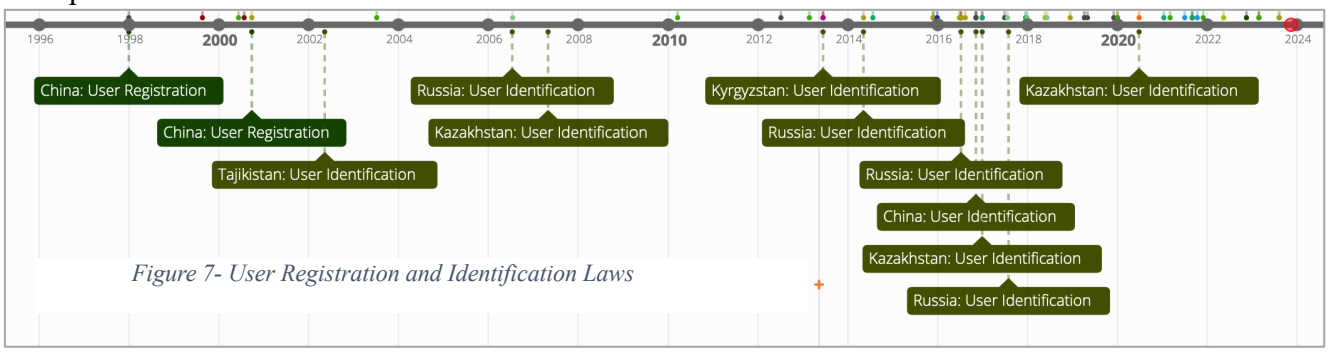

Figure 7- User Registration and Identification Laws

Interestingly, this development of harmonised data policies within a RO was not taking place for the first time. The European Union's adoption of the Data Retention Directive (2006) was the first instance, before being overturned by a landmark decision in the Court of Justice of the European Union (2014). The harmonisation in the SCO, therefore, seems to counteract the idea that international norms would drive the diffusion of practices, with the SCO taking the opposite path to the EU in reducing user's data rights. The parallel is, however, important to indicate. The increased formalisation of cooperation between the member states of the SCO can be seen, in this period at least, to have led to significant increases in harmonisation, as had been the case with European integration.

As such, for the case of data retention and surveillance, the diffusion hypothesis (H6) can be confirmed, with diffusion through practice (H5) the mechanism with the highest influence on this process, as the training in surveillance necessitated the introduction of data retention and user identification laws. Here, further adoption has been driven by domestic

regime stability concerns, with the SCO providing ready-made policy solutions for emerging problems. As before, therefore, the "diffusionary" effect of this RO has been shown to be most effective in providing solutions to common problems across the block, where direct regime stability benefits can be felt.

4.32 Cross Border Restrictions and Data Localisation

The restriction of data flows across national borders and data localisation are most widely viewed as the quintessential internet sovereignty provisions (Fraser, 2016; Polatin-Reuben & Wright, 2014). Whilst China has mandated controls on such transfers since the establishment of the internet on its territory, such laws were not widely developed in other member states until Russia's Federal Law No. 242-FZ (2014) which began a period of rapid adoption across other members of similar provisions. Such laws fulfil several useful functions for authoritarian regimes. Firstly, relocating servers can allow for direct access for security services in cases of operational search, increasing the capacity for repressive control of the population. At the same time, as seen in Russia, the purpose can be rhetorical. Painting foreign tech companies as an enemy and then achieving victory by forcing their contrition in opening more offices on a country's territory, also providing domestic jobs, can create a legitimising narrative for rulers. Finally, the vast fines levied against companies for failure to comply with such restrictions, such as the 41 million RUB from Facebook in Russia (Federal Service for Supervision of Communications, Information Technology and Mass Media, 2021), can be a means to force rents from the world's most wealthy companies, a source of capital which can be invested into the security forces or in the continued loyalty of co-opted elites.

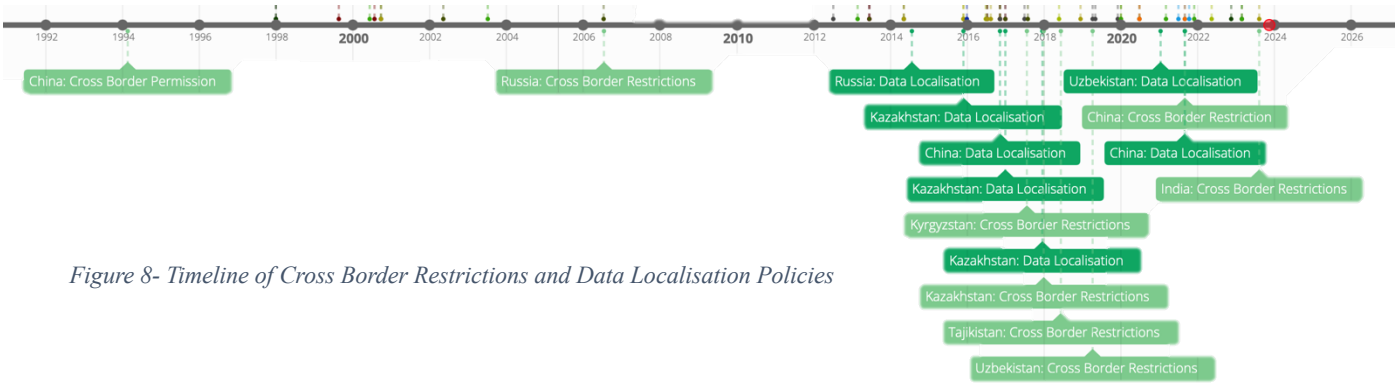

Figure 8- Timeline of Cross Border Restrictions and Data Localisation Policies

Russia's innovation of such a policy in 2014 came as a result of the country's invasion of Ukraine and the resulting stand-off with the West, including sanctions. With a concern of over-exposure to foreign systems, the movement to consolidate Russian data "onshore" came as part of a wider drive towards increased self-sufficiency in Russia, with isolation described

euphemistically as "sovereignty". Whilst such a logic of adoption could also apply to China, which faces similar "strategic competition" from the West, the Central and South Asian countries adopted such policies for other reasons. Chan et al. (2022) argue that for Kazakhstan and Uzbekistan these laws are used as a means to strike a balance with big tech companies, trading market access for access to the companies' content control systems. Importantly, in Uzbekistan and India, localisation laws have not just been applied to Western tech companies, with Chinese TikTok and WeChat having been restricted in both jurisdictions[34] (Putz, 2022; Doval, 2020). In all of these cases, however, policies have the same ultimate goal of allowing greater state control over the tech companies which wield influence on their territory.

A connection with the activities of the SCO is, however, harder to draw. The transfer of data localisation policies seems connected to the rhetorical frames promoted in discussions at the institution around the concept of information security, with the normative calls for "internet sovereignty" and the recentring of governance around the state most impactful. In this sense, the WIC conference calls for internet sovereignty and submission to the UN from the SCO members, which came about at the same time as these laws were introduced, seem the most likely influence on these policy shifts[35]. This makes the "international legitimation" hypothesis (H4) the most likely for the case of data localisation laws, with prior adoption in neighbouring states and the legitimation of the concept through international institutions the greatest cause for transfer. This argument has its limitations, however, not least because this correlation could come as a result of countries appraising the successes of the Russian adoption outside of the auspices of the SCO, through other legal entities such as the CIS or through bilateral communication. As such, it is inappropriate to claim that the SCO alone caused diffusion. Instead, the normative legitimation provided by the international efforts of the organisation should be considered as playing a role in policy transfer, alongside external factors. In this sense, the RO has again been shown to be most valuable in diffusing a particular rhetorical frame, which uses "sovereignty" as a justification for repressive and rent seeking practice.

4.33 Data Control Laws Conclusions

This discussion of data control has exposed new mechanisms and motivations for the diffusion of internet sovereignty policies through the SCO. Surveillance laws, including data

[34] Also now in Kyrgyzstan, Pakistan and Russia.
[35] See Appendix A.

retention and user identification, were diffused through the practice mechanism, with training provided to member states providing the impetus for further adoption. Data localisation laws, including limitations on the cross-border transfer of data, provided a more complicated case. The authoritarian logic of their adoption, with surveillance and rent seeking motivations, was clear. The mechanism for their diffusion, however, is opaquer, with the "international legitimation" of norms seemingly the most viable explanation for the role of the SCO, with the transfer of rhetorical framing of "sovereignty" most influential.

Importantly, there exist a number of external factors which conceivably drive harmonisation which preclude confirming the diffusion hypothesis for data localisation. The adoption of such laws can, for instance, be attributed to the exposure of these authoritarian regimes' digital economies to foreign tech companies in the globalised market and resulting concerns of their significant influence. Going forward, therefore, the extent to which countries chose to segregate their internet through such measures could greatly depend on their perceptions of the role of such players and their perceived ability to coerce them into obedience with state monetary and access demands.

4.4 Infrastructure Control Laws

The final main category to discuss is that of infrastructure control, which largely supports the introduction and implementation of the policies described in the previous analysis. Policies in this area strengthen state capacity in the digital realm, which, not lost on SCO members, has seen an increasing focus in recent years on regimes' abilities to gain control over the physical and digital infrastructure of the network, described by Denardis and Musiani (2014) as the "turn to infrastructure". Despite public ownership of the largest telecommunications providers in all members aside from India, policies have been introduced across the region to provide the state with even greater tools to control the network. In the data were 29 separate provisions which were coded according to the sub-categories of *nationalisation, national DNS, technical equipment mandates,* and *infrastructure registration.* Within these subcategories, four types of provision were found to be harmonised based on the significant similarities of their text with one another: *operational search equipment* (9), *state*

exchange points (5), *national DNS* (3), and *registers of critical infrastructure* (3), as displayed below the line on Figure 9.

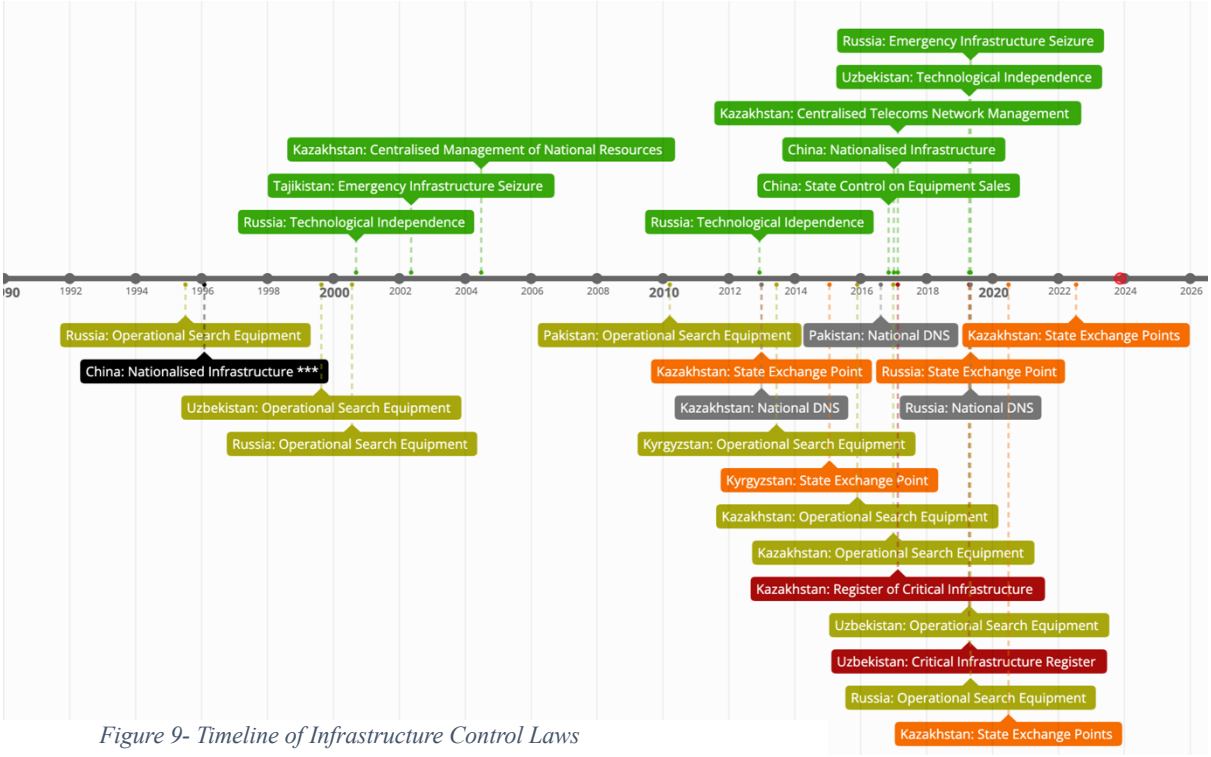

Figure 9- Timeline of Infrastructure Control Laws

4.41 Technical Equipment for Operational Search Activities

The first group of harmonised policies were those mandating the installation and operation of equipment used to conduct operational-search activities on telecommunications networks which were first innovated through Russia's adoption of the SORM system in the late nineties[36]. The wordings of these provisions, as displayed in yellow on the table, were almost identical, leading to a confirmation of harmonisation (H1). In Russia, the use of such equipment has expanded over the years with increasing technical possibilities allowing for greater usage cases, as well as the increasing surveillance requirements from the security forces as described in the previous chapters. The practical benefit of these systems is considerable, in 2012 alone, the Russian state used the SORM and SORM-2 systems 540,000 times for the interception of phone and internet traffic, allowing for the gathering of significant volumes of data on citizens (Lewis, 2014). It is unsurprising, therefore, that such policies would become popular across

[36] Federal Law No. 144-FZ (1995); "On Communications" (2000). Order of the Ministry of Communications No. 2339 of 9 August 2000.

fellow Asian autocracies, with Uzbekistan, Pakistan, Kyrgyzstan and Kazakhstan aligning their policies with Russia.

The initial harmonisation of these laws were justified through the same securitised language, with Uzbekistan's law, taking on almost the identical terms following the ratification of the Russian law (Law of the Republic of Uzbekistan No. 822-1, 1999). In this case, the narrative norms surrounding internet governance in Russia allowed for the further adoption of such control measures but, crucially, occurred before the SCO's foundation, showing that narrative frames can transfer outside of the institutionalised structures of an RO. The formulations of the laws in Central Asia similarly have been linked to existing Soviet network monitoring techniques, meaning legal culture has again been a factor limiting conclusions as to diffusion. Simultaneously, there are myriad external factors which preclude claiming that the SCO membership is the root cause of these developments. Firstly, significant technology transfers have been shown to take place outside of the organisation with the Chinese "Digital Silk Road" project, which accompanies the larger "One Belt, One Road" initiative, having invested significantly into member states. Pakistan, for instance, most recently announced the "China South Asia Tech Transfer Centre" in Islamabad – the result of years of bilateral transfer agreements (Shafqat, 2023).

For this case, therefore, it would be erroneous to assume that the SCO played a crucial part in the diffusion of these legal practices. Instead, the rhetorical framing of the introduction of such laws in Central Asia took influence from Russian security narratives and the techniques themselves were pushed by technology transfer. In this regard, external factors have again been shown as more influential than the structures of the organisation for legal harmonisation, weakening the claims made to diffusion (H6).

4.42 National DNS

The final aspect included in the analysis of this thesis pertains to the digital infrastructure on which the internet relies, namely the central registers of domain names, the "digital address book" for every page on the internet. Originally established by the US government, the DNS system was initially organised by the ICANN and IANA, which, as non-profits, registered most new domains throughout the developmental stage of the internet as well as many national top-level domains. Crucially, this was organised globally, which in recent years has clashed with nations' attempts to control a national internet segment. As such, a significant movement has developed within member states towards the development of national

DNS systems, which would work independently of the international system, and would be particularly effective if external internet connections were to be disrupted.

Whilst such a system has existed in China since the "China Internet Domain Name Regulation" (2004), such national DNS registries were first introduced in other member states through Kazakhstan's "Law of the Republic of Kazakhstan No. 128-IV of 2012", which "determine(d) the administrator and registrar of domain names, approve the rules for registration, use and distribution of domain names in the space of the Kazakhstani segment of the Internet" and established the KazNIC as the national registry. In practice, however, Kazakhstan continues to rely on the international domain system, with domain registration companies, which, whilst regulated under the strict remit of the Kazakhstani government, continue to act as middlemen to the global registries of ICANN and IANA. Russia's sovereign internet law[37], by comparison, does foresee the establishment of a fully separate national DNS system (Paganini, 2019). Claimed to be operational since January 2021, this system would allow a Russian intranet to function, even if all connections to the world wide web were to be severed. This movement towards a more segregated internet is concerning for the civil societies of these nations, with such systems only seen in the most closed regimes of North Korea's "Kwangmyong" intranet and Iran's potential National Information Network (Gerschewski & Dukalskis, 2018; Stone, 2023). Again, it is infeasible to draw a direct causal link between these domestic developments and the SCO. The isolation of a national intranet is an attempt to consolidate domestic power, rather than a project of regional security cooperation. At the same time, this disconnection is an application of the internet sovereignty norms endorsed by the organisation, in that it represents a maximisation of the role of the state to govern its own network.

Importantly, however, such a movement towards segregated national networks has been promoted on an international level by Russia as a proponent. The nomination of a Russian candidate for the Secretary General of the ITU against the American candidate Bogdan-Martin, for instance, was a move to increase the influence of the country on international internet norms and promote the position it takes and shares with the SCO (ICANN, 2022). Whilst unsuccessful, the continued commitment in statements from the organisation in favour of the "international promotion" of its own internet governance model would indicate this is to remain a crucial aspect of geopolitical contention for the years to come. As such, these laws mirror the organisation's narrative framing, accepting, and purporting the same norms. Whilst causality

[37] Federal Law of the Russian Federation 90-FZ, 2019.

is again impossible to prove, it does seem once again, therefore, that SCO norms play a role in states' justifications for creating national DNS registers, with narratives promoted by the SCO internationally justifying practice.

4.43 Infrastructure Control Conclusions

Infrastructure control represents the most challenging aspect for claiming the SCO as an institution causes the diffusion of internet sovereignty practices. The requirements for technical equipment for operational search were adopted due to internal considerations and as a result of technical developments, rather than because of SCO processes. Similarly, whilst mirroring the norms of the SCO for internet governance, the nationalisation of DNS systems seems caused more significantly by concerns of being disconnected from the global network, either voluntarily or involuntarily, rather than institutional conventions. As the lynch pin from which other measures can be introduced, however, infrastructure controls should not be seen as separate from the processes originating from SCO cooperation. The narrative frames of the organisation justify their introduction and the technology transfers led by China facilitate their spread. As such, with the foundation of the "SCO Technology Transfer Center" in 2020, it can be expected that the greater cooperation of member states in developing practice based on these new capabilities could drive further harmonisation in future through H5, the practice mechanism (Xinhua, 2020).

5 Concluding Remarks

This thesis took the concept of "internet sovereignty" to investigate the role of the SCO in diffusing authoritarian practices in the digital sphere. In a theoretical sense, sovereignty, as applied to the network, was shown to logically presuppose a territorialisation of the internet, where digital borders can be drawn around national "information spheres". This concept developed through a blending of Chinese sovereignty and Russian information security ideals and first entered official discourse around the SCO conference in 2011. In turn, it came to justify the reorientation of internet governance around the state and the securitisation of narratives around the internet, it was codified in the SCO's conventions, and shaped official agreements between member states in information security. On a normative level, it was used to justify stringent controls over internet access, content, data, and infrastructure.

These aspects were the main categories of analysis to investigate the extent to which the SCO, as a claimed "League of Authoritarian Gentlemen" (Cooley, 2012), played a role in the diffusion of these norms into the separate member states. Using the method of causal process tracing as developed by Lemon and Antonov (2018) to describe "legal harmonisation" of the provisions enacted by member states to govern the internet on their own "digital territory", it was shown that the organisation causes diffusion in specific circumstances:

The rhetorical frame of the "Three Evils" was most influential. Once introduced through the SCO founding convention (2001), it was frequently recreated in the domestic internet governance laws of member states, driving diffusion through the state-organisational alignment of access and content control laws to the RO's conventions. In turn, this narrative helped to bolster the SCO's authoritarian regimes by controlling the information available to citizens. As a narrative innovated by China, this confirmed the assumptions of previous scholars that the SCO functions as a platform for the promotion of their internet governance norms. Even at its least influential, the idea of the "Three Evils" was used by all member states to justify a myriad of authoritarian practices and aligning provisions discursively, despite external developments being the ultimate cause for adoption.

Similarly, cooperation through the RATS and in cybersecurity drills caused diffusion through practice, having formalised shutdown laws, proliferated content controls on calls for mass protest, and expanded user data retention. In this case, Russia is the key player in innovating policy, learning from the mass protests in the winter of 2011-2012 and transferring this knowledge through direct exchange to China. In turn, the Chinese Cyber Authority taught such strategies to fellow member states by hosting cybersecurity drills in Xiamen. The expansion of technology transfers was also a driver of legal harmonisation, with the caveat that bilateral agreements through multiple institutions, including the DSR, were at least as important as the SCO for causing transfer.

At the same time, some key aspects to internet sovereignty, in data localisation, the tightening of state control over infrastructure, and foreign business restrictions could only partially be linked to the processes of the SCO. These provisions were harmonised through their reliance on the rhetorical framing of internet sovereignty as a legitimising narrative, confirming a partial role for international legitimation. The development of the practices, however, occurred independent of the institution's processes and related to domestic security concerns. In this sense, the SCO provided the norms to justify authoritarian states' development of practices centring the state in internet governance, rather than providing the impetus to implement them.

Significantly, India, as the state most prolific in implementing internet shutdowns, was shown to also engage with these norms in the justification of its practice, showing that the learning process spreading through the SCO does not just affect consolidated authoritarian states, but also impacted a democracy. This finding is important for future studies of ROs. The internet sovereignty narrative can not only bolster authoritarian states but can also drive the legitimation of illiberal policies in democracies. This has serious implications for the liberal multistakeholder model which continues to prevail in Western democracies and should be the subject of future research into ROs in studies of authoritarianism.

This thesis has further implications for future study. Applying Gerschewski's (2013) "Three Pillars" to digital authoritarian practice was valuable in understanding the conversion of practice in this region. Outside the straightforward conclusions which can be drawn on the benefits of digital surveillance and censorship for repression and legitimation, more studies should focus on how controls on tech companies using citizens' data, such as those innovated by Kazakhstan, can strengthen authoritarian regimes' co-optation abilities. Indeed, with expanding discussions on "surveillance capitalism", more thought should be cast on how to theorise the role of big data companies in authoritarian economic systems and whether a rise of "state surveillance capitalism" can be observed. Understanding these practices can also help in democratic contexts to counteract the risks of backsliding in digital policy and be used to bolster the ability of civil societies in authoritarian states to circumvent such controls.

In sum, authoritarian learning within the SCO takes place, with cooperation in cyberspace, including the diffusion of internet sovereignty practices, contributing to the stabilisation of member states' authoritarian regimes. In this sense, ROs deserve more focus within the literature on authoritarianism, specifically concerning their role for supporting non-democratic practices and bolstering regimes. Furthermore, attention should be paid as to how illiberal internet governance narratives play out in further ROs and territories outside the remit of this paper. Is China's norm promotion as effective in ASEAN? Does BRICS membership help spread authoritarian digital approaches to the democracies of India, Brazil, and South Africa? Answering such questions should help understand the greatest current challenges in global internet governance. How great is the threat of movement towards a "splinternet"? And, more importantly, how can modern democracies counteract narratives legitimising authoritarian policies, when promoted through the structures of ROs? Through answering such questions, methods can be found for supporting liberal models of internet governance and buttress democracies against the expansion of authoritarian "internet sovereignty" ideals and their realisation in practice.

References

Acharya, Amitav and Alastair Johnston. 2017. *Crafting Cooperation: Regional International Institutions in Comparative Perspective.* Cambridge: Cambridge University Press. DOI: https://doi.org/10.1017/CBO9780511491436

Al Jazeera. 2005. *Ousted Kyrgyz leader flees to Russia.* Online. [access 08.11.2023 https://www.aljazeera.com/news/2005/3/26/ousted-kyrgyz-leader-flees-to-russia]

Allison, Roy. 2008. "Virtual regionalism, regional structures and regime security in Central Asia." *Central Asian Survey* 27(2). pp. 185–202. https://doi.org/10.1080/02634930802355121

Ambrosio, Thomas. 2008. "Catching the 'Shanghai Spirit': How the Shanghai Cooperation Organization Promotes Authoritarian Norms in Central Asia". *Europe-Asia Studies* 60 (8). pp. 1321-1344

Ambrosio, Thomas. 2010. "Constructing a framework of authoritarian diffusion: concepts, dynamics, and future research." *International Studies Perspectives* 11(4). pp. 375–92. DOI: 10.1111/j.1528-3585.2010.00411.x

Ambrosio, Thomas and Jakob Tolstrup. 2019. "How do we tell authoritarian diffusion from illusion? Exploring methodological issues of qualitative research on authoritarian diffusion" *Qual Quant.* 53. pp. 2741–2763. DOI: https://doi.org/10.1007/s11135-019-00892-8

Applebaum, Anne. 2012. *Iron Curtain: The Crushing of Eastern Europe, 1944-1956.* New York: Anchor.

Areddy, James. 2014. "China Delivers Midnight Internet Declaration – Offline". *The Wall Street Journal.* Online. [accessed 27.10.2023 https://www.wsj.com/articles/BL-CJB-24963]

Aris, Stephen. 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): 457-482.

Barlow, J.P. 1996. *A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation. Online. [accessed 16.10.2023 https://www.eff.org/fr/cyberspace-independence]

Bartelson, Jens. 2006. "The Concept of Sovereignty Revisited." *European Journal of International Law*, 17 (2). pp. 463–474. DOI: https://doi.org/10.1093/ejil/chl006

Belli, Luca. 2021. “BRICS Countries to Build Digital Sovereignty” in ed. Belli, Luca. 2021. *CyberBRICS: Cybersecurity Regulations in the BRICS Countries.* Cham: Springer.

Belvodeyev, Daniil, Andrei Soshnikov and Reid Standish. 2023. “Exclusive: Leaked Files Show China And Russia Sharing Tactics On Internet Control, Censorship”. *Radio Free Europe, Radio Liberty.* Online. [accessed 07.11.2023 https://www.rferl.org/a/russia-china-internet-censorship-collaboration/32350263.html#:~:text=On%20the%20sidelines%20of%20the,information%20inside%20Russia%20under%20the]

Best, Michael and Keegan Wade. 2009. “The Internet and Democracy Global Catalyst or Democratic Dud?” *Bulletin of Science, Technology & Society,* 29 (4). Online. [accessed 15.10.2023 https://bpb-us-w2.wpmucdn.com/sites.gatech.edu/dist/e/965/files/2018/12/internet.democ_.pdf]

Börzel, Tanja and Thomas Risse. 2014. “From Europeanization to diffusion: Introduction” in. eds. Risse, Thomas. 2017. *Domestic Politics and Norm Diffusion in International Politics.* New York: Routledge.

Budnitsky, Stanislav and Lianrui Jia. 2018. “Branding Internet sovereignty: Digital media and the Chinese-Russian cyberalliance” *European Journal of Cultural Studies.* 21(5). pp. 594-613. DOI: https://doi.org/10.1177/1367549417751151

Cali, Jeanine. 2012. *Sedition Laws in India.* Online. [accessed 08.11.2023 https://blogs.loc.gov/law/2012/10/sedition-law-in-india/]

Cameron, David and Mitchell Orenstein. 2012. “Post-Soviet authoritarianism: the influence of Russia in its “near abroad”’, *Post-Soviet Affairs* 28(1), pp. 1–44.

Celeste, Edoardo. 2021. “Digital Sovereignty in the EU: Challenges and Future Perspectives” in eds. Fabbrini, Federico, Edoardo Celeste and John Quinn. 2021. *Data Protection beyond Borders: Transatlantic Perspectives on Extraterritoriality and Sovereignty.* London: Bloomsbury.

CGTN. 2017. *Combating Terrorism: SCO joint cyber exercise held in Xiamen.* Online. [accessed 07.11.2023 https://news.cgtn.com/news/3d556a4d79594464776c6d636a4e6e62684a4856/share_p.html]

Chen, Titus. 2010. “China’s Reaction to the Colored Revolutions: Adaptive Authoritarianism in Full Swing.” *Social Science Research Network.* Online. [accessed 06.09.2023 https://www.zbw.eu/econis-archiv/bitstream/11159/90547/1/EBP07338092X_0.pdf]

Claessen, Eva. 2020. “Reshaping the Internet – the impact of the securitization of internet infrastructure on approaches to internet governance: the case of Russia and the EU.” *Journal of Cyber Policy,* 5 (1). pp. 140-157. DOI: https://doi.org/10.1080/23738871.2020.1728356

Collins, K. 2009. “Economic and security regionalism among patrimonial authoritarian regimes: The case of Central Asia.” *Europe-Asia Studies*, 61(2). pp. 249-281.

Commonwealth of Independent States. 1996. *Kontseptsiya formirovaniya informatsionnogo prostranstva Sodruzhestva Nezavisimykh Gosudarstv ot. 18 Oktyabrya 1996 goda.* Online. [accessed 20.10.2023 https://cis.minsk.by/page/7548]

Cooley, Alexander. 2012. *Great Games, Local Rules*. Oxford: Oxford University Press.

Cooley, Alexander. 2015. “Authoritarianism Goes Global: Countering Democratic Norms.” *Journal of Democracy,* 26(3). pp. 49-63.

Couture, Stephane and Sophie Toupin. 2019. “What does the notion of “sovereignty” mean when referring to the digital?” *New Media & Society*. 21(10). pp. 2305-2322. DOI: https://doi.org/10.1177/1461444819865984

Creemers, Rogier. 2020. *China’s Approach to Cyber Sovereignty.* Berlin: Konrad Adenauer Stiftung. Online. [accessed 20.10.2023 https://www.kas.de/documents/252038/7995358/China’s+Approach+to+Cyber+Sovereignty.pdf/2c6916a6-164c-fb0c-4e29-f933f472ac3f?version=1.0&t=1606146961537]

Darwich, M. 2017. “Creating the enemy, constructing the threat: the diffusion of repression against the muslim brotherhood in the middle east.” *Democratization* 24, pp. 1289–1306.

Debre, Maria J. 2021. “The dark side of regionalism: how regional organizations help authoritarian regimes to boost survival” *Democratization*, 28(2), pp. 394-413, DOI: 10.1080/13510347.2020.1823970

Debre, Maria. 2022. “Clubs of Autocrats: Regional Organisations and Authoritarian Survival”. *The Review of International Organisations,* 17. pp. 485-511.

De Haas, Marcel. 2017. "Relations of Central Asia with the Shanghai Cooperation Organization and the Collective Security Treaty Organization." *The Journal of Slavic Military Studies* 30 (1): 1-16. DOI: 10.1080/13518046.2017.1271642.

Deibert, Ronald J. 2008. “The Geopolitics of Internet Control: Censorship, Sovereignty, and Cyberspace”. in: eds. Chadwick, Edward and Philip Howard. 2008. *Routledge Handbook of Internet Politics*. London: Routledge. DOI: https://doi.org/10.4324/9780203962541

de la Torre, C. 2017. “Hugo Chávez and the diffusion of Bolivarianism.” *Democratization* 24, pp. 1271-1288.

DeNardis, L, and F. Musiani. 2016. “Governance by Infrastructure”. In: Musiani, F., Cogburn, D.L., DeNardis, L., Levinson, N.S. (eds) *The Turn to Infrastructure in Internet Governance. Information Technology and Global Governance*. New York: Palgrave Macmillan. DOI: https://doi.org/10.1057/9781137483591_1

Dey, Ian. 1993. *Qualitative Data Analysis: A User-Friendly Guide for Social Scientists.* London: Routledge.

Dolowitz, David and David Marsh. 1996. “Who Learns What from Whom: A Review of the Policy Transfer Literature”. *Political Studies* 44(2). pp. 343-357. DOI: https://doi.org/10.1111/j.1467-9248.1996.tb00334.x

Dolowitz, David and David Marsh. 2002. “Learning from Abroad: The Role of Policy Transfer in Contemporary Policy-Making”. *Governance* 13(1). pp. 5-23. DOI: https://doi.org/10.1111/0952-1895.00121

Doval, Pankaj. “Tiktok, UC Browser among 59 Chinese apps blocked as threat to sovereignty”. *The Times of India.* Online. [accessed 21.11.2023 https://web.archive.org/web/20200630043219/https://timesofindia.indiatimes.com/business/india-business/chinese-apps-banned-in-india-tiktok-uc-browser-among-59-chinese-apps-blocked-as-threat-to-sovereignty/articleshow/76699679.cms]

Dragu, Tiberiu and Yonatan Lupu. 2021. “Digital Authoritarianism and the Future of Human Rights.” *75(4).* pp. 991-1017. DOI:10.1017/S0020818320000624

Duarte, Marisa Elena. 2017. *Network Sovereignty: Building the Internet across Indian Country.* Washington: Washington University Press.

Eichensehr, Kristen. 2015. “International Cyber Governance: Engagement Without Agreement?”. *Just Security.* Online. [accessed 19.09.2023 https://www.justsecurity.org/19599/international-cyber-governance-engagement-agreement/]

El-Khawas, Mohamed. 2009. “Musharraf and Pakistan: Democracy Postponed.” *Mediterranean Quarterly*, 20(1). pp. 94-118.

Elkink, J. A. 2011. "The International Diffusion of Democracy." *Comparative Political Studies* 44 (12): 1651-1674. https://doi.org/10.1177/0010414011407474.

Epifanova, Alena. 2020. “Deciphering Russia’s “Sovereign Internet Law”. Tightening Control and Accelerating the Splinternet.” *DGAP Analysis No. 2, January 2020*.

Online. [accessed 15.10.2023 https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law]

Epifanova, Alena and Philipp Dietrich. 2022. "Russia's Quest for Digital Sovereignty. Ambitions, Realities, and its Place in the World." *DGAP Analysis No. 1, February 2022*. Online. [accessed 16.10.2023 https://dgap.org/en/research/publications/russias-quest-digital-sovereignty]

Evans, Mark and Jonathon Davies. 2002. "Understanding Policy Transfer: A Multi-Level, Multi-Disciplinary Perspective." *Public Administration* 77(2). pp. 361-385. DOI: https://doi.org/10.1111/1467-9299.00158

Federal Service for Supervision of Communications, Information Technology and Mass Media. 2021. *Sud oshtrafoval Facebook, Twitter i WhatsApp na 36 mln rublei za nelokalizatsiyu baz dannykh rossiiskikh pol'zovatelei na territorii RF.* Online. [accessed 21.11.2023 https://rkn.gov.ru/news/rsoc/news73828.htm]

Ferdinand, Peter. 2000. "The Internet, democracy and democratization" *Democratization, 7:1, 1-17*. DOI: 10.1080/13510340008403642

Finnemore, Martha and Kathryn Sikkink. 1998. "International Norm Dynamics and Political Change". *International Organisation* 52 (4). pp. 887-917.

Flonk, Daniëlle. 2021. "Emerging illiberal norms: Russia and China as promoters of internet content control" *International Affairs* 97 (6). pp.1925-1944. DOI: https://doi.org/10.1093/ia/iiab146

Flonk, Danielle, Markus Jachtenfuchs, and Anke S. Obendiek. 2020. "Authority Conflicts in Internet Governance: Liberals vs. Sovereigntists?" *Global Constitutionalism* 9(2): 364–86. DOI: 10.1017/S2045381720000167.

Fond "Obshestvennoe Mnenie". 2023. *Predpochtitel'nye istochniki informatsii: internet: Vostrebovannost' novostnykh saito, sotsial'nykh setei i messendzherov.* Online. [accessed 07.11.2023 https://fom.ru/SMI-i-internet/14836]

Freedom House. 2012. *Freedom on the Net 2012 - Pakistan, 25 September 2012*. Online. [accessed 08.11.2023 https://www.refworld.org/docid/5062e89c1e.html]

Fung, Courtney J. 2022. "China's use of rhetorical adaptation in development of a global cyber order: a case study of the norm of the protection of the public core of the internet." *Journal of Cyber Policy*, 7(3). pp. 256-274, DOI: 10.1080/23738871.2023.2178946

Gallagher, Mary and Jonathon Hanson. 2013. "Authoritarian Survival, Resilience, and the Selectorate Theory." in ed. Dmitrov, Martin. 2013. *Why Communism Didn't Collapse:*

Understanding Regime Resilience in China, Vietnam, Laos, North Korea and Cuba. Cambridge: Cambridge University Press.

Gandhi, J., and E. Lust-Okar. 2009. "Elections under authoritarianism." *Annual Review of Political Science*, 12, pp. 403-422.

Gerschewski, Johannes. 2013. "The three pillars of stability: legitimation, repression, and co-optation in autocratic regimes" *Democratization Vol. 20, Iss. 1*, pp. 13-38. DOI: https://doi.org/10.1080/13510347.2013.738860

Gerschewski, Johannes and Alexander Dukalskis. 2018. "How the Internet can reinforce Authoritarian Regimes: The Case of North Korea". *Georgetown Journal of International Affairs.* 12.

Glaser, Barney and Anselm Strauss. 1967. *The Discovery of Grounded Theory: strategies for qualitative research.* London: Aldine Transaction.

Glasius, Marlies. 2018. "What authoritarianism is … and is not: a practice perspective". *International Affairs* 94 (3). pp. 515-533. DOI: 10.1093/ia/iiy060

Glen, Carol. 2014. "Internet Governance: Territorialising Cyberspace?" *Politics and Policy,* 42(5). pp. 635-657. DOI: https://doi.org/10.1111/polp.12093

Goldsmith, Jack and Tim Wu. 2006. *Who controls the Internet? Illusions of a Borderless world.* Oxford: Oxford University Press.

Gorbunova, Yulia. 2017. "Online and On All Fronts Russia's Assault on Freedom of Expression". *Human Rights Watch.* Online. [accessed 21.11.2023 https://www.hrw.org/report/2017/07/18/online-and-all-fronts/russias-assault-freedom-expression]

Gosudarstvennaya Duma. 2019. *Prinyat' zakon o "suvernnom internete.* Online [accessed 27.05.2023 http://duma.gov.ru/news/44551/]

Government of the Russian Federation. 2015. "O podpisanii Soglashcheniia mezhdu Pravitel'stvom Rossiiskoi Federatsii i Pravitel'stvom Kitaiskoi Narodnoi Respubliki o sotrudnichestve v oblasti obespecheniia mezhdunarodnoi informatsionnoi bezopasnosti". *Rasporyazhenie ot 30 Aprelia 2015 goda No. 778-P.* Online. [accessed 20.09.2023 https://www.documentcloud.org/documents/2076545-5amaccs7mslxgbff1ua785wwmwcabdjw.html]

Grauvogel, J. 2018. "The spread of term limit manipulations in Sub-Saharan Africa: an example of authoritarian learning?". as quoted in Ambrosio and Tolstrup (2019).

Griffiths, James. 2019. *The great firewall of China: How to build and control an alternative version of the internet*. London: Zed Books.

Gupta, Shubh and Reeta Sony. 2021. "Quest of Data Colonialism and Cyber Sovereignty: India's Strategic Position in Cyberspace". *Legal Issues in the Digital Age.* 2(2). pp.70-81 DOI: https://doi.org/10.17323/2713-2749.2021.2.68.81

Guriev, Sergei and Daniel Treisman. 2019. "Informational Autocrats." *Journal of Economic Perspectives* 33 (4). pp. 100-127. DOI: 10.1257/jep.33.4.100

Hall, Stephen G. F. 2023. *The Authoritarian International: Tracing How Authoritarian Regimes Learn in the Post-Soviet Space*. Cambridge: Cambridge University Press.

Hall, Stephen and Thomas Ambrosio. 2017. "Authoritarian learning: A conceptual overview" *East European Politics,* 33(2). pp.143-161. DOI: https://doi.org/10.1080/21599165.2017.1307826

Hegre, Havard. 2014. "Democracy and Armed Conflict". *Journal of Peace Research* 51(2). pp. 159-172. DOI: https://doi.org/10.1177/0022343313512852

Herold, David Kurt. "Escaping the World: A Chinese Perspective on Virtual Worlds". *Journal of Virtual Worlds Research* 5(2). pp. 4-15. DOI: 10.4101/jvwr.v5i2.6206

Hitchens, Thereas and Nilsu Goren. 2017. *International Cybersecurity Information Sharing Agreements.* Center for International & Security Studies. Online [accessed 16.10.2023 https://www.jstor.org/stable/pdf/resrep20426.pdf?refreqid=excelsior%3A11d55bfc72b6a5ad25dc81c0c28ef83c&ab_segments=&origin=&initiator=&acceptTC=1]

Howard, Phillip, Agarwal Sheetal and Hussain Muzammil. 2011. "The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks?" *Issues in Technology Innovation* 13(2011). pp. 1-11.

Hulvey, Rachel. 2022. *Cyber Sovereignty: How China is Changing the Rules of Internet Freedom.* Working Paper: IGCC. Online. [accessed 20.10.2023 https://ucigcc.org/wp-content/uploads/2022/06/hulvey_sovereignty-v2-richardsonfoundation-1.pdf]

Human Rights Watch. 2021. *"Break Their Lineage, Break Their Roots"*

China's Crimes against Humanity Targeting Uyghurs and Other Turkic Muslims. Online. [accessed 20.11.2023 https://www.hrw.org/report/2021/04/19/break-their-lineage-break-their-roots/chinas-crimes-against-humanity-targeting]

Kaleji, Vali. 2023. "Challenges of Expanding the SCO to Caucasus and the Middle East". *Valdai Discussion Club.* Online. [accessed 16.08.2023 https://valdaiclub.com/a/highlights/challenges-of-expanding-the-sco-to-caucasus/]

Karmazin, Ales. 2023. "China's Promotion of Cyber Sovereignty Beyond the West" in eds. Kolmasova, Sarka and Ricardo Reboredo. 2023. *Norm Diffusion Beyond the West:*

Agents and Sources of Leverage. Cham: Springer. DOI: https://doi.org/10.1007/978-3-031-25009-5

Kerr, Jaclyn. 2016. *Authoritarian Management of (Cyber-) Society: Internet Regulation and the New Political Protest Movement.* Washington DC: Georgetown University.

Kneuer, M. and T. Demmelhuber. 2016. "Gravity centres of authoritarian rule: A conceptual approach." *Democratization* 23(5). pp. 775-796. [accessed 16.10.2023 https://doi.org/10.1080/13510347.2015.1018898]

Kolozaridi, Polina and Dmitry Muravyov. 2021. "Contextualizing sovereignty: A critical review of competing explanations of the Internet governance in the (so-called) Russian case." *First Monday* 26 (5). DOI: https://doi.org/10.5210/fm.v26i5.11687

Kolton, Michael. 2017. "Interpreting China's Pursuit of Cyber Sovereignty and its Views on Cyber Deterrence". *The Cyber Defence Review* 2(1). pp.119-154.

Kovrigin, D.E. "Formation of the institution of "sovereign internet" in the Russian Federation." *Gumanitarniye Nauki Vestnik Finasovogo Universiteta.* 12(2). 153-158. DOI: 10.26794/2226-7867-2022-12-2-153-158

Kukutai, Tahu and John Taylor (eds). 2016. *Indigenous Data Sovereignty: Toward an Agenda.* Centre for Aboriginal Economic Policy Research, College of Arts and Social Sciences, The Australian National University, Canberra. Research Monograph No. 38 2016.

Kumar, Anilesh and Daya Thussu. 2023. "Media, digital sovereignty and geopolitics: the case of the TikTok ban in India". *Media, Culture and Society.* DOI: https://doi.org/10.1177/01634437231174351

Laidlaw, Emily. 2015. *Regulating Speech in Cyberspace.* Cambridge: Cambridge University Press.

Lee, Kate Sangwon and Huaxin Wei. 2020. "Social Media as Heterotopia: Applying Foucault's Concept of Heterotopia to Analyze Interventions in Social Media as a Networked Public." *Archives of Design Research*, 33(2). pp. 5-17. DOI: http://dx.doi.org/10.15187/adr.2020.05.33.2.5

Lemon, E., & Antonov, O. 2020. Authoritarian legal harmonization in the post-Soviet space. *Democratization* 27(7). pp. 1221-1239. DOI: https://doi.org/10.1080/13510347.2020.1778671

Lemon, Edward. 2021. "The Kazakh Model? Dynamics of Regime Succession in Eurasia". pp. 53-78 in (ed.) Caron, Jean-Francois. 2021. *Understanding Kazakhstan's 2019*

Political Transition. Singapore: Palgrave Macmillan. [accessed 13.11.2023 10.1007/978-981-33-4308-5_4]

Levitsky, Steven and Lucan Way. 2002. "The Rise of Competitive Authoritarianism: Elections without Democracy." *Journal of Democracy* 13(2). pp. 51-65.

Levitsky, Steven and Lucan Way. 2006. "Linkage versus Leverage. Rethinking the International Dimension of Regime Change". *Comparative Politics,* 38 (4) pp. 379-400. DOI: https://doi.org/10.2307/20434008.

Leung, Hilary. 2023. "Hong Kong student arrested over 'seditious' posts handed strict bail terms incl. deleting all social media apps". *Hong Kong Free Press.* Online. [accessed 08.11.2023 https://hongkongfp.com/2023/06/19/hong-kong-student-arrested-over-seditious-posts-handed-strict-bail-terms-incl-deleting-all-social-media-apps/]

Lewis, David. 2012. "Who's socialising whom? Regional Organisation and Contested Norms in Central Asia". *Europe-Asia Studies.* 64(7). pp. 1219-1237. DOI: 10.1080/09668136.2012.701391

Lewis, James Andrew. 2014. "Reference Note on Russian Communications Surveillance". *Center for Strategic and International Studies.* Online. [accessed 21.11.2023 https://www.csis.org/analysis/reference-note-russian-communications-surveillance]

Li, Enshen. 2019. "Fighting the 'Three Evils': A Structural Analysis of Counter-Terrorism Legal Architecture in China." *Emory International Law Review* 33: 311.

Litvinenko, Anna. 2021. "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty." *Media and Communication* 9 (4). pp. 5-15. DOI: https://doi.org/10.17645/mac.v9i4.4292

Lokshina, Tanya. 2017. "Authorities in Southern Russia Scared of Feminism:

Police and Cossacks Harass Local Activists". *Human Rights Watch.* Online. [accessed 20.11.2023 https://www.hrw.org/news/2017/08/14/authorities-southern-russia-scared-feminism]

Major, April, Mara. 2000. "Norm Origin and Development in Cyberspace: Models of Cybernorm Evolution". *Washington University Law Review.* 78(1). Online. [accessed 16.10.2023 https://openscholarship.wustl.edu/law_lawreview/vol78/iss1/2]

Marsh, David and J.C. Sharman. 2009. "Policy Diffusion and Policy Transfer". *Policy Studies* 30(3). pp. 269-288. DOI: https://doi.org/10.1080/01442870902863851

Masilamani, Nitin and Anup Kuruvilla John. 2001. "The Future of State Sovereignty: Emerging Concerns in the Internet Era." *National Law School of India Review* 13(1), Article 6. pp. 226-239. Online. [accessed 20.10.2023

https://repository.nls.ac.in/cgi/viewcontent.cgi?article=1145&=&context=nlsir&=&sei-redir=1&referer=https%253A%252F%252Fscholar.google.com%252Fscholar%253Fstart%253D10%2526q%253Dinternet%252Bsovereignty%252Bindia%2526hl%253Den%2526as_sdt%253D0%252C5#search=%22internet%20sovereignty%20india%22]

McKune, Sarah and Ahmed, Shazeda. 2018. "The Contestation and Shaping of Cyber Norms Through China's Internet Sovereignty Agenda." *International Journal of Communication* 12. pp. 3835-3855. Online. [accessed 16.10.2023 https://ijoc.org/index.php/ijoc/article/view/8540]

McKune, Sarah. 2015. "An Analysis of the International Code of Conduct for Information Security". *Citizen Lab.* Online. [accessed 20.09.2023 https://citizenlab.ca/2015/09/international-code-of-conduct/]

McGlinchey, Eric and Erica Johnson. 2007. "Aiding the Internet in Central Asia", *Democratization.* 14(2). pp. 273-288. DOI: https://doi.org/10.1080/13510340701245785

Mejias, Ulises Ali. 2013. "Strategies for disrupting networks." In *Off the Network: Disrupting the Digital World*. pp. 81–94. Minnesota: University of Minnesota Press. https://doi.org/10.5749/j.ctt3fh6jh.9.

Melvin, Neil and Tolkun Umaraliev. 2011. "New Social Media and Conflict in Kyrgyzstan" *SIPRI Insights on Peace and Security.* 2011(1). pp. 1-23. Online. [accessed 30.10.2023 https://www.sipri.org/sites/default/files/files/insight/SIPRIInsight1101.pdf]

Michaelsen, Marcus and Marlies Glasius. 2018. "Authoritarian Practices in the Digital Age." *International Journal of Communication* 12(2018). pp. 3788-3794.

Ministry of Foreign Affairs of the People's Republic of China. 2007. *Joint Communique of Meeting of Heads of SCO Members.* Online. [accessed 19.09.2023 https://www.fmprc.gov.cn/eng/wjdt_665385/2649_665393/200708/t20070823_679182.html]

Mirza, Muhammad Nadeem, Lubna Abid Ali and Irfan Hasnain Qaisrani. 2021. "Conceptualising Cyber Sovereignty And Information Security: China's Image Of A Global Cyber Order." *Webology* 18 (5), pp.598-610.

Moerel, Lokke. 2021. "Reflections on Digital Sovereignty". *EU Cyberdirect*. Online. [accessed 22.10.2023 https://ssrn.com/abstract=3772777]

Moore, G.J. 2023. "Huawei, Cyber-Sovereignty and Liberal Norms: China's Challenge to the West/Democracies." *Journal of Chinese Political Science* 28. pp. 151–167 https://doi.org/10.1007/s11366-022-09814-2

Mueller, Milton. 2010. *Networks and States: The Global Politics of Internet Governance.* Cambridge MA: The MIT Press.

Mueller, Milton. 2017. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace.* Cambridge: Polity.

Nanni, Riccardo. 2022. *Rising China and Internet governance: Multistakeholderism, fragmentation and the Liberal Order in the age of digital sovereignty*, [Dissertation thesis]. DOI: 10.48676/unibo/amsdottorato/10371.

Newman, Nic, Richard Fletcher, Kirsten Eddy, Craig Robertson and Rasmus Nielsen. 2023. *Reuters Institute Digital News Report 2023.* London: Yougov. Online. [accessed 08.11.2023 https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf]

Nizamani, Usama and Afeera Firdous. 2020. "Rise of Digital Sovereignty". *Center for International Strategic Studies.* Online. [accessed 31.10.2023 https://ciss.org.pk/rise-of-digital-sovereignty/]

Nocetti, Julien. 2015. "Contest and conquest: Russia and global internet governance." *International Affairs* 91(1). pp. 111-130. DOI: https://doi.org/10.1111/1468-2346.12189

Obydenkova, Anastassia and Alexander Libman. 2018. "Understanding Authoritarian Regionalism." *Journal of Democracy* 29(4). pp. 151-165.

Obydenkova, Anastassia V. and Alexander Libman. 2019. *Authoritarian Regionalism in the World of International Organizations: Global Perspective and the Eurasian Enigma.* Oxford: University of Oxford Press.

Oldberg, Ingmar. 2007. *The Shanghai Cooperation Organisation: Powerhouse or Paper Tiger?* Stockholm: Swedish Defence Research Agency. Online. [accessed 07.11.2023 https://foi.se/rest-api/report/FOI-R--2301--SE]

Olson, Mancur. 1993. "Dictatorship, Democracy, and Development." *The American Political Science Review*, 87(3), pp. 567–576. DOI: https://doi.org/10.2307/2938736

Omelicheva, Mariya Y. 2009. "Convergence of Counterterrorism Policies: A Case Study of Kyrgyzstan and Central Asia." *Studies in Conflict & Terrorism* 32 (10): 893-908. DOI: 10.1080/10576100903182518.

OVD Info. 2023. *Repressii v Rossii v 2022 godu.* Online. [accessed 08.11.2023 https://data.ovd.info/repressii-v-rossii-v-2022-godu#4]

Østbø, Jardar. 2021. "Hybrid surveillance capitalism: Sber's model for Russia's modernization." *Post-Soviet Affairs* 37(5). pp. 435-452. DOI: https://doi.org/10.1080/1060586X.2021.1966216

Pankaj, Jayant. 2016. "Mapping the Rising Internet Shutdowns in India since 2016". Online. [accessed 08.11.2023 https://thewire.in/government/mapping-the-rising-internet-shutdowns-in-india-since-2016]

Parasol, Max. 2018. "The impact of China's 2016 Cyber Security Law on foreign technology firms, and on China's big data and Smart City dreams". *Computer Law and Security Review* 34(1). pp. 67-81. DOI: https://doi.org/10.1016/j.clsr.2017.05.022

Peceny, M., Beer, C. C., & Sanchez-Terry, S. 2002. "Dictatorial peace?" *American Political Science Review*, 96(1), pp. 15-26. DOI: https://doi.org/10.1017/S0003055402004203

Pepinsky, Thomas. 2013. "The Institutional Turn in Comparative Authoritarianism". *British Journal of Political Science* 44(3). pp. 631-653. DOI: 10.1017/S0007123413000021

Perper, Rosie. "India blocks TikTok and dozens of other Chinese apps that the government says pose a security threat". *Business Insider.* Online. [accessed 20.11.2023 https://www.businessinsider.com/india-bans-tiktok-dozens-of-other-chinese-apps-security-concerns-2020-6]

Pevehouse, J. C. 2005. *Democracy from Above? Regional Organizations and Democratization.* New York: Cambridge University Press.

Pohle, J. 2020. "Digitale Souveränität." in T. Klenk, F. Nullmeier, & G. Wewer (Eds.), *Handbuch Digitalisierung in Staat und Verwaltung* (pp. 1–13) DOI: https://doi.org/10.1007/978-3-658-23669-4_21-1

Polatin-Reuben, Dana and Joss Wright. 2014. "An Internet with BRICS Characteristics: Data Sovereignty and the Balkanisation of the Internet". *4th USENIX Workshop on Free and Open Communication on the Internet.* Online. [accessed 20.10.2023 https://www.usenix.org/conference/foci14/workshop-program/presentation/polatin-reuben]

Prasad, Revati. 2022. "People as data, data as oil: the digital sovereignty of the Indian state" *Information, Communication & Society*, 25:6, 801-815, DOI: 10.1080/1369118X.2022.2056498

Pundir, Pallavi. 2023. “India cuts off internet to 27 million people to catch one man”. *Vice News.* Online. [accessed 20.11.2023 https://www.vice.com/en/article/ak3z4e/amritpal-singh-india-khalistan-sikh-punjab]

Putz, Catherine. 2022. “Uzbekistan Unblocks Twitter, TikTok Still Restricted”. *The Diplomat.* Online. [accessed https://thediplomat.com/2022/08/uzbekistan-unblocks-twitter-tiktok-still-restricted/]

Quingsheng, Meng. 2019. *SCO joint anti-cyber terrorism exercise held in Xiamen.* Online. [accessed 07.11.2023 https://www.meiyapico.com/sco-joint-anti-cyber-terrorism-exercise-held-in-xiamen-cgtn-by-meng-qingsheng_n9]

Rayman, Noah. 2014. “Putin: The Internet is a ‘CIA Project’”. *Time Online.* Online. [accessed 31.10.2023 https://time.com/75484/putin-the-internet-is-a-cia-project/]

Roberts, Huws, Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo and Luciano Floridi. 2021. “Safeguarding European Values with Digital Sovereignty: An Analysis of Statement and Policies”. *Internet Policy Review.* DOI: *http://dx.doi.org/10.2139/ssrn.3937345*

Rotar, Igor. 2005. *Kyrgyzstan: Wide-Ranging extremism law not seen as threat.* Oslo: Forum 18. Online. [accessed 08.11.2023 https://www.forum18.org/archive.php?article_id=673]

Russo, A., and E. Stoddard. 2018. “Why do authoritarian leaders do regionalism? Ontological security and Eurasian regional cooperation.” *The International Spectator*, 53(3). pp. 20-37.

Schedler, Thomas. 2009. “The New Institutionalism in the Study of Authoritarian Regimes”. *Totalitarismus und Demokratie.* 6(2). pp. 323-340. DOI: https://doi.org/10.13109/tode.2009.6.2.323

Schreier, Margrit. 2012. *Qualitative Content Analysis in Practice.* London: Sage Publications.

Segal, Adam. 2017. “Chinese Cyber Diplomacy in a New Era of Uncertainty” in *Aegis Paper Series No. 1703.* Hoover Institution Essay. Online. [accessed 16.10.2023 https://www.hoover.org/sites/default/files/research/docs/segal_chinese_cyber_diplomacy.pdf]

Shafiev, Abdulfattoh and Marintha Miles. 2015. “Friends, Foes, and Facebook: Blocking the Internet in Tajikistan” *Demokratizatsiya: The Journal of Post-Soviet Democratization.* 23(3). pp. 297-319.

Shafqat, Rameen. 2023. “China, Pakistan strengthen technological ties”. *The Diplomatic Insight”.* Online. [accessed 22.11.2023 https://thediplomaticinsight.com/china-pakistan-strengthen-technological-ties/]

Shahbaz, Adrian. 2018. “The Rise of Digital Authoritarianism”. *Freedom House: Freedom on the Net 2018.* Online. [accessed 15.10.2023 https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism]

Shahid, Nidaa. 2023. “From Keystrokes to Conflicts: Safeguarding Pakistan’s Cyber Sovereignty”. *Pakistan Politico.* Online. [accessed 31.10.2023 https://pakistanpolitico.com/keystrokes/]

Shane, Peter. 2004. *Democracy Online: The Prospects for Political Renewal through the Internet*. New York: Routledge. DOI: https://doi.org/10.4324/9780203485415

Shanghai Cooperation Organisation. 2001. *Shanghai Convention on Combating Terrorism, Separatism and Extremism 15.06.2001.* Online. [accessed 06.09.2023 https://www.refworld.org/docid/49f5d9f92.html]

Shanghai Cooperation Organisation. 2009. *Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organisation.* Ekaterinburg: June 16, 2009.

Shanghai Cooperation Organisation. 2020. *Moscow Declaration of the Council of Heads of State of the Shanghai Cooperation Organisation.* Online. [accessed 07.11.2023 http://eng.sectsco.org/news/20201110/690356.html]

Shanghai Cooperation Organisation. 2023a. *Statement of the Council of the Heads of State on Cooperation in Digital Transformation.* Online. [accessed 07.11.2023 https://www.mea.gov.in/bilateral-documents.htm?dtl/36752/Statement_of_the_Council_of_SCO_Heads_of_State_on_Cooperation_in_Digital_Transformation]

Shanghai Cooperation Organisation. 2023b. *New Delhi Declaration of the Council of Heads of State of Shanghai Cooperation Organisation.* Online. [accessed 08.11.2023 https://www.mea.gov.in/bilateral-documents.htm?dtl/36751/New_Delhi_Declaration_of_the_Council_of_Heads_of_State_of_Shanghai_Cooperation_Organization]

Shcherbovich, Andrey. 2021. “Data Protection and Cybersecurity Legislation of the Russian Federation in the Context of the “Sovereignization” of the Internet in Russia.” In: Belli Luca (ed.), *Cyber BRICS. Cybersecurity Regulations in the BRICS Countries*. Cham: Springer. DOI: https://doi.org/10.1007/978-3-030-56405-6

Sigley, Gary. 2007. “Chinese Govermentalities: Government, Governance and the Socialist Market Economy”. *Economy and Society* 35(4). pp. 487-508. DOI: 10.1080/03085140600960773

Singh, Karan Deep. 2021. “Twitter Blocks Accounts in India as Modi Pressures Social Media”. *New York Times Online.* [accessed 08.11.2023 https://web.archive.org/web/20230210143403/https://www.nytimes.com/2021/02/10/technology/india-twitter.html]

Software Freedom Law Center India. 2023. *India Shutdowns.* Online. [accessed 08.11.2023 https://internetshutdowns.in]

Soldatov, Andrei and Irina Borogan. 2015. *The Red Web: The Struggle Between Russia's Digital Dictators and the New Online Revolutionaries.* New York: Public Affairs.

Söderbaum, Frederik. 2004. *The Political Economy of Regionalism: The Case of Southern Africa.* London: Palgrave Macmillan. DOI: https://doi.org/10.1057/9780230513716

Stadnik, Ilona. 2021. “Control by infrastructure: Political ambitions meet technical implementations in RuNet.” *First Monday* 26 (5). Online. [accessed 16.10.2023. https://journals.uic.edu/ojs/index.php/fm/article/download/11693/10124]

Stone, Richard. 2023. “Iran’s researchers increasingly isolated as government prepares to wall off internet”. *Science.org.* Online. [accessed 30.11.2023 https://www.science.org/content/article/iran-s-researchers-increasingly-isolated-government-prepares-wall-internet]

Strang, David. 1991. “Adding Social Structure to Diffusion Models: An Event History Framework.” *Sociological Methods & Research*, 19(3). pp. 324-353. DOI: https://doi.org/10.1177/0049124191019003003

Stroehlein, Andrew. 2008. “Internet Censorship in Uzbekistan.” *International Crisis Group.* Online. [accessed 30.10.2023 https://www.crisisgroup.org/europe-central-asia/central-asia/uzbekistan/internet-censorship-uzbekistan]

Syosev, Evgeny. 2017. *Statement at the OSCE Forum for Security Cooperation Hofburg, Vienna.* Online. [accessed 07.11.2023 https://www.osce.org/files/f/documents/3/e/316901.pdf]

Tashkinbayev, Renat. 2011. “President Nazarbayev proposed cyber police against Internet aggression”. *Tengri News Kz.* Online. [accessed 27.10.2023 https://en.tengrinews.kz/kazakhstan_news/president-nazarbayev-proposed-cyber-police-against-internet-2547/]

Taye, Berhan and Sage Cheng. 2023. “Report: the state of internet shutdowns”. *Access Now.* Online. [accessed 07.11.2023 https://www.accessnow.org/the-state-of-internet-shutdowns-in-2018/]

Tolstrup, J. 2015. “Black knights and elections in authoritarian regimes: why and how Russia supports authoritarian incumbents in post-Soviet states”. *European Journal of Political Research* 54, pp. 673–690.

United Nations General Assembly. 1999. *Resolution Adopted by the General Assembly. 530/70: Developments in the Field of Information and Telecommunications in the Context of International Security. A/RES/53/70.* Fifty Third Session Agenda Item 63. Online. [accessed 16.10.2023 https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F53%2F70&Language=E&DeviceType=Desktop&LangRequested=False]

United Nations General Assembly. 2011. “Letter dated 12 September 2011 from the Permanent Representatives of China, the Russian Federation, Tajikistan and Uzbekistan to the United Nations addressed to the Secretary-General”. *Developments in the field of information and telecommunications in the context of international security: A/66/358.* ”. Sixty-sixth session Agenda Item 93. Online. [accessed 16.10.2023 https://digitallibrary.un.org/record/710973?ln=en]

Van der Spuy, Anri. 2017. *What if we all governed the internet? Advancing Multistakeholder participation in Internet Governance.* Paris: UNESCO. Online. [accessed 19.10.2023 https://unesdoc.unesco.org/ark:/48223/pf0000259717]

Vardanyan, Lusine, Hovsep Kocharyan, Ondrej Hamul’ak and Tanel Kerikmae. 2023. “Digital Sovereignty in the EU: Searching for Legal Mechanisms for Marking the Borders”. *Digital Development of the European Union.* pp. 219-234. DOI: https://doi.org/10.1007/978-3-031-27312-4_14

von Soest, Christian. 2015. “Democracy Prevention: The International Collaboration of Authoritarian Regimes.” *European Journal of Political Research* 54 (4): 623–638.

Wagner, Benjamin. 2018. “Understanding Internet Shutdowns: A Case Study from Pakistan”. *International Journal of Communications* 12 (1). pp. 3917-3938. Online. [accessed 20.10.2023 https://ijoc.org/index.php/ijoc/article/view/8545]

Wang et al., "A Study of the Human Flesh Search Engine: Crowd-Powered Expansion of Online Knowledge," in *Computer*, 43 (8). pp. 45-53 DOI: 10.1109/MC.2010.216.

Wark, McKenzie. 1993. “Lost in space: Into the digital image labyrinth.” *Continuum*. 7(1). pp. 140-160. DOI: 10.1080/10304319309365594

Weber, V. 2021. “The Diffusion of Cyber Norms: Technospheres, Sovereignty, and Power.” PhD thesis, University of Oxford. Online. [accessed 16.10.2023 https://ethos.bl.uk/OrderDetails.do?uin=uk.bl.ethos.847370]

Weyland, K. 2019. *Revolution and Reaction: The Diffusion of Authoritarianism in Latin America.* Cambridge: Cambridge University Press.

Wilhelm, Dr. R. (Ed.). 1921. *Chinese Fairy Book*. New York: Frederick A. Stokes Company.

Wood, Peter. 2015. “China Conducts Anti-Terror Cyber Operations with SCO Partners”. *China Brief Volume XV (20).* Online. [accessed 20.09.2023 https://jamestown.org/wp-content/uploads/2015/10/China_Brief_Vol_15_Issue_20_1.pdf]

World Internet Conference. 2014. *World Internet Confernce: Wuzhan Summit 2014*. Online [accessed 27.05.2023 https://www.wuzhenwic.org/n_6822.htm]

Wong, Edward. 2010. “After a Long Ban, Western China Is Back Online”. *New York Times May 14 2010.* Online. [accessed 08.11.2023 https://www.nytimes.com/2010/05/15/world/asia/15china.html]

Wong, Hayley. 2023. “China and Russia looking to expand Shanghai Cooperation Organisation as alternative to Western order, analysts say.” *South China Morning Post.* Online. [accessed https://www.scmp.com/news/china/diplomacy/article/3227063/china-and-russia-looking-expand-shanghai-cooperation-organisation-alternative-western-order]

Wu, T.S. 1997. “Cyberspace sovereignty? The Internet and the international system.” *Harvard Journal of Law & Technology,* 10(3). pp. 647–666.

Wuzhen Declaration. 2014. *World Internet Conference Draft Declaration.* Online. [accessed 08.11.2023 https://www.scribd.com/document/247566581/World-Internet-Conference-Draft-Declaration]

Xi, Jinping & Vladimir Vladimirovich Putin. 2016. *The Joint Statement Between the Presidents of the Peoples’ Republic of China and the Russian Federation on Cooperation in Information Space Development.* Online. [accessed 27.11.2023 https://www.chinadaily.com.cn/china/2016-06/26/content_25856778.htm]

Xinhua. 2017. *SCO Countries Hold Drill Targeting Cyber-terrorism.* Online. [accessed 27.11.2023 http://www.xinhuanet.com/english/2017-12/06/c_136806108.htm]

Xinhua. 2020. *Technology Transfer Centre Opens in China.* Online. [accessed 04.12.2023 http://www.xinhuanet.com/english/2020-12/11/c_139580339.htm]

Yang, Yi Edward. 2021. “China’s Strategic Narratives in Global Governance Reform under Xi Jinping.” *Journal of Contemporary China* 30 (128). pp. 299 313. DOI: 10.1080/10670564.2020.1790904

Yau, Niva. 2022. “Chinese Governance Export in Central Asia.” *Security and Human Rights* 32(1-4). pp. 28-40. DOI: https://doi.org/10.1163/18750230-bja10009

Yom, S. 2014. “Authoritarian monarchies as an epistemic community diffusion, repression, and survival during the Arab spring” *Taiwan Journal of Democracy*. 10. pp. 43–62

Zeng, Jinghan; Stevens, Tim; Chen, Yaru. 2017. “China´s Solution to Global Cyber Governance: Unpacking the Domestic Discourse of “Internet Sovereignty””. *Politics & Policy* 45 (3), pp. 432-464. DOI: https://doi.org/10.1111/polp.12202

Zhou, Zunyou. 2018. "‘Fighting Terrorism According to Law’: China’s Legal Efforts against Terrorism." In Michael Clarke (ed.), *Terrorism and Counter-Terrorism in China: Domestic and Foreign Policy Dimensions.* DOI: https://doi.org/10.1093/oso/9780190922610.003.0004 .

Ziegler, C. 2016. “Great powers, civil society and authoritarian diffusion in Central Asia.” *Central Asian Survey* 35, pp. 549–569.

Zittrain, Jonathon and Benjamin Edelman. 2003. *Empirical Analysis of Internet Filtering in China.* Harvard: Berkman Center for Internet & Society. Online. [accessed 07.11.2023 https://cyber.harvard.edu/filtering/china/]

Zuboff, Shoshana. 2018. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power.* London: Profile Books.

Appendices

Appendix A – Timeline of the Shanghai Cooperation Organisation’s Cyber Security Development

2001	- **15.06:** Founding of the SCO through the ratification of the “Shanghai Convention on Combating Terrorism, Separatism and Extremism”
2002	- **19.09:** Signing of the “Charter of the Shanghai Cooperation Organisation” establishing the bodies of the organisation
2003	- **29.03:** Shanghai Convention enters force establishing the organisation - **August:** First joint military exercises among SCO members

	- **19.09:** Charter of the Shanghai Cooperation Organisation enters force
2004	- **17.06:** Establishment of the Regional Anti-Terrorist Structure (RATS)
2005	- **August:** "Peace Mission 2005" Second Joint Military Exercises
2007	- **23.08:** "Action plan on ensuring international information security" signed by member states at Bishkek summit - **August:** "Peace Mission 2007" Joint Exercises in Central Russia
2009	- **16.06:** Signing of the "Agreement - on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization" in Ekaterinburg - **July:** "Peace Mission 2009" military exercises in Russian Far-East
2011	- **June:** Astana summit takes place with Nazarbayev calling for a focus on e-sovereignty - **14.09:** Members' proposal to the UN (A/66/359) calling for a new "International Code of Conduct for Information Security" based on SCO norms
2013	- **September:** SCO Establishes internet expert group as part of the 2013–2015 outline of SCO Cooperation and began to strengthen Internet counter-terrorism law enforcement.
2015	- **09.01:** SCO member states submit redraft (A/69/723) of the "International Code of Conduct for Information Security" to the UN - **10.04:** Draft Anti-Extremism Laws agreed by organisation in cooperation - **30.04:** China-Russian "Joint agreement on Cooperation on Cybersecurity" signed - **July:** India and Pakistan's accension to organisation ratified - **14.10:** Xiamen 2015 joint exercises on the use of the internet for terrorism, separatism and extremism
2017	- **09.06:** Ratification of the "Convention of the Shanghai Cooperation Organisation on Combating Extremism" - **09.06:** Indian and Pakistani accession to organisation - **December:** Second Anti-Cyberterrorism Drill
2019	- **December:** Third SCO Anti-Cyberterrorism drill held in Xiamen
2022	- **19.09:** Signing of the Samarkand Declaration of the Council of the Heads of State deepening internet sovereignty commitments
2023	- **13.05:** First meeting of the heads of ministries and agencies of SCO member states responsible for development of information and communication technology - **04.07:** Signing of the New Delhi declaration of the Council of the Heads of State of Shanghai Cooperation Organisation establishing register of banned organisations

Source: Own research using Aris, Stephen. (2013) *Shanghai Cooperation Organization: Mapping Multilateralism in Transition No.2.* International Peace Institute. Online. [accessed

21.09.2023 https://www.ipinst.org/wp-content/uploads/publications/ipi_e_pub_shanghai_cooperation.pdf]

Appendix B –Timeline of Access Control Laws

Pre-1990	**India:** **25.01:** Code of Criminal Procedure 1974: - Section 144: State actions are justified in order to maintain law and order (later used to implement internet shutdowns)
1992	**Kyrgyzstan:** **02.07:** Law of the Kyrgyz Republic No. 938XII "On Mass Media": - Article 13: Dissemination of Mass Media (later applied to the internet) only allowed with permission of authorities.
1994	**China:** **18.02:** Computer Information System Security Protection Regulations of the People's Republic of China (1994): - Article 16: State permit system for specialized computer information system security product sales.
1996	**China:** **23.01:** Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China - Article 7: State approval required for newly built connected networks. - Article 8: International connection only through established networks; Work groups need permission from competent authorities to establish a connection. **Pakistan:** **17.10:** Pakistan Telecommunications Act: - Section 5(2): State has the power to grant and suspend licences to telecommunications operators. - Section 54: Act allowing the state to implement internet shutdowns in times of a national or regional emergency.
1997	**China:** **11.12:** Computer Information Network and Internet Security, Protection and Management Regulations:

	- Article 6: No-one may use computer networks or network resources without getting proper prior approval. No-one may without prior permission may change network functions or to add or delete information. No-one may without prior permission add to, delete, or alter materials stored, processed or being transmitted through the network. (5) Other activities which harm the network are also prohibited. **Uzbekistan:** **26.12:** Law of the Republic of Uzbekistan No. 541-I: - Article 15: Registering with State required for opening Mass Media outlet; applies to online also.
1999	**Uzbekistan:** **20.08:** Law of Republic of Uzbekistan No. 822-1: - Article 18: In the case of the use of telecommunication networks or means for criminal purposes detrimental to the interests of the individual, society and the state, the operation of such networks or means of telecommunications shall be suspended.
2000	**China:** **25.09:** Internet Information Service Management Measures Law No. 292: - Article 4: State licensing system for commercial Internet information services; and implements a filing system for non-commercial Internet information services. No licence no right to provide services. - Article 5: Those engaging in Internet information services, must undergo examination, verification and approval by the relevant controlling department to get a licence to provide online services. - Article 10: State list of names of Internet information service providers having obtained business permits or having completed filing formalities. - Article 17: Commercial Internet information service providers applying to go on the market at home or abroad or to establish joint ventures or cooperation with foreign businesses, shall undergo examination and agreement by the State Council information industry controlling department in advance; in particular, the proportion of foreign business investment shall conform to the provisions of relevant laws and administrative regulations.
2002	**Pakistan:** Pakistan Electronic Media Regulatory Ordinance 2002: - Section 30: Power of the State to suspend licencing for electronic media providers. - Section 34: Licencing restrictions for electronic media providers.

	- **Russia:** **25.07:** Federal Law No. 114 FZ "On Countering Extremist Activity": - Article 10: All activities of associations found to be extremist banned, including using mass media, and online resources. - Article 12: General use of networks for "extremist activity" is banned. **Tajikistan:** **10.05:** Law of the Republic of Tajikistan No. 55 "About Information": - Article 43: Information sovereignty to be protected through exclusive right of the State to information resources paid for by budget; and regimes of access control. **10.05:** Constitutional Law of the Republic of Tajikistan "On the Legal Regime of the State of Emergency": - Article 4 (14): The authorities can seize control of the internet in a state of emergency and control actions of the media. **Uzbekistan:** **30.08:** Law of the Republic of Uzbekistan No. 405-II: - Article 11: Companies with over 30% foreign ownership restricted from opening Uzbek media companies (including online).
2003	**Russia:** **18.06:** Federal Law No. 126 FZ "On Communications": - Article 29: Business licences introduced for communications and network providers. - Article 64 (3): Investigative or security authorities can limit communications services access to legal and natural persons based on a written decision. - Article 66: Internet shutdowns legalised for emergency situations **Tajikistan:** **08.12:** Law of the Republic of Tajikistan No. 69 "On the Fight Against Extremism": - Article 13: Suspension of activities of banned organisations including the publishing of materials online.
2005	**Kyrgyzstan:**

	17.08: Law of the Kyrgyz Republic No. 150 “On Countering Extremist Activity”: - Article 10: Organisations suspected of extremism suspended access to the internet whilst case is being heard; full restrictions possible if found guilty.
2006	**India:** **01.11:** Department of Telecommunications Order: SIM Card providers to verify identity of users before purchase
2007	**Uzbekistan:** **27.11:** Law of the Republic of Uzbekistan No. 1743 “On Communications”: - Article 19: Emergency situations to allow internet shutdowns.
2012	**Kazakhstan:** **18.01:** Law of the Republic of Kazakhstan No. 546-IV: - Article 3: Online activities of organisations suspended, who break content control laws. **Russia:** **28.07:** Federal Law No. 139-FZ: - Article 15.1(1): Unified register of banned websites created to restrict access.
2013	**Kazakhstan:** **03.07:** Law of the Republic of Kazakhstan No. 121-V: - Article 14(1): Internet shutdowns allowed in emergency situations. **Kyrgyzstan:** **11.06:** Law of the Kyrgyz Republic No. 129 - Article 21-1(5): The commencement and suspension of a connection of customers of operators takes place only with the approval of the national security body.
2014	**Kazakhstan:** **23.04:** Law of the Republic of Kazakhstan No. 128-VI; amending 'On Informatization': - Article 66. 3) Foreign online platform or instant messaging service with over one hundred thousand users must appoint a legal representative for interaction for authorised bodies; if not access restricted.

	Russia: **05.05:** Federal Law No. 97 FZ: - Article 15.4 (2): ISPs to limit access to computers of organisations to internet for not complying with content control requirements.
2015	**Kazakhstan:** **24.11:** Law of the Republic of Kazakhstan No. 419-V: - Article 15.1(1): Law enforcement and internal affairs given powers to use signal blocking technologies to protect institutions of penal enforcement. **Tajikistan:** **25.12:** Law of the Republic of Tajikistan No. 1271: - Article 6: State to control who has access to network infrastructure in the country.
2016	**Kazakhstan:** **22.12:** Law of the Republic of Kazakhstan No. 28-VI: - Article 41 (1-2): State ordered internet shutdowns legalised for emergency situations. **28.12:** Law of the Republic of Kazakhstan No. 36-VI: - Article 6: Cellular network operators to suspend users access on request of registration body.
2017	**China:** **01.06:** Cybersecurity Law of the People's Republic of China: - Article 24: Users to provide real identity information to gain provision of services to use the internet. - Article 58: National security and the social public order legal reasons for internet shutdowns. **India:** **07.08:** Temporary Suspension of Telecom Services (Public Emergency or Public Safety) Rules: - Rules establish the ability of Regional and Central Government to suspend access to networks in emergency situations. **Russia:**

	21.07: Federal Law No. 276-FZ "On Amendments to the Federal Law "On Information Technologies and Information Protection": - Article 15.8(1): Network, website, information system owners restricted from providing access to websites and information about these resources. - 15.8(12): Telecom operators providing services for providing access to the Internet are obliged to restrict access to the relevant software and hardware for access to information resources, information and telecommunication networks, access to which is restricted.Article **29.07:** Federal Law No. 241 FZ "On Amending Articles 10.1 and 15.4 of the Federal Law "On Information, Information Technologies and Information Protection": - Article 1 (4.2.2): Website owners legally required to ban users who have published public or private messages containing illegal information. - Article 10.1: Anonymous use of website messaging services restricted.
2019	**India:** **18.09:** Press Note No. 4 Amending FDI Policy: - Foreign investors are allowed to own up to 26% of a digital media company; companies above this limit to divest shares to reduce down to this limit. **Russia:** **01.05:** Federal Law No. 90 FZ 74. "On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection": - Article 562 (4): Owners or other owners of traffic exchange points shall not have the right to connect without installing equipment for operational search and restricting information. **Uzbekistan:** **16.04:** Law of the Republic of Uzbekistan No. ZRU-547: - Article 20: An application for registration of a personal data base in the State Register of Personal Data Bases shall be submitted to the authorized state body.
2020	**Tajikistan:** **02.01:** Law of the Republic of Tajikistan No. 1655 "On Countering Extremism":

	- Article 11(11): Communications service gains power to suspend activities of networks if extremism suspected; Suspend telecoms services of any kind in an emergency situation; forces telecoms companies to store users data for 6 months in the case of expected extremism.
2021	**Russia:** **01.07:** Federal Law No. 236 FZ: - Article 5(2) & (8): Foreign companies to register with Roskomnadzor before providing internet services for Russian citizens (or just in Russian) and must open a branch in Russia. **Uzbekistan:** **04.03:** Law of the Republic of Uzbekistan No. 3RU-679: - Article 121: State authorities to restrict access to sites not complying with content control laws.
2022	**China:** **16.11:** Provision on the Management of Internet Comment Post Services (2022): - Article 8: Social credit score designates the level of access to Social Media.
2023	**Kyrgyzstan:** **24.02:** Law of the Kyrgyz Republic No. 40 "On Countering Extremist Activity": - Article 12: Restriction on the use of telecoms networks for extremism, extremists access controlled. - Article 14(4): Termination of activities of organisations allowed if found to be extremist by a court.

Appendix C –Timeline of Content Control Laws

Pre-1990	**Pakistan**: Criminal Law (Amendment) Act, IV of 1986. - Sections 499, 500: Defamation laws also applied to online space Penal Code (Amendment) Act, 1870 (XXVII of 1870): - Section 124a: Sedition law also applied to online space. Pakistan Penal Code 1860

	- Section 505: Public mischief also applied to online space **India:** Indian Penal Code (Amendment) Act, 1870 (XXVII of 1870): - Section 124a: Sedition law also possible to apply to online space; 2023 high court suspends section. - Section 499, 500: Criminalising defamation. Code of Criminal Procedure (1973): - Section 119: Defamation as criminal offence.
1991	**Pakistan:** Code of Criminal Procedure 1898 (as amended 1991) - Section 295(c): Law against blasphemy, also applied to online space.
1992	**Kyrgyzstan:** **02.07:** Law of the Kyrgyz Republic No. 938-XII "On Mass Media": - Article 13: Permission required to disseminate information in the mass media. - Article 23: Banned information includes: state secrets, violent change of constitution, violation of sovereignty and territorial integrity, propaganda of war, violence, drugs, and cruelty; national religious exclusivity, intolerance, insulting civil honour, insulting religious feelings, pornography and soliciting of sex.
1996	**China:** **23.01:** Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China: - Article 13: Against the dissemination of information: impeding social order, state secrets, obscene, sexual, or other such information. **Pakistan:** **17.10:** Pakistan Telecommunications (re-organisation) Act - Article 19: Content control for religion and national security.
1997	**China:** **11.12:** Computer Information Network and Internet Security, Protection and Management Regulations:

	- Article 5: inciting: resist constitution, overthrow of government or socialism, hatred among nationalities, separatism, falsehood, feudal superstitions, sexually explicit, gambling, violence, terrorism, slander, reputation of the State, other information against laws. - Article 10: work groups to remove information based on art. 5. - Article 14: approval of chief administration required for information dissemination. - Article 18: Removal of content under art. 5 through Public Security Management and Supervision Organisation - Article 21: Access restricted for businesses if found in contempt of art. 5. **Pakistan:** Code of Criminal Procedure 1898 (as amended Act 2 of 1997) - Section 99: Restrict information prejudicial to broad national interest.
2000	**China:** **01.10:** Internet Information Service Management Measures Act: - Article 15: ISPs banned from disseminating information: opposing constitution, divulging state secrets, endangering national security, subverting state, harming national honour, inciting ethnic hatred, destroying state religious policies, propagating feudal superstitions, disordering social order, disseminating rumours, disseminating obscenity, sex, gambling, violence, slander, insults, national unity, defamation. **India:** **09.06:** The Information Technology Act No. 21: - 66(a): Criminalises information causing annoyance, inconvenience or danger. - 69(a): Information access can be restricted: to protect sovereignty or integrity of India, the security of the State, friendly relations with foreign Stales or public order or for preventing incitement to the commission of any cognizable offence, for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource. **Russia:** **09.09:** Doctrine of Information Security: - Calls for the creation of legal mechanisms to protect Russian sovereign information space; to ensure preservation of the cultural and historical values of the peoples and nationalities of the Russian Federation and

	rational utilization of the information resources amassed by society that constitute national property. - Recognises foreign threats in an information war which utilises "false information".
2002	**Uzbekistan:** **30.08:** Law of the Republic of Uzbekistan No. 405-II: - Article 6: law against disseminating information: violent change in constitutional order, calling for territorial change, propaganda of violence, national/racial hatred, state secrets, endangering national security; defamation, information on ongoing investigations. **Pakistan:** **01.10:** Defamation Ordinance 2002: Strict anti-defamation law. **Russia:** **25.07:** Federal Law No. 112 FZ (amending Federal Law 2124-1 "On Mass Media" (1991)): - No provision shall be made for the use of mass media for purposes of committing criminally indictable deeds, divulging information making up a state secret or any other law-protective secret, the performance of extremist activities, and also for the spreading of broadcasts propagandizing pornography or the cult of violence and cruelty. **25.07:** Federal Law No. 114 FZ "On Countering Extremist Activity": - Articles 1, 8, 13: Establish illegality of disseminating "extremist materials" including: violent change to constitution; undermining integrity/security; incitation of social, racial, national or religious animosity; insult national dignity; mass disorder/hooliganism motivated by ideological, political, racial, nationalistic, religious hatred; Nazi propaganda.
2003	**Tajikistan:** **08.12:** Law of the Republic of Tajikistan No. 69 "On Countering Extremism" - Article 9: Against the dissemination of extremist materials. - Article 15: Against using internet for extremism. - Article 16: Against dissemination and storage extremist information.
2005	**Kazakhstan:** **08.02:** Law of the Republic of Kazakhstan No. 31-III "On Countering Terrorism": - Article 1, 12: Establishing extremist materials and criminalisation of their publication: forcible change to constitution; violation of

	sovereignty/territory; undermining national security; incitement of social discord (political extremism); incitement to racial, national, tribal discord; incitement of religious enmity/discord.
2006	**Russia:** **14.07:** Federal Law No. 149-FZ "On Information, Informational Technologies and the Protection of Information: - Article 9: Restricted access to information can be introduced to protect the basic foundations of the constitutional system, morality, health, rights and legitimate interests of other persons, ensuring the defences of the country and security of the state. - Article 10: It is prohibited to disseminate information which is aimed at the propaganda of war, inciting national, racial or religious hatred and hostility and also other information the dissemination of which is subject to criminal or administrative responsibility.
2009	**Kazakhstan:** **10.07:** Law of the Republic of Kazakhstan No. 178-IV: - Article 4: dissemination of information: violent change of constitutional order, violation of territorial integrity, undermining security, propaganda of extremism or terrorism, information on interethnic or interfaith hatred. **India:** **27.10:** Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009: - Sections 7 & 8: Establish process for requesting the blocking of information according to section 69a of the IT Act (2000) - Section 9: Allows interim blocking of access to information resources from the Central Government without a hearing in an emergency situation.
2010	**China:** **08.06:** On the Internet in China (White Paper) - 2 paragraphs against dissemination of information in line with 3 evils. - prohibit the spread of information that contains contents subverting state power, undermining national unity, infringing upon national honour and interests, inciting ethnic hatred and secession, advocating heresy, pornography, violence, terror and other information that infringes upon the legitimate rights and interests of others.
2012	**Kazakhstan:** **27.04:** Law of the Republic of Kazakhstan No. 15-V

	- Article 36 (1-3) : ISPs to block information covered by court order requested by security services. **Russia:** **28:07:** Federal Law No. 139 FZ; amending Federal Law 126-FZ of 07.07.2003: - Article 2 (5): Telecoms operators to block information in accordance with 149-FZ of 2006 (blacklist law creating a register of blocked sites). **Tajikistan:** **03.07:** Law of the Republic of Tajikistan No. 848: - Article 37: Law against internet for spreading information: against constitutional order and state security, against information security, inciting of racial/ethnic hatred, localism, religious or linguistic discord, information calling for violence, extremism, terrorism, social enmity, separatism, encroachment on the person, human and civil rights and freedoms, propaganda and advertising of an immoral and immoral lifestyle (pornography). - Article 38: Against defamation, falsehood.
2013	**Russia:** **26.06:** Federal Law No. 136 FZ; amending Article 148 of the Criminal Code of the Russian Federation and Certain Legislative Acts of the Russian Federation in order to Counteract the Insult of Religious Beliefs and Feelings of Citizens: - Article 148 (1): Against information insulting religious feelings. **29.06:** Federal Law No. 135 FZ: amending Federal Law 124 FZ 1998: - Article 14 (1): Against information promoting non-traditional sexual relations (gay propaganda). **25.12:** Federal Law No. 398 FZ: amending Federal Law 149-FZ of July 27, 2006: - Article 15.3 (1): Against disseminating information calling for mass demonstrations, protests, extremism.
2014	**Kazakhstan:** **23.04:** Law of the Republic of Kazakhstan No. 200-V - Article 41-1 (3 (1)): against information: violates the legislation on elections, containing calls for extremism/terrorism, riots, mass (public)

	events, promoting sexual exploitation of minors and child pornography, cyberbullying against a child, advertising of gambling.
2015	**China:** **27.12:** Counter-Terrorism Law of the People's Republic of China - Article 19: Telecommunications operators and internet service providers to automate content detection to remove extremist content in accordance with other laws of PRC. **Kazakhstan:** **24.11:** Law of the Republic of Kazakhstan No. 418-V 3PK - Article 17 (3): Authorised body to restrict access to online resources. - Article 35 (7): Authorized bodies, owners, and holders to restrict information according to court order requested by security services. **Pakistan:** **11.12:** Telecommunications Policy 2015 - 9.8.3: Pakistan Telecommunication Authority (PTA) to manage content according to Islamic rules.
2016	**China:** **07.11:** Cybersecurity Law of the People's Republic of China: - Article 12: banning information: subverting national sovereignty, overturning the socialist system, inciting separatism, breaking national unity, advocating terrorism or extremism, advocating ethnic hatred /discrimination, disseminate violent, obscene, or sexual information, create or disseminate false information to disrupt the economic or social order, or information that infringes on the reputation, privacy, intellectual property or other lawful rights and interests of others, and other such acts. - Article 47: Network operators to block information according to art. 12. - Article 50: State cybersecurity and informatisation depts. to also restrict access to content. **Russia:** **23.06:** Federal Law 208 FZ: amending Federal Law 149-FZ (2006); - Article 10.4 (1): Restrictions on disseminating information on sites with more than 1,000,000 users with terrorism, extremism, pornography, obscene language.

	- Article 10.4 (4): Restriction on defamation. - Article 10.4 (8): False information. **05.12:** Doctrine of Information Security of the Russian Federation - Part IV; 23: Against use of internet promote extremist ideology, spread xenophobia, national exceptionalism for the purposes of undermining the sovereignty, political and social stability, forcible changing the constitutional order and violating the territorial integrity. - Part IV; 34c: Restrictions of information in favour of national security. **Pakistan:** **11.08:** Prevention of Electronic Crimes Act - Section 9: Against glorification of an offence. - Section 10: Against disseminating terrorist information. - Section 11: Against hate speech
2017	**Kazakhstan:** **28.12:** Law of the Republic of Kazakhstan 128-VI; amending Law of the Republic of Kazakhstan 451-1 "On Mass Media" (1999) - Article 1 (3): Against dissemination of information on terrorism, drugs, extremism, violence and pornography - Article 17 (2.3): Duty of informatization owner to restrict or prohibit access to electronic information sources, infrastructure. - Article 18-2(6): Binding foreign companies to also restrict access to information in Kazakhstan. **Russia:** **29.07:** Federal Law No. 276 FZ; amending Federal Law No. 149 FZ (2006) - Article 15.8 (6): Prohibits references to banned websites; VPN services restricted also from accessing banned websites. - Network and website owners to restrict access to "resources with restricted access" listed by Roskomnadzor. **25.11:** Federal Law No. 327 FZ: - Article 1 (2b): Restricting posting in violation of the law. - Article 2: Foreign agents' law restricting actions of people legally recognised as agents, including removing or otherwise limiting their online content
2019	**Russia:**

	18.03: Federal Law No. 30 FZ; amending Federal Law No. 149 FZ (2006); - Article 151 (1): Restricting access to information offending human dignity, public morality, disrespecting society, the state, official symbols, or state bodies. **18.03:** Federal Law No. 31 FZ; amending Article 15.3 of Federal Law "On Information, Information Technologies and Information Protection" (2006): - Part 1: unreliable information disseminated as a threat to life, property, mass violation of public order, public safety. - Part 14: requiring telecom operators to restrict access to this information. **02.12:** Federal Law No. 426 FZ; - Article 2 (amending 149 FZ article 10 (7)) : Requirement for foreign agent warning.
2020	**Russia:** **30.12:** Federal Law No. 482 FZ: - Article 3.3 (1) (amending 272 FZ (2012)): Roskomnadzor can use its own measures to restrict access to prohibited content. - Article 3.3 (6) (amending 272 FZ (2012)) **30.12:** Federal Law No. 530 FZ; amending 149 FZ (2006): - Article 10.6 (1) : Social networks (including foreign sites required to remove banned content) - Article 10.6 (2) : Defamation also applies to social networks **30.12:** Federal Law No. 538 FZ; amending Criminal Code of the Russian Federation: - Article 128.1 (2) : Jail term for defamation. **Tajikistan:** **02.01:** Law of the Republic of Tajikistan “On Countering Extremism” No. 1655: - Article 3: Recognises the dissemination of a wide amount of ‘extremist’ items as illegal, and specific publication in the internet: violent overthrow or change of constitution, violation of sovereignty, independence; incitement of racial, national, regional, religious and social hatred; propaganda of exclusivity, superiority of citizens on the basis of their religious, confessional, linguistic, national, racial or regional affiliation, actions aimed at undermining security; humiliation of national dignity; - Article 4: Propaganda to be used to counter extremism.

	- Article 11 (2): Ministry of internal affairs given powers to propagandise against extremism. - Article 16: Prohibited to publish or store extremist materials in Tajikistan. - Article 17: Communications service to limit access to extremist materials or materials calling for mass protest. - Article 19: Authorized state body can decide what is 'extremist' material.
2021	**Russia:** **01.07:** Federal Law No. 236 FZ: - Article 7: Foreign legal entities with more than 500 000 users in Russia required to have a representative office in Russia to handle content control. **Uzbekistan:** **04.03:** Law of the Republic of Uzbekistan No. 3RU-679: - Article 121: Requirement of bloggers and owners of websites to remove unreliable information. **Pakistan:** **12.10:** Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguard) Rules - Section 1: Establishes Social Media companies as licensees. - Section 3: Blocking of content against Islamic principles, public morality, decency, integrity of Pakistan - Section 7: Social media are to introduce measures to restrict access to information including closing live streams. **25.09:** *Proposed* Criminal Law Reforms 2021 of the Pakistan Penal Code 1860 - Section 500: Discreditation of Pakistani army banned. **India:** **25.02:** Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021: - Section 16: Allows for blocking of content under section 69(a) of the IT Act (2000) without receiving a court order in an emergency situation. - Part II. Section 3 (1d): Court order or government agency can force internet intermediaries to restrict content access to information: in the

	interest of sovereignty; security of the state; relations with other states; public order, decency and morality; defamation; incitement. **Kyrgyzstan:** **23.08:** Law of the Kyrgyz Republic No. 101 "On Protection from False and Inaccurate Information": - Article 3: state authorised body given powers to delete information flagged as fakes without a court order
2022	**China:** **16.11:** Management of Internet Comment Post Services: - Article 4: Post comment providers to remove unlawful comments in real time, prior review of news published, R&D for comment management. - Article 9: Users to carry forwards Core Socialist Values, not publish banned information. - Article 10: Report and address illegal and negative comments. **Kazakhstan:** **03.05:** Law of the Republic of Kazakhstan No. 118-VII; amending Law on "Informatization": - Article 18-2 (6): legal representatives of foreign online platform providers to ensure compliance with content controls. **Russia:** **04.03:** Federal Law No. 31 FZ: amendments to the Code of Administrative Offences: - Article 20.3.3 (1): Discreditation of the Russian army - Article 20.3.3 (2): Block calling for protests. - Article 20.3.4: Block calls for sanctions. **04.03:** Federal No. 32 FZ: amendments to the Criminal Code of the Russian Federation: - Article 207.3 (1): Law about fakes of the Russian armed forces.

Appendix D – Timeline of Data Control Laws

1994	**China:** **18.02:** Computer Information System Security Protection Regulations of the People's Republic of China - Article 11: When implementing computer information systems' international networking, the work unit using computer information systems reports to the provincial-level or higher People's Government public security organ for filing. -
1997	**China:** **30.12:** Computer Information Network and Internet Security, Protection and Management Regulations - Article 10: Connecting network units, entry point units and corporations that use computer information networks and the Internet and other organizations must assume the following responsibilities for network security and protection: ; - (5) Establish a system for registering the users of electronic bulletin board systems on the computer information network as well as a system for managing bulletin board information; - Article 16: The Public Security organization computer management and supervision organization should have information on the connecting network units, entry point unit, and users, establish a filing system for this information, maintain statistical information on these files and report to higher level units as appropriate.
1999	**Uzbekistan:** **20.08:** Law of the Republic of Uzbekistan No. 822-I: - Article 15. Secrecy of telephone conversations, telegraph and other messages transmitted over telecommunications networks - Wiretapping of telephone conversations, familiarization with messages transmitted over telecommunications networks, obtaining information about them, as well as other restrictions on the secrecy of conversations and messages are allowed only in cases and in the manner prescribed by law. - Article 18. Operators and providers operating in the territory of the Republic of Uzbekistan are obliged to ensure, at their own expense, the installation and operation of equipment used to conduct operational-search activities on telecommunications networks by bodies engaged in operational-investigative activities, as well as to provide measures to prevent the disclosure of organizational and tactical methods of carrying out these activities.
2000	**China:** **25.09:** Internet Information Service Management Measures

	- Article 14: Internet information service providers engaging in news, publishing as well as electronic advertising and other service programmes shall record the content and the publishing time of provided information, the Internet address or domain; Internet access service providers shall record the online time, user account, Internet address or domain, main telephone number and other information of online users. - Internet information service providers and internet access service providers' back-up records shall be preserved for 60 days, and is to be provided when relevant State organs enquire about it according to the law. **India:** **09.06:** Information Technology Act 2000: - Section 69: Allows surveillance for the investigation of any offence. **Russia:** **25.07:** Order 130 of the Russian Federation - Install SORM Into networks; in agreement with the law 144-FZ 1995 and 40-FZ 1995
2002	**Tajikistan:** **10.05:** Law of the Republic of Tajikistan "On Communications" - Article 9 - draws up and monitors the implementation of the national communication numbering plan of the Republic of Tajikistan (including long-distance and international codes), ensures the effective use of numbers, as well as the allocation of numbers or ranges of numbers to telecommunications operators
2003	**Russia:** **07.07:** Federal Law No. 126-FZ "On Communications": - Article 64. 1. Communications operators are obliged to supply to the authorized state bodies performing operational-search activity or ensuring the security of the Russian Federation, information on the users of communications services and the communications services rendered to them, as well as other information necessary for carrying out the tasks imposed upon these bodies, in the cases established in federal laws.
2006	**Russia:** **17.07:** Federal Law No. 152 FZ - Article 12. The Transborder Personal Data Flow 1. The transborder flow of personal data to the territories of the foreign states being a party to the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data and also of the other foreign states that ensure adequate protection in respect

	of the rights of personal data subjects shall take place in accordance with this Federal Law and it may be prohibited or restricted for the purposes of protecting the foundation of the constitutional system of the Russian Federation, the morals, health, rights and lawful interests of citizens and safeguarding national defence and state security. **14.07:** Federal Law No. 149 FZ - 4. Federal laws may provide for the obligatory identification of personality, organisations using an information-telecommunications network when conducting entrepreneurial activity. Notably, the recipient of an electronic message located on the territory of the Russian Federation shall have the right to conduct a check-up making it possible to identify the sender of an electronic message and in instances specified by federal laws or agreement of the parties, it shall be obligated to conduct such a check-up.
2010	**Pakistan:** **15.03:** Monitoring and Reconciliation Telephony Traffic Regulations - Regulation 4: PTA to install web monitoring system
2012	**Tajikistan:** **03.07:** Law of the Republic of Tajikistan No. 848 - Article 35 Information as a commodity Information products and information services of citizens and legal entities of individuals and legal entities engaged in information activities may be objects of commodity relations, which are regulated by the current legislation of the Republic of Tajikistan. (ZRT of 3.07.12, No. 848)
2013	**Kazakhstan:** **21.05:** Law of the Republic of Kazakhstan 21.05.2013 No. 94-V: as amended: 2012, 2013, 2014, 2015, 2016,2017,2020,2022 - 5) ensuring the formation, operation, maintenance and development of a database of identification codes of subscriber devices of cellular communication and a centralized database of subscriber numbers, providing access to them; **Kyrgyzstan:** **11.06:** Law of the Kyrgyz Republic No. 129 - Article 21-1: 1. Communications operators shall be obliged to provide the investigator with information on users of communication services, as well as other information necessary for the performance of the tasks assigned to these bodies, when conducting special investigative actions and authorized state bodies carrying out counterintelligence activities in communication networks, to provide them with organizational and software and technical capabilities for conducting special investigative

	actions and counterintelligence measures in all networks and on communication channels, access to databases, automated systems of the telecom operator in cases established by the legislation of the Kyrgyz Republic. - **(**4) 4. Technical requirements for communication networks, special technical means designed to control and record legally obtained information/information transmitted through technical communication channels, the procedure for interaction in the implementation of the functions of the system of special investigative actions and counterintelligence measures in communication networks, including the development of the interface (technical regulations), the development of the necessary software, the solution of the issue of connection and access channels, other issues related to ensuring the legality of the implementation of special investigative actions and counterintelligence measures in communication networks, a comprehensive solution to all issues and problems related to the implementation and operation of a system of special investigative actions and counterintelligence measures in communication networks, in accordance with international recommendations and technical concepts developed in this area, as well as the requirements of the current legislation of the Kyrgyz Republic The Republics shall be established by the Government of the Kyrgyz Republic. - Article 24-1. Telecom operator's databases about subscribers 1. A communications operator shall create databases on subscribers and communication services provided to them. **Pakistan:** **20.02:** Investigation Fair Trial Act 2013: - allows security agencies to seek a judicial warrant to monitor private communications "to neutralize and prevent (a) threat or any attempt to carry out scheduled offences." It covers information sent from or received in Pakistan, or between Pakistani citizens, whether they are resident in the country or not. Warrants can be issued if a law enforcement official has "reason to believe" there is a risk of terrorism; warrants can also be temporarily waived by intelligence agencies.
2014	**Russia:** **05.05:** Federal Law No. 97-FZ: - 3. The organizer of the dissemination of information on the Internet is obliged to store on the territory of the Russian Federation information on the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds or other electronic messages of Internet users and information about these users within six months from the date of completion of such actions, as well as provide this information to authorized state bodies, carrying out operational-investigative activities or ensuring the security of the Russian Federation, in cases established by federal laws.

	- the second paragraph of paragraph 2 of article 44, after the words "execution of the contract for the provision of communication services ," add the words "the procedure for identifying users of communication services for data transmission and providing access to the information and telecommunications network "Internet" and the terminal equipment used by them,"; **21.07:** Federal Law No. 242-FZ - 3. The organizer of the dissemination of information on the Internet is obliged to store on the territory of the Russian Federation information on the facts of receiving, transmitting, delivering and (or) processing voice information, written text, images, sounds or other electronic messages of Internet users and information about these users within six months from the date of completion of such actions, as well as provide this information to authorized state bodies, carrying out operational-investigative activities or ensuring the security of the Russian Federation, in cases established by federal laws. - 7) the presence on the territory of the Russian Federation of databases of information, with the use of which are collected, recorded, systematized, accumulated, stored, clarified (updated, changed), extracted personal data of citizens of the Russian Federation.".
2015	**China:** **27.12:** Counterterrorism law of the People's Republic of China - Article 18: Telecommunications operators and internet service providers shall provide technical interfaces, decryption and other technical support assistance to public security organs and state security organs conducting prevention and investigation of terrorist activities in accordance with law. **Kazakhstan:** **24.11:** Law of the Republic of Kazakhstan No. 419-V: - As amended 2021.: Article 12. Point 2. Personal data shall be stored by the owner and/or operator, as well as by a third party in a database located in the territory of the Republic of Kazakhstan. - 2-1) maintain registers of registered periodicals, news agencies and online publications; - 2-2) maintain a register of entities distributing periodicals or Internet resources that post **24.11:** Law of the Republic of Kazakhstan No. 418-V ЗРК: - 17) 4) to transfer backup copies of electronic information resources to a single national backup platform for storing electronic information resources in the manner and within the time limits determined by the authorized body in the field of information security, unless otherwise established by the laws of the Republic of Kazakhstan.
2016	**China:**

	07.11: Cybersecurity Law of the People's Republic of China - Article 21: The State implements a cybersecurity multi-level protection system [MLPS]. - - (3) Adopt technical measures for monitoring and recording network operational statuses and cybersecurity incidents, and follow provisions to store network logs for at least six months; - Article 24: Network operators handling network access and domain name registration services for users, handling stationary or mobile phone network access, or providing users with information publication or instant messaging services, shall require users to provide real identity information when signing agreements with users or confirming the provision of services. Where users do not provide real identity information, network operators must not provide them with relevant services. - Article 28: Network operators shall provide technical support and assistance to public security organs and national security organs that are safeguarding national security and investigating criminal activities in accordance with the law. - Article 37: Critical information infrastructure operators that gather or produce personal information or important data during operations within the mainland territory of the People's Republic of China, shall store it within mainland China. Where due to business requirements it is truly necessary to provide it outside the mainland, they shall follow the measures jointly formulated by the State cybersecurity and informatization departments and the relevant departments of the State Council to conduct a security assessment; where laws and administrative regulations provide otherwise, follow those provisions. - Article 71: When there is conduct violating the provisions of this Law, it shall be recorded in - credit files and made public in accordance with relevant laws and administrative regulations. **Russia:** **23.06:** Federal Law No. 208-FZ - 12. Only a Russian legal entity or a citizen of the Russian Federation can be the owner of a news aggregator. - 3. The federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications shall maintain a register of news aggregators. In order to ensure the formation of a register of news aggregators, the federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications: **07.07:** Federal Law No. 374-FZ - Organizer of the dissemination of information to provide the federal executive body in the field of security with the information necessary for decoding received, transmitted, delivered and (or) processed electronic messages,

	- Telecom operators are obliged to store on the territory of the Russian Federation: - 1) information on the facts of receiving, transmitting, delivering and (or) processing voice information, text messages, images, sounds, video or other messages of users of communication services - within three years from the date of completion of such actions; - 1.1. Telecom operators are obliged to provide the authorized state bodies carrying out operational-search activities or ensuring the security of the Russian Federation, the specified information, information about users of communication services and the communication services rendered to them and other information necessary to perform the tasks assigned to these bodies, in cases established by federal laws.". - 3.1. The organizer of the dissemination of information on the Internet is obliged to provide the information specified in paragraph 3 of this article to the authorized state bodies carrying out operational-investigative activities or ensuring the security of the Russian Federation, in cases established by federal laws."; **05.12:** Doctrine of Information Security of the Russian Federation - Part IV (23d): d) enhancing the safe operation of information infrastructure objects, including with a view to ensuring stable interaction between government bodies, preventing foreign control over these objects, and ensuring the integrity, smooth operation and safety of the unified telecommunications network of the Russian Federation, as well as ensuring the security of information transferred through this network and processed within information systems in the territory of the Russian Federation; - Part IV (29e): e) developing a national system of the Russian Internet segment management. **Kazakhstan:** **28.12:** Law of the Republic of Kazakhstan dated 28.12.2016 No. 36-VI: - 3. Operators of communication, the operator of a centralized database of subscribers numbers and the operator of the database of identification codes of the subscribers devices of cellular communication shall be obliged to provide the access to information contained in the databases of subscribers numbers and identification codes of the subscribers devices of cellular communication to the bodies carrying out operational-investigative, counterintelligence activities on communication networks, in accordance with this Law and the laws of the Republic of Kazakhstan "On operational-investigative activity", "On counterintelligence activities", "On personal data and their protection". - 2) collect and store official information in the manner determined by the Government of the Republic of Kazakhstan. Service information shall be stored in the territory of the Republic of Kazakhstan. It shall be prohibited to transfer service information and aggregated data outside the Republic of Kazakhstan, except in case of provision of communication services to subscribers of the Republic of Kazakhstan located abroad;

	- 1) provide the bodies carrying out operational-investigative, counterintelligence activities on communication networks with organizational and technical capabilities of conducting operational-investigative, counterintelligence actions on all communication networks, as well as take measures for prevention of disclosure of forms and methods for conducting the specified actions; **Pakistan:** **11.08:** Prevention of Electronic Crimes Act - Chapter 2 (17). Unauthorised used of sim cards (large amounts of verification data required) - Chapter 2 (31). Expedited preservation and acquisition of data. - (32). Retention of Traffic data
2017	**China:** **27.06:** PRC National Intelligence Law - Article 11: National intelligence work institutions shall lawfully collect and handle intelligence related to foreign institutions, organizations or individuals carrying out, directing or funding foreign or domestic institutions, organizations, or individuals colluding to carry out, conduct endangering the national security and interests of the People's Republic of China; so as to provide intelligence references and bases for preventing, stopping, and punishing the above conduct. **Kazakhstan:** **15.02:** Decree of the President of the Republic of Kazakhstan No. 422 : - Due to the centralization of Internet connection through the Unified Internet Access Gateway of government agencies, the threat of unauthorized access and harmful effects on the electronic information resources of government agencies has been significantly reduced. More than 180 million attacks of various levels are recorded and repelled on a daily basis. - The national segment of the Internet has more than 120,000 Internet resources in . KZ and .KAZ, in accordance with the legislation physically located on the territory of the Republic of Kazakhstan. **28.12**: Law of the Republic of Kazakhstan No. 128-V: amending 'On Communications' 25) - 4. It shall be forbidden to exchange Internet traffic between telecommunication operators through telecommunication networks located in the territory of another state. - 1-2. Communication operators shall be prohibited to render communication services without entering information about the subscriber in the system of collection and storage of service information about subscribers.

	Kyrgyzstan: **20.07:** Law of the Kyrgyz Republic No. 129: - Article 25: 1. In the case of cross-border transfer of personal data, the holder (owner) of an array of personal data under the jurisdiction of the Kyrgyz Republic transmitting the data proceeds from the existence of an international agreement between the parties, according to which the receiving party ensures an adequate level of protection of the rights and freedoms of personal data subjects and protection of personal data established in the Kyrgyz Republic. **Russia:** **25.11:** Federal Law 327-FZ - The prohibitions established by the subject of personal data on the transfer (except for granting access), as well as on the processing or processing conditions (except for obtaining access) of personal data authorized by the subject of personal data for distribution, do not apply to cases of processing personal data in the state, public and other public interests determined by the legislation of the Russian Federation. - 15. The requirements of this article shall not apply in the case of the processing of personal data in order to perform the functions, powers and duties assigned by the legislation of the Russian Federation to federal executive bodies, executive authorities of the constituent entities of the Russian Federation, local self-government bodies. "; **29.07:** Federal Law 241-FZ - 4.4. The organizer of the instant messaging service, which is a Russian legal entity or a citizen of the Russian Federation, is obliged to store information about the identification of the subscriber number of the mobile radiotelephone communication of the user of the instant messaging service (hereinafter referred to as the identification information about the subscriber number) only on the territory of the Russian Federation. Providing third parties with identification information about the subscriber number can be carried out only with the consent of the user of the instant messaging service, with the exception of cases provided for by this Federal Law and other federal laws. The obligation to provide proof of consent of the user of the instant messaging service to provide third parties with identification information about the subscriber number of the user of the instant messaging service shall be imposed on the organizer of the instant messaging service. " - 1) to carry out identification of Internet users, the transmission of electronic messages of which is carried out by the organizer of the instant messaging service (hereinafter referred to as the users of the instant messaging service), by the subscriber number of the mobile radiotelephone operator in accordance with the procedure established by the Government of the Russian Federation, on the basis of an identification agreement concluded by the organizer of the instant

	messaging service with the mobile radiotelephone operator communications, except as provided for by this Federal Law;
2018	**Tajikistan:** **08.06:** Law of the Republic of Tajikistan "On Personal Data Protection" Article 18. Cross-border transfer of personal data 1. Cross-border transfer of personal data on the territory of foreign states that provide adequate protection of the rights of personal data subjects shall be carried out in accordance with this Law. Cross-border transfer of personal data may be prohibited or restricted in order to protect the foundations of the constitutional order of the Republic of Tajikistan, morality, health, rights and legitimate interests of citizens, to ensure the defense of the country and the security of the state. **Kyrgyzstan:** **22.05:** Law of the Kyrgyz Republic No. 53: - Article 6: Article 6. Registration of mass mediaState registration (re-registration) and registration of termination of activity of mass media (further - registration) shall be carried out within 10 working days by entering in the state register of mass media information on creation, re-registration and termination of activity of mass media. **Pakistan:** **13.12:** Data Retention of Internet extended to Public Wifi Hotspot Regulations - Wifi Hotspot Data Retention
2019	**Russia:** **01.05:** Federal Law No. 90 “On a Sovereign Internet”: - In the case of centralized management of the public communications network, the persons participating in the centralized management shall be obliged to comply with the rules for routing telecommunication messages established by the federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications. The rules for routing telecommunication messages apply to telecommunication messages if the recipient or sender of such messages is a user of communication services in the territory of the Russian Federation. - a) part 21 shall be supplemented with the following sentence: "Operators of state information systems, municipal information systems, information systems of legal entities engaged in procurement in accordance with Federal Law No. 223-FZ of July 18, 2011 "On

	Procurement of Goods, Works, Services by Certain Types of Legal Entities" should not allow the use of databases and technical databases located outside the territory of the Russian Federation during the operation of information systems. means that are not part of such information systems. "; **02.12:** Federal Law No. 425-FZ: - 4.1. When selling certain types of technically complex goods with pre-installed programs for electronic computers, the consumer is provided with the opportunity to use certain types of technically complex goods with pre-installed programs for electronic computers, the countries of origin of which are the Russian Federation or other member states of the Eurasian Economic Union. The list of certain types of these technically complex goods, the procedure for compiling and maintaining a list of programs for electronic computers, the countries of origin of which are the Russian Federation or other member states of the Eurasian Economic Union and which must be pre-installed, and the procedure for their preliminary installation, including requirements for functioning, are determined by the Government of the Russian Federation. **Uzbekistan:** **16.04:** Law of the Republic of Uzbekistan No.ZRU-547: - article 15: Cross-border transfer of personal data may be prohibited or restricted in order to protect the foundations of the constitutional order of the Republic of Uzbekistan, morality, health, rights and legitimate interests of citizens of the Republic of Uzbekistan, to ensure the defense of the country and the security of the state. - Article 20. The procedure for registration of personal data bases Registration of the database of personal data is carried out on an application basis by notification. An application for registration of a personal data base in the State Register of Personal Data Bases shall be submitted to the authorized state body.
2020	**Kazakhstan:** **25.06:** Law of the Republic of Kazakhstan No. 347-VI: - 41-1 3) 2) provide assistance to the national security bodies of the Republic of Kazakhstan and law enforcement bodies of the Republic of Kazakhstan in identifying the person using networks and (or) means of communication for criminal purposes, damaging the interests of the individual, society and the state, as well as for disseminating information that violates the legislation of the Republic of Kazakhstan on elections, containing calls for extremist and terrorist activities, mass riots, as well as for participation in mass (public) events held in violation of the established order. - 16) ensure the functioning of the National Video Monitoring System;

	Tajikistan: **02.01:** Law of the Republic of Tajikistan "On Countering Extremism" No. 1655 - obliges individuals and legal entities engaged in the provision of communication services, including Internet providers, to ensure the storage of extremist information in their servers for up to 6 months. - 11. The Communications Service under the Government of the Republic of Tajikistan in the field of countering extremism shall have the following powers: - monitors all Internet communication services, including social networks and, if necessary, prevents extremist activity, restricts or suspends the activities of these networks (Internet providers);
2021	**China:** **01.09:** Data Security Law of the People's Republic of China - Article 26: The installation of image collection or personal identity recognition equipment in public venues shall occur as required to safeguard public security and observe relevant State regulations, and clear indicating signs shall be installed. Collected personal images and personal distinguishing identity characteristic information can only be used for the purpose of safeguarding public security; it may not be used for other purposes, except where individuals' separate consent is obtained. - Personal information handled by State organs shall be stored within the mainland territory of the People's Republic of China. If it is truly necessary to provide it abroad, a security assessment shall be undertaken. Relevant authorities may be requested to support and assist with security assessment. - Article 53: Personal information handlers outside the borders of the People's Republic of China, as provided in Article 3, Paragraph 2, of this Law, shall establish a dedicated entity or appoint a representative within the borders of the People's Republic of China to be responsible for matters related to the personal information they handle, and are to report the name of the relevant entity or the personal name of the representative and contact method, etc., to the departments fulfilling personal information protection duties and responsibilities. **Russia:** **01.07:** Federal Law No. 236-FZ - 3) create a branch, or open a representative office, or establish a Russian legal entity and ensure the functioning in the territory of the Russian Federation of a branch, or representative office, or a Russian legal entity in accordance with the requirements provided for in Article 7 of this Federal Law. - Article 8. List of foreign persons operating on the Internet in the territory of the Russian Federation

	Kazakhstan: **30.12:** Law of the Republic of Kazakhstan No. 97-VII - Article 36. 4. Owners or holders of information systems of state bodies shall be obliged to notify the subjects of personal data or their legal representatives through the state service for controlling access to personal data in automatic mode about all cases of using, changing and supplementing personal data in the framework of information interaction, except for the activities of law enforcement, special state bodies of the Republic of Kazakhstan and courts, enforcement proceedings, subject to registration of subjects of personal data or their legal representatives on the web portal of "electronic government". **Uzbekistan:** **14.01:** Law of the Republic of Uzbekistan No. ZRU-666: - Article 271. The owner and (or) operator, when processing personal data of citizens of the Republic of Uzbekistan using information technologies, including in the World Wide Web, is obliged to ensure their collection, systematization and storage in personal data databases on technical means physically located on the territory of the Republic of Uzbekistan and registered in accordance with the established procedure in the State Register of Personal Data Bases. **04.03:** Law of the Republic of Uzbekistan No. 3RU-679: - Article 121: monitor their website and (or) pages of the website or other information resource on the World Wide Web, including instant messaging systems on which publicly available information is posted, in order to identify information and materials specified in part one of this article; **Kyrgyzstan:** **29.11:** Law of the Kyrgyz Republic "On Personal Data" No. 142: - Article 17 (h): h) provide upon request of the authorized state body or the Ombudsman (Akyikatchy) of the Kyrgyz Republic, within one week, the information necessary to perform their powers. **Pakistan:** **12.10:** Removal and Blocking of Unlawful Online Content (Procedure, Oversight and Safeguards) Rules 2021: - “significant social media companies,” defined as those with over 500,000 users, to register with the PTA, establish a permanent registered office in Pakistan, and appoint an in-country representative.
2022	**China:** **16.11:** Provision on the Management of Internet Comment Post Services

	- Article 4: Post comment service providers shall strictly implement primary responsibility for the management of post comment services, performing the following obligations in accordance with law: (1) Carrying out verification of registered accounts through means such as mobile phone numbers, ID numbers, or uniform social credit codes in accordance with the principle of having 'real names behind the scenes, but whatever you wish up front", and comment services must not be provided to accounts for which identification has not been verified or that are falsely usurping the identity information of organizations or other persons. **Kazakhstan:** **03.05:** Law of the Republic of Kazakhstan No. 118-VII: - The authorized body in the field of mass media maintains a register of legal representatives of foreign online platforms and (or) instant messaging services that interact with the authorized body in the field of mass media, in accordance with the procedure, determined by the authorized body in the field of mass media. - 18-2) 3. An online platform or instant messaging service operating on the Internet in the territory of the Republic of Kazakhstan shall be obliged to install a program to determine the number of users of this resource on the Internet.
2023	**Kyrgyzstan:** **24.02:** Law of the Kyrgyz Republic "On Countering Extremist Activity" No. 40 - Article 8 (9): monitoring of the Internet space in order to prevent the dissemination of extremist materials in this network; - Article 5 (2): 2. The Internet service provider, the owners of public access points shall be obliged to identify their subscribers. **India:** **09.08:** The Digital Personal Data Protection Bill 2023: - The state is able to retain data in the interests of national security. - Cross border transfers can be limited to countries decided upon by the state.

Appendix E – Timeline of Infrastructure Control Laws

1995	**Russia:** **05.07:** Federal Law No. 144-FZ - Law establishing SORM equipment
1996	**China:**

	01.02: Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China - Article 6: Computer information networks directly conducting international access must use international entry and exit channels provided by the Ministry of Post and Telecommunications' public telecommunications networks.
1999	**Uzbekistan:** **20.08:** Law of the Republic of Uzbekistan No. 822-1: - Article 18. Relations of operators and providers with bodies carrying out operational-search activities. Operators and providers operating in the territory of the Republic of Uzbekistan are obliged to ensure, at their own expense, the installation and operation of equipment used to conduct operational-search activities on telecommunications networks by bodies engaged in operational-investigative activities, as well as to provide measures to prevent the disclosure of organizational and tactical methods of carrying out these activities.
2000	**Russia:** **09.09:** Doctrine of Information Security - securing the technological independence of the Russian Federation in the major areas of informatization, telecommunications and communication determining its security, and - primarily in the field of developing specialized computer hardware for weapon and military equipment specimens. **25.07:** Order 130 - Install SORM Into networks; in agreement with the law 144-FZ 1995 and 40-FZ 1995
2002	**Tajikistan:** **10.05:** Law of the Republic of Tajikistan "On Communications" - Article 33: In case of emergency circumstances (military actions, natural disasters, quarantines, etc.) defined by the legislation of the Republic of Tajikistan, the authorized state bodies have the right of priority use, as well as restriction or suspension of the functioning of any networks and means of telecommunications, regardless of their departmental affiliation.
2004	**Kazakhstan:** **05.06:** Law of the Republic of Kazakhstan No. 567-II; - 5) 8) ensuring of the centralized management of national resources in the field of communications.
2010	**China:** **08.06:** [White Paper] "On the Internet in China" - The state telecommunications administration department is responsible for the administration of the Internet industry, including the

	administration of basic resources of the Internet such as domain names, IP addresses within China." **Pakistan:** **15.03:** Monitoring and Reconciliation Telephony Traffic Regulations - Regulation 4: PTA to install web monitoring system into networks
2011	**Uzbekistan:** **30.12:** Law of the Republic of Uzbekistan No. ZRU-314: - article 8: Specialised body in the field of telecommunications develops and approves the procedure for using the address space, determines the system of domain names of the national segment of the World Wide Web;
2013	**Kyrgyzstan:** **11.06:** Law of the Kyrgyz Republic 11.06.2013 No. 129: amending Law of the Kyrgyz Republic "On electrical and Postal Communications" No. 31 (1998): Article 21-1: (2) - Article 21-1: (4) 4. Technical requirements for communication networks, special technical means designed to control and record legally obtained information/information transmitted through technical communication channels, the procedure for interaction in the implementation of the functions of the system of special investigative actions and counterintelligence measures in communication networks, including the development of the interface (technical regulations), the development of the necessary software, the solution of the issue of connection and access channels, other issues related to ensuring the legality of the implementation of special investigative actions and counterintelligence measures in communication networks, a comprehensive solution to all issues and problems related to the implementation and operation of a system of special investigative actions and counterintelligence measures in communication networks, in accordance with international recommendations and technical concepts developed in this area, as well as the requirements of the current legislation of the Kyrgyz Republic The Republics shall be established by the Government of the Kyrgyz Republic.
2015	**Kazakhstan:** **24.11:** Law of the Republic of Kazakhstan No. 419-V - 1) consulting and technical assistance to internal affairs bodies when installing special technical equipment on the territory of penal institutions to block a radio signal or identification and (or) suppression of unauthorized use of subscribers devices; **Kyrgyzstan:** **20.01:** Law of the Kyrgyz Republic No. 20:

	- Article 34-1. Construction and operation of communication lines in the border area of the Kyrgyz Republic. The procedure for the construction, operation and maintenance of communication lines, including cable laying and construction of linear-cable structures, implementation of construction and emergency restoration works on linear-cable communication facilities when crossing the state border of the Kyrgyz Republic, in the border territory of the Kyrgyz Republic, shall be determined by the Government of the Kyrgyz Republic
2016	**China:** **06.11:** Cybersecurity Law of the People's Republic of China: - Article 23: Critical network equipment and specialized cybersecurity products shall follow national standards and mandatory requirements, and be security certified by a qualified establishment or meet the requirements of a security inspection, before being sold or provided. The state cybersecurity and informatization departments, together with the relevant departments of the State Council, will formulate and release a catalog of critical network equipment and specialized cybersecurity products, and promote reciprocal recognition of security certifications and security inspection results to avoid duplicative certifications and inspections. - Article 35: Critical information infrastructure operators purchasing network products and services that might impact national security shall undergo a national security review organized by the State cybersecurity and informatization departments and relevant departments of the State Council. **Kazakhstan:** **28.12:** Law of the Republic of Kazakhstan No. 36-VI: - 4) provide at the expense of own or attracted funds the functions of own telecommunication equipment for technical conduct of operational-investigative, counterintelligence actions in accordance with the requirements for communication networks and means and the order which are determined by the Government of the Republic of Kazakhstan. **Pakistan:** **11.08:** Prevention of Electronic Crimes Act - Central domain name system to be introduced **Russia:** **05.12:** Doctrine of Information Security of the Russian Federation - Part II, 8, c): c) developing the sector of information technologies and electronics in the Russian Federation and improving the performance of production, research and scientific and technological community to

	develop, produce and operate information security means and provide information security services; - Part IV (23c): c) enhancing the protection of the critical information infrastructure and reliability of its functioning, developing mechanisms of identification and prevention of information security threats and elimination of their effects, as well as enhancing the protection of citizens and territories from the effects of emergencies caused by information and technical impacts on the objects of critical information infrastructure; - Part IV (33): The information security system includes the following actors: owners of critical information objects and organizations operating such objects; mass media and mass communications; monetary, foreign currency, banking and other financial institutions; telecommunication operators; information system operators; organizations that create and operate information and communications systems; organizations that develop, produce and operate information security means; organizations that provide information security services; organizations that provide education services in this sphere; public associations and other organizations and individuals involved in information security under the laws of the Russian Federation.
2017	**China:** **03.01:** International Strategy of Cooperation on Cyberspace - They exercise jurisdiction over ICT infrastructure, resources and activities within their territories, and are entitled to protect their ICT systems and resources from threat, disruption, attack and destruction so as to safeguard citizens' legitimate rights and interests in cyberspace. **Kazakhstan:** **15.02:** Decree of the President of the Republic of Kazakhstan No. 422**:** - Approaches to ensuring the security of communication infrastructure and public telecommunications networks are built around a system of centralized management of telecommunications networks, through the capabilities of backbone telecom operators that implement the concept of "electronic border" on border equipment. - Along with building work with critical information and communication infrastructure facilities from among strategic and especially important state facilities, objects of strategic sectors of the economy, revise the criterion for classifying as critically important objects of information and communication infrastructure with the possibility of classifying them as critically important objects focused on providing information and communication services to the population. **28.12:** Law of the Republic of Kazakhstan No. 128-IV - 2. For networks that make up a unified telecommunications network of the Republic of Kazakhstan, with the exception of presidential communication networks, the national security bodies shall determine

	the procedure for functioning the system of centralized management of telecommunications networks of the Republic of Kazakhstan, including: organization, registration and operation of international junction points; - 7-1) 16) determine the administrator and registrar of domain names, approve the rules for registration, use and distribution of domain names in the space of the Kazakhstani segment of the Internet;
2019	**Russia:** **01.05:** Federal Law of the Russian Federation 90-FZ - 3) c) 51.: "51. The telecom operator providing services for providing access to the information and telecommunication network "Internet" is obliged to ensure the installation in its communication network of technical means to counter threats to the stability, security and integrity of the functioning in the territory of the Russian Federation of the information and telecommunication network "Internet" and the public communication network (hereinafter referred to as technical means of countering threats), to provide information to the federal body executive power, exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications, the actual place of installation of technical means of countering threats within three days from the date of installation and comply with the technical conditions provided for in paragraph 3 of Article 651 of this Federal Law, the installation of technical means of countering threats, as well as the requirements for communication networks. - 562 1. 1. In the case of transfer into possession or use of a communication line crossing the State Border of the Russian Federation, the contract for such transfer shall contain information on the purpose of using the specified communication line, as well as on the means of communication established on the specified communication line. Owners or other owners of the specified communication line within the terms, procedure, composition and format determined by the federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications, are obliged to submit in electronic form to this federal executive body information on the purpose of using the communication line, as well as on the means of communication, installed on the specified communication line. The procedure for monitoring the accuracy and completeness of the information provided shall be approved by the federal executive body exercising the functions of control and supervision in the field of mass media, mass communications, information technology and communications. - 2. In the event of threats to the stability, security and integrity of the functioning of the Internet information and telecommunications network and the public communication network on the territory of the Russian Federation, centralized management of the public communications network may be carried out by the federal executive body exercising the functions of control and supervision in the field of

	mass media, mass communications, information technology and communications. **Uzbekistan:** **16.04:** Law of the Republic of Uzbekistan 16.04.2019 No. ZRU-547 - article 11: The state security service of the republic of Uzbekistan has the powers in the formation of a unified register of critical information infrastructure facilities, as well as the organization and maintenance of its maintenance; - article 28: provide the authorized state body with the right of access to monitoring systems or critical information infrastructure facilities for the implementation of organizational and technical measures for monitoring the state of cybersecurity; - Article 8. The principle of priority of participation of domestic producers in the creation of a cybersecurity system - When purchasing goods (works, services) necessary to ensure the cybersecurity of state and economic management bodies, local government bodies, goods (works, services) produced in the territory of the Republic of Uzbekistan have priority over products manufactured abroad.
2020	**Kazakhstan:** **25.06:** Law of the Republic of Kazakhstan; No. 347-VI: - 3-1. Long-distance and/or international operators shall: 1) publish a list of standard connection points (connections); 2) provide, at the expense of its own funds, the lines and communication channels necessary to ensure the functioning of the system of centralized management of telecommunication networks of the Republic of Kazakhstan, and ensure the connection of its communication networks to the system of centralized management of telecommunication networks of the Republic of Kazakhstan in the manner determined by the National Security Committee of the Republic of Kazakhstan; 3) ensure connection and transfer of their networks and communication subnetworks to Internet traffic exchange points on a regional basis, subject to the presence of an operator of long-distance and (or) international communication in the region where Internet traffic exchange points are located, as well as receiving Internet traffic from Internet traffic exchange points in the manner determined by the National Security Committee of the Republic of Kazakhstan; 4) carry out traffic transmission using the protocols, supporting encryption with the use of a security certificate, except for the traffic encrypted by means of cryptographic protection of information on the territory of the Republic of Kazakhstan. -
2022	**Kazakhstan:**

	14.07: Law of the Republic of Kazakhstan No. 141-VII - 25) 3. Passage of international traffic shall be carried out only through the networks of international communications operators, taking into account observance of the procedure for operation of the centralized management system of telecommunications networks of the Republic of Kazakhstan.

Appendix F – Relevant Laws Listed by Country

China:

1. Computer Information System Security Protection Regulations of the People's Republic of China | 18.02.1994 |
2. Provisional Management Regulations for the International Connection of Computer Information Networks of the People's Republic of China | 23.01.1996 |
3. Computer Information Network and Internet Security, Protection and Management Regulations | 11.12.1997 |
4. Internet Information Service Management Measures | 25.09.2000 |
5. On the Internet in China | 08.06.2010 |
6. Counter-Terrorism Law of the People's Republic of China | 27.12.2015 |
7. International strategy of cooperation on cyberspace | 02.03.2017 |
8. Cybersecurity Law of the People's Republic of China | 01.06.2017 |
9. Data Security Law of the People's Republic of China | 01.09.2021 |
10. Personal Information Protection Law of the People's Republic of China | 01.11.2021 |
11. Provisions on the Management of Internet Post Comments Services | 16.11.2022 |

India:

12. Indian Penal Code (Amendment) Act | 1870 |
13. Code of Criminal Procedure | 1973 |
14. The Information Technology Act 2000 No. 21 | 09.06.2000 |
15. Information Technology (Procedure and Safeguards for Blocking Access of Information by Public) Rules 2009 | 27.10.2009 |
16. Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules | 25.02.2021 |
17. The Digital Personal Data Protection Act, 2023 (No. 22 of 2023) | 11.08.2023 |

Kazakhstan:

18. Law of the Republic of Kazakhstan No. 567 'On Communications' | 05.07.2004 |
19. Law of the Republic of Kazakhstan No. 31-III "On Countering Terrorism" | 08.02.2005 |
20. Law of the Republic of Kazakhstan No. 178-IV | 10.07.2009 |
21. Law of the Republic of Kazakhstan No. 15-V | 27.04.2012 |
22. Law of the Republic of Kazakhstan No. 516-IV | 18.01.2012 |
23. Law of the Republic of Kazakhstan No. 121-V | 03.07.2013 |
24. Law of the Republic of Kazakhstan No. 200-V | 23.04.2014 |
25. Law of the Republic of Kazakhstan No. 419-V | 24.11.2015 |
26. Law of the Republic of Kazakhstan No. 128-VI | 22.12.2016 |

27. Law of the Republic of Kazakhstan No. 36-VI | 28.12.2016 |
28. Decree of the President of Kazakhstan No. 422 | 15.02.2017 |
29. Law of the Republic of Kazakhstan No. 128-VI | 28.12.2017 |
30. Law of the Republic of Kazakhstan No. 241-V | 02.04.2019 |
31. Law of the Republic of Kazakhstan No. 347-VI | 25.06.2020 |
32. Law of the Republic of Kazakhstan No. 97-VII | 30.12.2021 |
33. Law of the Republic of Kazakhstan No. 118-VI | 03.05.2022 |
34. Law of the Republic of Kazakhstan No. 141-VII | 14.07.2022 |
35. Law of the Republic of Kazakhstan No. 118-VII | 03.05.2023 |

Kyrgyzstan:

36. Law of the Kyrgyz Republic No. 938-XII "On Mass Media" | 02.07.1992 |
37. Law of the Kyrgyz Republic No. 30 "On Electrical and Postal Communications" | 02.04.1998 |
38. Law of the Kyrgyz Republic No. 150 "On Countering Extremist Activity" | 17.08.2005|
39. Law of the Kyrgyz Republic No. 101 "On Protection from False and Inaccurate Information | 23.08.2021 |
40. Law of the Kyrgyz Republic No. 142 "On Personal Data" | 29.11.2021 |
41. Law of the Kyrgyz Republic No. 40 "On Countering Extremist Activity" | 24.02.2023 |

Pakistan:

42. Pakistan Penal Code | 1860 |
43. Penal Code (Amendment) Act XXVII | 1870 |
44. Code of Criminal Procedure 1898 (as amended 1991) | 1898 |
45. Criminal Law (Amendment) Act IV | 1986 |
46. Pakistan Telecommunications (re-organisation) Act | 17.10.1996 |
47. Amendment to the Code of Criminal Procedure | 1997 |
48. Defamation Ordinance 2002 | 01.10.2002 |
49. Telecommunications Policy 2015 | 11.12.2015 |
50. Prevention of Electronic Crimes Act | 11.08.2016 |
51. Removal and Blocking of Unlawful Online Content (Procedure and Oversight and Safeguard) Rules | 12.10.2021 |
52. Criminal Law Reforms 2021 of the Pakistan Penal Code 1860 | 25.09.2021 |

Russia:

53. Federal Law 2124-I "On Mass Media" | 1991 |
54. Doctrine of Information Security | 09.09.2000 |
55. Federal Law No. 112 FZ | 25.07.2002 |
56. Federal Law No. 114 FZ "On Countering Extremist Activity" | 25.07.2002 |
57. Federal Law. No. 126 FZ "On Communications" | 07.07.2003 |
58. Federal Law No. 149 FZ "On Information, Informational Technology and the Protection of Information" | 14.07.2006 |
59. Federal Law No. 139-FZ. ("Blacklist law") | 28.07.2012 |

60. Federal Law No. 34 -FZ "Concerning the Introduction of Amendments to Article 4 of the Law of the Russian Federation "On the Mass Media" and Article 13.21 of the Code of Administrative Offences of the Russian Federation | 05.04.2013 |
61. Federal Law No. 136-FZ (Protecting Religious Sentiment) | 26.06.2013 |
62. Federal Law No. 135-FZ (Gay Propaganda Law) | 29.06.2013 |
63. Federal Law No. 398-FZ "On Amendments to the Federal Law 'On Information, Information Technologies and Information Protection'" (Website blocking) | 25.12.2013
64. Federal Law No. 97-FZ (Registration of Mass Media) | 05.05.2014 |
65. Federal Law No. 242-FZ (Law on Data Localisation) | 21.07.2014 |
66. Federal Law No. 208-FZ "On Amending the Federal Law 'On Information, Information Technologies and Information Protection' and the Code of Administrative Offenses of the Russian Federation" | 23.06.2016 |
67. Doctrine of Information Security of the Russian Federation | 05.12.2016 |
68. Federal Law No. 374-FZ (Yarovaya Law) | 06.07.2017 |
69. Federal Law No. 276-FZ "On Amendments to the Federal Law "On Information, Information | 21.07.2017 |
70. Federal Law No. 241-FZ "On Amending Articles 10.1 and 15.4 of the Federal Law "On Information, Information Technologies and Information Protection" (End anonymity) | 29.07.2017 |
71. Technologies and Information Protection" (Controlling VPN) | 29.07.2017 |
72. Federal Law No. 327-FZ (New foreign agent law) | 25.11.2017 |
73. Federal Law No. 30-FZ "On Amending the Federal Law "On Information, Information Technologies and Information Protection" | 18.03.2019 |
74. Federal Law No. 31-FZ, "On Amending the Article 15.3 of the Federal Law "On Information, Information Technologies, and Information Protection" (Fake News Law) | 18.03.2019 |
75. On Amendments to the Federal Law "On Communications" and the Federal Law "On Information, Information Technologies and Information Protection" | 01.05.2019 |
76. Federal Law No. 425-FZ | 02.12.2019 |
77. Federal Law No. 426-FZ"On Amendments to the Law of the Russian Federation "On Mass Media" and the Federal Law "On Information, Information Technologies and Information Protection" (Expansion of Definition of Foreign Agents) | 02.12.2019 |
78. Federal Law No. 519-FZ (Amendments to Personal Data Law) | 25.12.2020 |
79. Federal Law No. 482-FZ | 30.12.2020 |
80. Federal Law No. 530-FZ "On Amendments to the Federal Law "On Information, Information Technologies and Information Protection" | 30.12.2020 |
81. Federal Law No. 538-FZ (New Defamation) | 30.12.2020 |
82. Federal Law. 236-FZ "On the Activities of Foreign Persons in the Internet Information and Telecommunication Network on the Territory of the Russian Federation" | 01.07.2021 |
83. Federal Law No. 31-FZ (Discreditation of the Armed Forces) | 04.03.2022 |
84. Federal Law No. 32-FZ (Law of fakes) | 04.03.2022 |

Tajikistan:

85. Law of the Republic of Tajikistan No. 55 "On Information" | 10.05.2002 |
86. Law of the Republic of Tajikistan "On the Legal Regime of the State of Emergency" | 10.05.2002 |

87. Law of the Republic of Tajikistan No. 69 “On the fight against Extremism” | 08.12.2003 |
88. Law of the Republic of Tajikistan No. 848 | 03.07.2012 |
89. Law of the Republic of Tajikistan “On Personal Data Protection” | 08.06.2018 |
90. Law of the Republic of Tajikistan No. 1655 “On Countering Extremism” | 02.01.2020 |
91. Law of the Republic of Tajikistan No. 56 “On Communications” | 10.05.2022 |

Uzbekistan:

92. Law of the Republic of Uzbekistan No. 541-I | 26.12.1997 |
93. Law of the Republic of Uzbekistan No. 822-1 | 20.08.1999 |
94. Law of the Republic of Kazakhstan No. 405-I | 30.08.2002 |
95. Law of the Republic of Uzbekistan of No. 560-II | 11.12.2003 |
96. Law of the Republic of Uzbekistan No. 1743 | 27.11.2007 |
97. Law of the Republic of Uzbekistan No. ZRU-314 | 30.12.2011 |
98. Law of the Republic of Uzbekistan No. ZRU-547 | 16.04.2019 |
99. Law of the Republic of Uzbekistan No. ZRU-666 | 14.01.2021 |
100. Law of the Republic of Uzbekistan No. 3RU-679 | 04.03.2021 |

Shanghai Cooperation Organisation:

101. Agreement on Regional Anti-terrorist Structure between the Member States of the Shanghai Cooperation Organization, 7 June 2002. Entered into force on 14 November 2003.
102. Protocol on Amendments to the Agreement on Regional anti-terrorist Structure between the Member States of the Shanghai Cooperation Organization, 5 September 2003. Entered into force on 1 October 2004.

103. Agreement on the Protection of Confidential Information in the Framework of Regional Anti-terrorist Structure of the Shanghai Cooperation Organization, 17 June 2004. Entered into force on 19 November 2015.

104. Protocol on Amendments to the Agreement on Regional Anti-terrorist Structure between the Member States of the Shanghai Cooperation Organization, 16 August 2007. Entered into force on 25 June 2009.

105. Convention on the Privileges and Immunities of the Shanghai Cooperation Organization, 17 June 2004. Entered into force 4 October 2007.

106. Agreement on the Databank of the Regional Anti-terrorist Structure of the Shanghai Cooperation Organization, 17 June 2004. Entered into force on 11 April 2007.

107. Agreement on Cooperation in Ensuring International Information Security between the Member States of the Shanghai Cooperation Organization, 16 June 2009. Entered into force on 2 June 2011.

108. Agreement on the Training of Personnel for Anti-terrorist Units of the Member States of the Shanghai Cooperation Organization, 16 June 2009. Entered into force on 13 September 2011.
109. 16. Convention of the Shanghai cooperation organization against terrorism, 16 June 2009. Entered into force on 14 January 2012.

110. Convention of the Shanghai Cooperation Organization on Countering Extremism of June 9, 2017. Entered into force on May 10, 2019.

111. Agreement on Technical Protection of Information in the Regional Anti-terrorist Structure of the Shanghai Cooperation Organization, 15 June 2006. Entered into force on 05 September 2015.
112. Agreement on Cooperation in Combating Crime between the Governments of the Member States of the Shanghai Cooperation Organization, 11 June 2010. Entered into force on 11 January 2012.

113. Agreement on scientific and technological cooperation between the Governments of the Shanghai Cooperation Organization Member States, 13 September 2013. Entered into force on 20 October 2015.

114. Agreement on cooperation between the Ministries of Defense of the Shanghai Cooperation Organization member States dated April 24, 2018. Entered into force from the date of signing.

115. Agreement between the Governments of the Shanghai Cooperation Organization member States on cooperation in the field of mass media, dated 14 June 2019. Entered into force on November 28, 2021.