CONTROLLING THE INTERNET: HOW AND UNDER WHAT CONDITIONS STATES CONTROL THE DIGITAL FLOW OF INFORMATION

Baurzhan Rakhmetov

A thesis is submitted to the School of Law and Politics, Cardiff University in requirement for the degree of Doctor of Philosophy (PhD) in Politics and International Relations

December 2020

STATEMENTS AND DECLARATIONS

STATEMENTS

1. This thesis is being submitted in partial fulfilment of the requirements for the degree of PhD.

2. This work has not been submitted in substance for any other degree or award at this or any other university or place of learning, nor is it being submitted concurrently for any other degree or award (outside of any formal collaboration agreement between the University and a partner organisation).

3. I hereby give consent for my thesis, if accepted, to be available in the University’s Open Access repository (or, where approved, to be available in the University’s library and for inter-library loan), and for the title and summary to be made available to outside organisations, subject to the expiry of a University-approved bar on access if applicable.

DECLARATION

1. This thesis is the result of my own independent work, except where otherwise stated, and the views expressed are my own. Other sources are acknowledged by explicit references. The thesis has not been edited by a third party beyond what is permitted by Cardiff University's Use of Third Party Editors by Research Degree Students Procedure.

Signed: Rakhmetov Baurzhan Date: 31.12.2020

WORD COUNT: 72 741

(excluding summary, acknowledgements, contents pages, appendices, tables, diagrams and figures, references, bibliography, footnotes and endnotes).

SUMMARY

This thesis addresses tactics and conditions of state control over the internet. Internet control is defined as the implementation by states of censorship, disruption, propaganda, and other means to shape and restrict the digital flow of information within national borders. First, I conduct a comparative analysis of sixty-five countries to identify to what extent and under what conditions states seek control of the internet. The main novelty of my study is the inclusion of democratic states in the analysis. In addition, I resort to two in-depth case studies (Kazakhstan and Ukraine) to further scrutinise and refine the findings drawn from the comparative analysis. Overall, two main conditions of state control over the internet were found. These are (1) the extractive (authoritarian) nature of domestic political institutions and (2) political instability and/or a leadership contest within inclusive (democratic) institutional settings. These findings supplement internet control scholarship, which tends to focus largely on authoritarian countries. I demonstrate that many democracies also seek to substantially control digital information.

ACKNOWLEDGMENTS

This thesis will not be possible without support from my family and friends, guidance from my supervisors and colleagues, and funding from my sponsor.

First, I want to thank my parents, who supported me throughout the whole period of the PhD program. I appreciate your love and faith in me. I dedicate this doctoral study to my parents, Zhanat and Bakhytzhan.

I am deeply grateful to Dr Brandon Valeriano, my first supervisor, who has been very helpful during my 4-year PhD journey. I learnt and keep learning a lot from you. I also want to thank Dr Andrea Calderaro and Professor Sergey Radchenko for helping me to understand the specifics of internet control and post-Soviet politics. I greatly benefited from your supervision. I am indebted to you for your support, patience, and contribution, which facilitated my growth as a researcher. And I am very thankful to Dr Hannes Hansen-Magnusson for reading my chapters and giving insightful comments on how to improve the main arguments of the thesis.

This thesis also benefited from continuous discussions and debates with my colleagues from 32 Park Place, especially with Tony, Tia, and Rhianwen. That was a fun time!

Last but not least, my study at Cardiff University won’t be real without funding from my sponsor, the Centre for International Programs (Bolashak). It is an honour to be a holder of the Bolashak Scholarship and I hope to conform to high standards of Bolashak graduates back in Kazakhstan.

I have met many wonderful people in Wales. My time and study in Cardiff will always be one of the most interesting periods of my life.

CONTENTS:

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1. INTRODUCTION

1. INTRODUCTION

In this chapter, I introduce the central pillars of my research: why it is important to examine state control of information online (or internet control) and how my study contributes to knowledge. The chapter starts with the outline of a research problem (section 2) and background that sums up the main tactics of internet control (section 3). Then, I discuss why and how I study conditions of state control over information on the internet (section 4). The main point is that my study emerges from a gap in the scholarly literature: there is a lack of studies addressing conditions of internet control. Next, I discuss why my research is important, focusing on contributions to knowledge (section 5). The main contribution is the identification and analysis of conditions leading to state interference with digital information with a particular focus on the post-Soviet region. Another novelty of my approach is that I include democratic states in the study. As I discuss below, democracies are largely absent in internet control studies as the focus is mainly on autocracies and autocrats. Finally, I conclude the chapter by providing the structure of the thesis (section 6).

2. RESEARCH PROBLEM

In August 2013, Alexandra Garmazhapova arrived at a white cottage located in Olgino, Saint Petersburg, seeking employment. She had seen an advertisement on social media for internet operators tasked with writing posts and comments. After successfully passing the interview, Alexandra started her work: her duties included writing one-hundred comments on the internet a day, her first topics were the 2013 G-20 summit and the 2013 Russian law on education. As Alexandra later discovered, the agency she worked for was extensively engaged in publishing critical posts and negative comments about Russian opposition politicians and spreading positive messages praising the Russian president and government. Thanks to Garmazhapova (2013), an undercover journalist of Novaya Gazeta, the world eventually learnt of a factory of paid-for commentators and trolls in Russia that produced the pro-government narrative on the internet, influencing public perception of actual events[1]. As it turned out, the agency, formally called the Internet Research Agency, was well staffed and financed, having close ties to the Kremlin (Chen 2015).

[1] Besides, after probing social media manipulation on the domestic audience, the infamous agency expanded the sphere of operations. Several years later it was accused of interfering in the 2016 presidential elections in the US (Apuzzo and LaFraniere 2018).

While the Internet Research Agency was busy manipulating Russian public opinion, elsewhere in the world an investigative journalist, Maria Ressa, was exposing the Philippines' paid-for trolls and commentators. The latter, in the wake of the 2015 presidential elections, flooded the internet (via bots[2] and fake accounts) with messages promoting and praising Rodrigo Duterte, then one of the presidential candidates, as well as harshly criticising his opponents (Ressa 2016). Yet, after revealing pro-Duterte trolls and disinformation campaigns, Ressa began encountering considerable problems. The journalist and her website (Rappler.com) were investigated by the government while facing attacks and accusations from the same army of online trolls that she previously uncovered (Pomerantsev 2019a). In addition, Ressa was arrested several times and in June 2020 convicted of online libel (Ratcliffe 2020).

Although state-orchestrated manipulation of public opinion on social media and arrests of online journalists and internet users might appear to have little in common, both serve the same goal. Both are considered internet control tactics that states employ to control the digital flow of information within national borders. That is, governments organise an army of paid-for commentators and penalise journalists and users in order to shape and limit information distributed over the internet[3]. In both cases, the focus on and the amount of undesirable information is reduced. Bots and trolls, undermining opposition accounts, switch public attention to pro-government narratives. Meanwhile, it is challenging for an arrested person to publish investigations on the internet from a cell.

Such practices of state interference with the digital flow of information were a result of states' efforts to fight back the impact of the internet on the exchange of information[4]. Consequently, governments' attempts to control information online were generally called internet control[5] (Deibert 2009, Deibert 2015, Signer and Brooking 2018). With the advent and proliferation of digital technologies, internet control has before long become an essential component of national politics. As the example of Ressa above demonstrates, a journalist who crossed the president's path can be penalised and prosecuted for investigative reports published on the internet. However,

[2] Bots are defined as "pieces of software or code designed to mimic human behavior online" (Bradshaw and Howard 2017: 11).

[3] The internet (and cyberspace) in this thesis is understood as "a hierarchical contingent system composed of (1) the physical foundations and infrastructures that enable the cyber playing field, (2) the logical building blocks that support the physical platform and enable services, (3) the information content stored, transmitted, or transformed, and (4) the actors, entities and users with various interest who participate in this arena in various roles" (Choucri 2012: 8).

[4] In chapter 2, I provide more details.

[5] Thus, throughout this thesis, I use "internet control", "control of information online", and "control of the digital flow of information" interchangeably. In these cases, I mean state-based efforts to shape and restrict the digital (online) flow of information within national borders. As the focus on state control of digital information within national borders, I do not study in this thesis states' attempts to control information flows in other countries.

the Philippines, a flawed democracy according to the 2019 Democracy Index (The Economist Intelligence Unit 2020), is not the only country trying to silence journalists along with regular internet users. As I show throughout this thesis, the punishment for online publications – be it an investigative report or merely a critical post on social media – is a common practice in many countries.

The armies of commentators and bots organised and financed by governments and political parties are also not exceptions. Rather, the number of countries, including democracies, where such armies have been reported, has been growing (Bradshaw and Howard 2019). Democratic societies are also not exceptions, becoming vulnerable to state-affiliated manipulation of public opinion. For instance, the 2016 Brexit and the 2020 US presidential elections were both marred by digital propaganda and disinformation campaigns, which affected the public perception of respective events (Nielsen 2018, Coppins 2020). It is thus unsurprising that the body of literature, investigating the phenomena of the increasing number of mobs of bots and trolls inhabiting cyberspace – many of which are associated and financed by government agencies and political parties – grows as well (Benkler et al 2018, Chaturvedi 2019).

The 45th US President Donald Trump’s actions to tame social media giants by trying to revoke Section 230 of the 1996 Communications Decency Act in 2020 (Siripurapu 2020), which provides legal guarantees to tech corporations for content posted on their platforms, also demonstrate that the internet, technological companies, and online content are all on the agenda of political leaders. President’s executive act was a response to perceived censorship of Trump’s social media posts by tech giants, though it has not been successfully implemented as the US social media companies are still protected by Section 230.

Nevertheless, it can be seen that internet control is increasingly in demand in countries across the world and the tendency to apply digital tactics only grows, even at the time of a world health emergency. As I argue in Chapter 5, disturbingly many countries continued to apply information controls while other countries exploited the global Covid-19 pandemic as a chance to extend political powers by employing various tactics of internet control. For instance, Hungary and the Philippines, amidst the outbreak of coronavirus, passed restrictive legislation that limited the freedom of expression online. Meanwhile, other countries, including democratic ones such as India, South Africa, and Malaysia, arrested internet users and journalists for Covid-19-related publications on the internet. Even having their citizens confined in physical spaces during national lockdowns, states keep controlling flows of information within digital spaces.

It is thus no exaggeration to suggest that, once the internet “has turned into another useful tool of power” (Runciman 2018: 155), internet control has become a recurrent feature of contemporary politics. Yet, manipulation of public opinion on social media via paid-for commentators, prosecution of internet users and digital journalists, and attempts to amend internet legislation, like in the examples above, are not the only tools available to states to control the digital domain. As I discuss below, there are plenty of ways for governments to exercise control over the internet.

Moreover, following numerous examples and cases discussed in this thesis, there is little indication that the number of state-employed information controls will decrease in the observable future. Therefore, dynamics of internet control should be carefully studied with the focus being not only on typical case studies (such as China, Russia, and Iran) but also on less known countries and regions (for example, the post-Soviet space). In other words, internet control is going to be with us for a while and, thus, we need to thoroughly study it. For this reason, this thesis attempts to address the issue of state control of the internet from a global and regional (post-Soviet) perspective, attempting to contribute to the growing body of internet control literature (section 5).

3. BACKGROUND: HOW STATES CONTROL INFORMATION ONLINE

In this section, I summarise how governments seek control of the internet. Internet control is defined as state-based efforts to shape and/or restrict the digital flow of information within national borders through the implementation of the following tactics (techniques): censorship of online content, internet disruptions, covert surveillance of communications, cyberattacks, implementation of legislation that expands government's powers in the digital sphere, manipulation and propaganda campaigns, crackdown on journalists and internet users, and/or dominance of internet infrastructure and actors[6].

First, many countries systematically censor online content to control information distributed over the internet[7]. They do it by filtering, deleting, or restricting access to materials and websites they find or perceive threatening to the existing political regime. For instance, China censors materials and posts that could lead to collective action such as protests and demonstrations (King et al 2014) whereas the government of South Korea methodically filters content that propagates and praises North Korea (Volodzko 2019). Ukraine, in the aftermath of the 2014 confrontation with Russia, banned and consequently blocked Russian social networking platforms (Luhn 2017). Uzbekistan, besides restricting access to websites of opposition media, is known for blocking VoIP

[6] This definition is based on studies of internet control (e.g. Deibert et al 2010, Morozov 2012, Deibert 2015).

[7] Censorship of materials related to (child) pornography and copyrights issues is not included in this tactic. In chapters 2 and 4, I provide further details.

(Voice over Internet Protocol) applications and international human rights and news resources[8] (Freedom House Uzbekistan 2018).

States also disrupt or shut down internet and mobile services to affect the dissemination of digital information. For instance, both India and Pakistan are the world leaders in cutting off internet and mobile access within their borders. In 2019 alone, India disconnected the internet in the country 106 times (Internet Shutdown Tracker n/d). In Kazakhstan, government agencies switch off communication networks whenever a political dissident streams on the internet from abroad (Putz 2019). One of the latest internet shutdowns took place in Belarus in August 2020 when the internet became inaccessible for almost three days in the wake of post-election protests (Gallagher 2020). In all these cases, citizens were temporarily left without access to the internet and thus could not communicate and exchange information with one another.

In addition, communications surveillance, usually by installing special security equipment on servers, can be deployed. Surveillance, by enabling state agencies to access users' data, monitor their activities, and extract information flows, has thus become "a very powerful force of information control" (Deibert and Rohozinski 2010a: 9). For example, Russia is known for installing SORM (systems for operative and investigative activities) in internet service providers' (ISP) facilities to intercept, collect and store communications of users. However, democratic regimes are also in the surveillance business (Naughton 2012: 260-261). In 2013, Edward Snowden's disclosures revealed how some western liberal democracies were actively and secretly employing mass surveillance of communications (Curran et al 2016: 126).

Governments, to restrict information flows, also resort to computer attacks that often directed at independent media and individuals. For example, the government of Kazakhstan is believed to infiltrate computers of exiled oppositionists with malicious software (Menn 2016). Meanwhile, the Belarus government reportedly resorts to cyberattacks that target opposition media outlets (Freedom House Belarus 2018). As a result, deactivated websites and hacked dissidents become (temporarily) unable to share information online. The main challenge is, however, the attribution of cyberattacks due to the absence of geographic restrictions on the internet. That is, someone in country A by accessing computers in country B can launch a cyberattack against the infrastructure and/or actors in country C, whose servers might be located in country D (Singer and Friedman 2014: 73). It is thus challenging to trace and detect with undeniable proof those standing behind attacks, creating for states an opportunity of plausible

[8] Only in May 2019, after three years of blocking, many foreign websites became again accessible in Uzbekistan (Putz 2019).

deniability[9]. Moreover, governments can outsource the launch of cyberattacks to third parties given that hackers often work as freelancers (Segal 2016: 55).

To control the digital flow of information within national borders, many states also pass restrictive laws and rules that significantly expand, and in some cases justify, government's sweeping powers in the digital domain. In some post-Soviet countries, for example, the authorities apply anti-extremist legislation to remove allegedly illegal materials distributed on the internet. In Russia, the 2019 law on the autonomous internet, which was passed under the pretext of national security, significantly expanded the state's authority to filter and block online content[10]. In another example, the 2017 Network Enforcement Act in Germany envisages huge fines if social media platforms do not take down illegal content after being notified by the government (Oltermann 2018).

Furthermore, states organise armies of bots and trolls, which shape the flow of information online by influencing public debates and opinions on social media; this was also called "censorship through noise" Pomerantsev (2019b: 37). The Internet Research Agency and Chinese 50-cent army (discussed in the following chapter) are popular examples in the media and internet studies. However, China and Russia are not the only countries resorting to this tactic of internet control. Bradshaw and Howard (2018) revealed that no less than forty-eight countries, including both democracies and autocracies, turned to social media manipulation by 2018. In 2019, the overall number already included seventy states, in which "evidence of organised social media manipulation campaigns" by government agencies and/or political parties was found (Bradshaw and Howard 2019: 2). Information control through noise, in other words, is relatively common across the world.

Another tactic employed by governments is a crackdown on online journalists and internet users by the way of arresting, prosecuting, fining, and/or intimidating them ostensibly for digital activities. The latter, among other things, can include hate speech, calls for protests, or criticism of officials. In this regard, the main goal "is to threaten and frighten people into inaction and silence" (Lacy and Mookherjee 2020: 294), thereby decreasing the amount of potentially negative information. The penalty for internet activities can vary from detainment to lengthy imprisonment to even death. For instance, in 2017 in Thailand, a man was sentenced to thirty-five years for publishing posts on social media that were interpreted as insulting the monarch (The Guardian 2017). In a

[9] Nevertheless, it is sometimes possible to build a probable case of attribution based on intelligence and other evidence like it happened with the attribution of cyberattacks on Sony Entertainment to North Korea (Global Commission on Internet Governance 2016: 71, Lacy and Prince 2018).

[10] Officially, the law was adopted to protect critically important web services in case of switching Russia off the global internet and thus make the Runet more autonomous (BBC 2019).

more extreme example, in 2017 in Pakistan, for the first time, an internet user was sentenced to death for making allegedly blasphemous comments on social media (Rasmussen 2017).

Finally, states also attempt to dominate the physical infrastructure to control information online. Exchange points and service providers tend to be the main targets. Governments can either put pressure on ISPs through a strict legal framework or by simply financing them. Many state-owned telecommunication and internet providers operate and dominate the ICT market in their respective countries. For instance, as I showcase in chapters 6 and 7, the Kazakhstan government owns the main internet provider outright whereas in Ukraine the local authorities influence internet actors via legislative acts. In both cases, governments have obtained necessary leverage over private operators and can ask them to block websites and disrupt communications whenever needed.

Overall, these are the main tactics employed by states to control the digital flow of information within national borders. Consequently, the issue of internet control was extensively analysed in the scholarly literature (Deibert 2015, Hussain et al 2013). In the following section, I discuss why we still need to study control of information on the internet.

4. WHY STUDY INTERNET CONTROL?

As noted in the previous section, numerous tools of internet control have been examined by scholars. However, there is a lack of studies of possible factors leading to government interference with information distributed over the internet. The latter, unlike tactics, have not been thoroughly addressed in the scholarly literature. Consequently, this thesis, in addition to tactics, also addresses conditions of state control over digital information. I study how and under what conditions countries shape and restrict the online flow of information.

In addition, as examples in the previous section demonstrate, both autocracies and democracies tend to resort to internet control tactics. Nevertheless, scholars (e.g. Roberts 2018, Singer and Brooking 2018) focus largely on authoritarian regimes as actors and initiators of internet control (China, Russia, and Iran are the main examples). Analyses of how democratic states employ various tactics to control information online are either absent or inconsistent[11]. As I discuss in the literature review (chapter 2), scholars examine either all tactics of internet control in authoritarian countries (Deibert

[11] I do not consider censorship or blocking of content related to (child) pornography and copyrights issues as part of internet control. In chapters 3 and 4, I provide additional details.

2015, Roberts 2018) or only one tactic (such as surveillance of communications or social media propaganda) in democracies (Hintz and Milan 2018, Bradshaw and Howard 2017). As a result, although it is known that democratic states resort to some information controls, the extent of their interference with information on the internet has not been systematically studied.

My study considers these gaps in the literature. I examine conditions leading to state control over the online flow of information, focusing on both authoritarian and democratic countries. The research question is thus related to the identification and analysis of conditions of internet control. The main proposition is that the logic of political survival shapes the extent to which governments and their executives can control digital information. As survival strategies of political leaders are defined by the nature of political institutions (Bueno de Mesquita et al 2003, Acemoglu and Robinson 2013), I started with the following assumptions. First, the extent of internet control is substantial in countries with extractive (authoritarian) political institutions, in which a small group of people holds all political power in their hands, having no restrictions to dominate the digital sphere. Second, and conversely, internet control is limited (but not absent) in countries with inclusive (democratic) institutions, in which the political authority of executives is constrained.

Consequently, I conduct a comparative analysis of sixty-five countries (the first research objective) followed by the case studies of two countries, Kazakhstan and Ukraine (the second research objective), to test the outlined propositions and address the research question. Combined together, these two steps allow for a more thorough examination of tactics and conditions of internet control, broadening the scope for research and, as I discuss in the following section, contributing to knowledge.

5. CONTRIBUTIONS OF THE STUDY

There are no recent studies that have comprehensively covered both: all main tactics of internet control and democracies. Those examinations that included both (e.g. Deibert et al 2012b, Hussain et al 2013) have not been updated[12]. Thus, building on the existing gaps in the scholarly literature, one of my contributions to knowledge is a comparative analysis of all main tactics of internet control in both autocratic and democratic states. Overall, I study sixty-five countries that altogether comprise almost 90% of world internet users, covering incidents of internet control from 2016 to 2018. When necessary, state-employed tactics before and after the coverage period are also considered. For instance,

[12] For example, Deibert et al' (2012b) study covers incidents of internet control in 2009-2010; Hussain et al (2013) also examine state interference with the internet until 2010. In chapter 2, I discuss other limitations of internet control studies.

to broaden the analysis, I include the discussion of state interference with digital information during the current global Covid-19 pandemic.

By utilising a comparative analysis of authoritarian and democratic countries as a preliminary step, I identify main patterns of state control over information on the internet. After that, I further scrutinise conditions of internet control, conducting two case studies of post-Soviet Kazakhstan and Ukraine. The case studies, the second and final step of the study, supplementing the main findings drawn from the comparative analysis, also aim to provide more refined conclusions. This shall deepen my study of internet control.

Also, as I argue in the following chapter, there is a tendency among scholars to neglect and disregard cases of internet control in democracies. Instead, pundits, often almost exclusively, focus on how authoritarian regimes employ numerous tactics to control the internet. China, Iran, and Russia are the main case studies from which conclusions about the authoritarian nature of internet control are drawn (Roberts 2018, Singer and Brooking 2018). Most importantly, based on their findings drawn from a hardly representative sample, scholars extend their conclusions to the rest of the world. For example, Roberts (2018) extensively investigates how the Chinese government shapes and restricts the digital flow of information, identifying three main tactics of control (fear, friction, and flood). Yet, the author – although continuously mentions but later neglects examples of internet control tactics implemented by democracies – exceptionally applies identified patterns of digital control to all other authoritarian countries. That is, democracies are discussed as actors and initiators of internet control, but the author's conclusion is still that it is only authoritarian regimes that shape and restrict digital information.

Despite such a contradiction, the tendency to consistently highlight the authoritarian nature of digital control is commonplace in the literature. For instance, Deibert (2015) also identifies various tactics of internet control[13] and, like Roberts (2018), attributes them solely to authoritarian governments. Although the author acknowledges that democracies and hybrid regimes, too, shape and limit information online, the conclusion is that cyberspace is solely under the authoritarian regimes' command. As I discuss in Chapter 2, such a tendency to attribute information controls predominantly to the orbit of authoritarian states – while democracies are overlooked by default – is widespread in internet control scholarship (Clarke and Knake 2019, Kendall-Taylor et al 2020, Rosenberger 2020). This is not to say that authoritarian regimes do not control the internet but that democracies cannot be disregarded in (comparative) studies of digital

[13] I discuss Deibert's (2015) classification of internet control in detail in Chapter 2.

control. That is, both democratic and non-democratic polities should be considered when we study the dynamics of internet control globally.

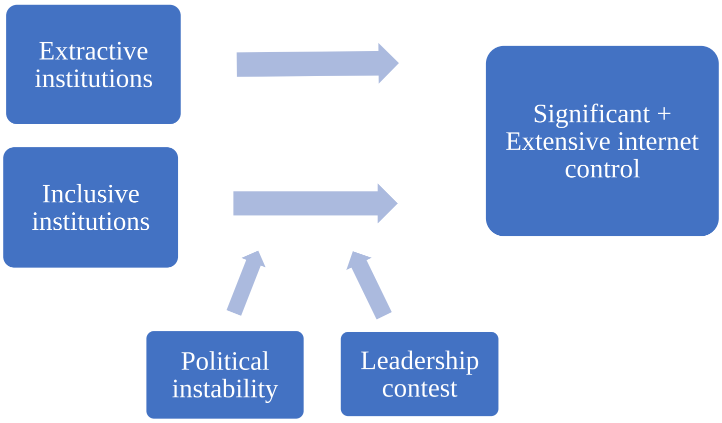
Besides the overconcentration on digital authoritarianism, there is also a tendency to focus on the same cases. As noted above, China, Russia, and Iran are the most referred (and probably the most obvious) examples of state control over the digital domain. Meanwhile, no less interesting cases all over the world are neglected to a great extent. As this thesis posits, the post-Soviet region tends to be specifically underemphasized in the literature. Apart from Russia, the remaining fourteen post-Soviet countries are scarcely discussed in internet control scholarship. Yet, as I demonstrate in Chapters 6 and 7, former Soviet Union republics are particularly well-versed in imposing information controls. For example, Kazakhstan is no less experienced than China and Russia in controlling the digital domain within national borders. All the main tactics discussed in section 3 above are routinely employed in the country: online content is thoroughly censored, websites are routinely blocked, both internet and mobile access are timely disrupted, state's unrestrained surveillance capabilities are deployed, restrictive digital laws are swiftly passed, pro-government online mobs of trolls and bots to manipulate public opinion are widely used, and ordinary internet users and journalists are systematically persecuted and prosecuted. In other words, the extent of state internet control in post-Soviet Kazakhstan is comprehensive.

Ukraine, sandwiched between Russia and European states, is another neglected in the literature post-Soviet country that is well-versed in controlling the internet. Despite having the democratic EU as a neighbor, the extent of internet control in Ukraine has been extended since 2014. As I demonstrate in Chapter 7, after Russia annexed the Crimean peninsula at the beginning of 2014, Ukrainian authorities, like in Kazakhstan, have been methodically applying numerous tactics to strictly control the digital domain. Moreover, information controls have been employed in Ukraine despite the inclusive nature of domestic political institutions.

In short, both Kazakhstan and Ukraine serve as great examples to study specifics of state control over the internet. For this reason, after critically reviewing the literature (Chapter 2), the research focus is upon the post-Soviet region (Chapters 6 and 7). Given the striking regularity of the post-Soviet authorities' masterful employment of digital control tactics and yet an appalling lack of studies of the post-Soviet experience, this thesis attempts to contribute to the literature by exploring and shedding light on the less obvious but highly telling cases of state control of the internet. Apart from Russia, China, and Iran, other countries – especially democracies and hybrid regimes like Ukraine – that extensively shape and limit the digital flow of information should not be overlooked.

The scope of internet control scholarship should be broadened if we want to know how the internet is controlled across the world.

Figure 1. Model of conditions of internet control



Ultimately, the combination of levels of analysis (a global comparative analysis and the case studies of post-Soviet Kazakhstan and Ukraine) helps to explore conditions of internet control – another key contribution of my research. Consequently, I found the following main conditions leading to state control over the online flow of information (Figure 1). The first is the extractive (authoritarian) nature of political institutions. The second is political instability, which can be provoked by various political crises including the coronavirus outbreak, and/or a forthcoming leadership contest in the form of presidential or parliamentary elections in countries with inclusive (democratic) institutional settings. Under these conditions, governments appeared to shape and restrict digital information within national borders.

Last but not least, this thesis draws insights from positivist traditions and institutional theory of political science, focusing on observable patterns of state behavior. In terms of state-employed information controls, we can know whether an internet control tactic was employed by observing its occurrence or non-occurrence. For instance, if internet connection is disrupted in a country, we can see consequences of such disruption. After studying the details of the incident, we can (in most cases) conclude whether the internet was disconnected due to the government authorities' deliberate action or a technical bug. Consequently, after collecting and analysing data, we can identify various patterns and regularities of how states approach and treat the digital domain.

Although the thesis is grounded in a positivist epistemology to a great extent[14], in both case studies the focus is also on non-observable phenomena. I draw attention to how governments in both Kazakhstan and Ukraine attempt to manipulate the political discourse (of internet control) by promoting state narratives. In both countries, for instance, authorities justify the heavy regulation of communication and information spheres through different state programs and concepts.

In terms of the disciplinary location, this study contributes to a field of political science. The thesis, by applying a comparative method (Ragin 2008) and drawing insights from institutional theory (Peters 2019), analyses whether political institutions are an essential component of state-employed tactics of internet control on a global scale (Chapter 5). Besides, this study traces the evolution of political institutions and the balance of domestic political power in two post-Soviet countries in order to see to what extent local and regional politics affect the employment of information controls.

6. STRUCTURE OF THE THESIS

The structure of the thesis is as follows. In *chapter 2*, I review the literature that addresses tactics and conditions of internet control. Two common patterns were consequently found. The first one is a tendency to emphasise the authoritarian nature of control over digital information, neglecting the employment of same information controls by democratic states. Scholars (e.g. Deibert 2015, Singer and Brooking 2018, Kendall-Taylor et al 2020), as a result, conclude that it is the authoritarians who control the dissemination of information online, implicitly assuming that democratic leaders do not shape or restrict information flows. However, as discovered in a comparative study (chapter 5), such a view is only partially correct. Another pattern in the internet control literature is a lack of studies addressing conditions of control over digital information. Pundits focus on what and how states control information online, whereas underlying conditions leading to internet control have not been thoroughly examined. Yet, it is still possible to suggest the logic of political survival as the main factor driving many countries to apply internet control tactics (Wagner 2018, Roberts 2018).

Drawing from the literature and building on the identified gaps, the assumption of political survival as the main condition of internet control is further developed. In *chapter 3*, drawing insights from institutional theory, I hold that the nature of political institutions shapes survival strategies of those in power (Bueno de Mesquita et al 2003, Acemoglu

[14] It is, however, of note that the author of this thesis supports the view, which holds that ontological and epistemological positions are rather a sweater, not a skin (Moses and Knutsen 2012, Peters 2019). That is, the choice of theories, methods, and ontological and epistemological positions can vary depending on a research problem, context, and aims.

and Robinson 2013). Hence, institutions, by structuring the logic of political survival, affect the extent of internet control within national borders. Overall, I distinguish between two main types of institutions: extractive and inclusive, which are associated with authoritarian and democratic polities, respectively. Consequently, the initial research propositions maintain that extractive institutional settings are conducive to a high number of state-employed information controls whereas inclusive institutions lead to a limited extent of state interference with digital information[15].

In *chapter 4*, before testing the outlined propositions, I discuss the research design. In particular, I consider a method of the qualitative comparative analysis advanced by Ragin (2000, 2008), which is used to unravel the possible causal relations between the proposed condition (the nature of political institutions) and the expected outcome (the extent of internet control). I also formulate the research questions, objectives, and hypotheses and provide the definition, operationalisation, and calibration of the main concepts of the study. In addition, I develop a model of internet control to study the extent of state control over the online flow of information. Finally, I explain how two case studies are conducted.

After explaining how research variables are defined and measured and what method is applied, I proceed to a comparative analysis. In *chapter 5*, I examine the proposed causal relations between political institutions and internet control in sixty-five countries. After identifying the nature of political institutions and the extent of internet control (defined and operationalised in chapter 4) in analysed countries, I can test the research propositions. As a result, I confirm the first proposition that extractive institutions lead to substantial control of information on the internet (that is, more tactics are employed). However, I do not find sufficient evidence that inclusive institutional settings are conducive to limited control over digital information (that is, fewer tactics are used). Rather, under additional conditions such as political instability and/or a leadership contest, many countries with inclusive institutions tend to resort to internet control tactics almost as often as countries with extractive institutions. Thus, following these findings, I refine the research propositions.

Consequently, a case study of Kazakhstan is conducted to scrutinise the first (confirmed) proposition that extractive institutional settings lead to extensive control of information online. In *chapter 6*, I analyse the development of political institutions in Kazakhstan that have become irrevocably extractive. As a result of that transformation,

[15] Although it was known that democracies resort to some tactics (such as communications surveillance and social media propaganda), the extent of their control over digital information was not yet established. Thus, the initial proposition is that internet control is limited (but not absent as many internet studies assumed).

the Kazakh authorities turned to comprehensive control of the internet within national borders. In other words, the “rules of the political game” in Kazakhstan were changed to the advantage of a few, who seized all political power in the country and, subsequently, resorted to internet control tactics to further hold onto power (that is, to secure political survival).

In addition, I conduct a case study of Ukraine to explore the second (refined) proposition that countries with inclusive institutions, under additional conditions, also substantially control information flows. In *chapter 7*, I analyse the development of political institutions in Ukraine, which since the Soviet Union’s collapse became and continue to be inclusive. Political power in the country is fairly distributed, the Parliament and civil society are strong whereas the President’s executive authority is circumscribed. As a result, state interference in the digital sphere was limited. However, in 2014, in the wake of the acute political crisis caused by a regional conflict with Russia, the extent of government control over digital information was significantly expanded. Ukraine’s authorities, despite the inclusive nature of political institutions, applied numerous tactics to control information distributed over the internet.

After combining a comparative analysis of sixty-five countries and two case studies, I was able to explore and refine conditions of internet control. As a result, two causal paths leading to substantial control over information on the internet were found. The *first* path is the extractive nature of political institutions. The *second* path is political instability and/or forthcoming elections in countries with inclusive institutions[16]. In this regard, my research helps to broaden the scholarly literature, which tends to focus on autocracies and (explicitly or implicitly) assume that democracies do not resort to internet control. My analysis demonstrates that studies that do not consider democracies as actors and initiators of internet control offer only a partial perspective of the issue under consideration. This is because, in practice, many democratic governments appeared to systematically shape and restrict the digital flow of information. Thus, the inclusion of democratic states in the analysis secured a more comprehensive view, contributing to a better understanding of the dynamics of state engagement with the internet within national borders.

[16] In addition, I did not find sufficient evidence to support the assumption that inclusive institutions are conducive to limited control of information on the internet.

CHAPTER 2. LITERATURE REVIEW: INTERNET CONTROL

1. INTRODUCTION

This chapter provides a critical review of the literature that examines tactics and conditions of internet control. Before proceeding to the review, I first account for how the internet has been perceived by scholars and observers (section 2). Initially, the internet was widely believed to be a revolutionary technology that would irrevocably change our society (Negroponte 1995, Gilder 2000) and significantly undermine state control of information flows (Wright 2000, Kristof 2005). These early optimistic hopes faded but the internet was still viewed as a liberating tool able to enhance democracy and open oppressed societies by allowing the activists to expose dictators' wrongdoings via social media (Diamond 2012, Howard and Hussain 2013). On the other hand, there have been more sceptical conclusions about the internet's potential to challenge state monopoly over information, seeing information and communication technologies as empowering governments rather than citizens (Morozov 2011, Curran et al 2016). Yet, notwithstanding the internet's real impact on governments and society, many states have eventually sought to tame the new technology.

After providing the background information, I review the literature that discusses how governments have adapted to a new environment, opting to control information on the internet (section 3). Overall, there are many tools at the state's disposal to affect the dissemination of digital information within national borders. These include censorship of online content, shutdown of communication networks, social media manipulation, arrests of internet users, covert surveillance and cyberattacks, restrictive legal framework, and dominance of domestic internet infrastructure. These tactics of internet control have been classified in numerous ways (Deibert 2015, Sanovich et al 2018, Hussain et al 2013). However, regardless of how information controls are categorised (i.e. into different generations, mechanisms, tools), they separately or in concert shape the digital flow of information.

In addition to exploring how governments seek to control information online, I discuss a common pattern in the literature (section 3). In particular, there is a tendency to attribute internet control tactics solely to authoritarian states. Many scholars (e.g. Deibert 2015, Roberts 2018, Singer and Brooking 2018) conclude that it is authoritarian regimes that control information distributed over the internet. Yet, the same scholars also provide examples of the implementation of information controls by democracies. The authors, nevertheless, discuss the resurgence and resilience of authoritarian countries, being aware of but overlooking practices of internet control within democratic settings. Consequently, such an approach can lead to a partial and thus distorted perspective of the topic under consideration, given that democracies also tend to shape and restrict the digital flow of information.

Although there are some exceptions in the literature (e.g. Hintz and Milan 2018, Bradshaw and Howard 2017), only one of numerous tactics (such as mass surveillance and its implications for human rights or manipulation of public opinion on social media) that was employed by democracies has been analysed. That is, *all* main information controls (listed above) have not been recently studied within both autocratic and democratic countries.

As a result of focusing on internet control within mainly the authoritarian context, there is also a lack of research on conditions of control over digital information (section 3). Few pundits have addressed possible conditions that prompted some governments to implement (or to not implement) internet control tactics, though their analyses are either brief (Deibert et al 2010) or drawn from one case-study (Sanovich et al 2018). Nevertheless, it is possible to arrive at a common denominator behind control over information flows, which is the logic of political survival of those in power. For example, Wagner (2018) has identified that when the government of Pakistan felt pressured by political opposition, it resorted to shutdowns of communications in some regions to limit the dissemination of information online. Yet, given the lack of studies in this particular direction, the assumption of political survival is to be tested and possibly refined (chapters 3-5).

2. BACKGROUND: THE INTERNET, INFORMATION, AND DEMOCRACY

The internet has transformed the way people communicate, consume, and distribute information. This became possible because the internet, unlike the traditional information sources of “one-to-many” such as newspapers, radio, and TV, allows a fast information exchange from “many-to-many” at the same time[17] (Nye 2011: 116). In addition, traditional media is prone to influence from editors, owners, and governments whereas the internet enables instantaneous communication and the dissemination of information with less intermediaries. That is, if state authorities could previously control information flows by exerting influence over the media, now the public has become able to directly transmit stories bypassing one of the important tiers (Roberts 2018: 36). In other words, the internet has “changed the structure of communication by allowing individual users to broadcast information” (Tucker et al 2017: 48), creating a new information environment.

[17] As Jordan notes, “prior to the internet the idea of many-to-many communication was rarely if ever possible” (2015: 19).

Moreover, what makes the internet specifically unique, though it was not the first innovation deemed to change the world[18] (Spar 2001), is that "no other technology in history has grown with such speed and spread so far geographically in such a short period of time" (Deibert and Rohozinski 2010c: 43). Indeed, within less than three decades internet access[19] has reached more than half of the world population (4.1 billion users by 2019), according to the International Telecommunication Union's (2019) estimations[20]. In 2001, for comparison, only 8 people out of 100 had access to the internet. The share of developing countries has also increased, constituting currently almost three-quarters (3 billion) of all internet users. Out of all 4.1 billion internet users, around 2.7 billion have active Facebook accounts (Statista 2020) – an impressive achievement for a company created in 2004. Twitter, another social media platform created in 2006, has also become increasingly popular. Currently, 500 million "tweets" are sent every day, making 200 billion posts a year (Internet Live Stats n/d). YouTube, a video platform launched in 2005, has 2 billion logged-in monthly users who cumulatively watch billions of hours of video every day (YouTube n/d).

In other words, the use of the internet has become pervasive. In essence, we stepped into the age of "digital citizenship" in which digital platforms and devices have practically become embedded into our life (Hintz et al 2019). At the same time, a new technology, significantly affecting the information and communication structure, has attracted considerable interest from researchers, media and business figures, and officials. Below, I discuss two broad approaches – more optimistic and more pessimistic – to considering the internet's impact on politics and society.

2.1. Cyber-optimism

The initial rhetoric about the internet was highly optimistic, perceiving it (due to its decentralised structure) as a revolutionary technology that would transform society, as Negroponte predicted, "beyond people's wildest predictions" (1995: 231). Negroponte also foresaw a digital future where "physical space will be irrelevant" (1995: 7), diminishing the value of nation-states and that being digital would draw "people into greater world harmony" (1995: 230). Gilder (2000: 2), for another example, compared internet-enabled immediate communications with angels from the Bible, who also promptly pass through space and time, predicting a forthcoming paradise – the "telecosm". The world will be united and defined by the internet, according to Gilder.

[18] For instance, telegraph was also thought to irrevocably transform society, politics, and international relations.

[19] Although the internet was created in 1969, it became available to mass users in the beginning of the 1990s.

[20] All numbers of internet access are taken from the International Telecommunication Union.

Evidently, there was no lack of utopian prophesies at the beginning of the internet's global expansion.

In addition to anticipating the internet to irrevocably change our lives, scholars also examined the interplay between the new information technology and politics[21] (Bimber 1998). For example, pundits studied the benefits and shortcomings of electronic democracy (Browning 1996, Tsagarousianou et al 1998) and the internet's potential to enhance democratic practices (Tambini 1999). Gibson et al (2003) explored how political parties in the US and UK used the internet for campaigns' purposes. Castells (2015) analysed internet-empowered political activism in democracies, focusing on numerous anti-establishment protest movements in Europe and the US, while Lacy and Prince (2013) discussed how individuals used and would use new technologies for digital disruption – internet-enabled riots, movements, and social action.

Researchers considering the internet's impact were also keen to ponder its role in non-free societies, in particular how the new information technology could make the world freer. Wriston (1997) argued that the internet, by shaping national sovereignty, international economy, and military capabilities, enabled citizens to watch governments. Meanwhile, "the virus of freedom, for which there is no antidote, is spread by electronic networks to the four corners of the earth" (Wriston 1997: 172). Similarly, Wright (2000) opined that the internet, empowering society and undermining government's control over information, results in the expansion of economic and political liberties in the world. The new information technology was regarded as a tool that can promote democracy in dictatorships as the internet empowers civic activism, providing new opportunities such as "reports on atrocities, calls for nonviolent actions, polls, virtual elections, identification of individual oppressors, ridicule of dictators, attacks on corruption" (Palmer 2003: 78). Likewise, Kristof (2005) was confident that the internet would bring the Chinese communist rule to an end as blogs increasingly exposed wrongdoings of corrupted officials, undermining state monopoly over information. He reasoned that the Chinese government would eventually not be able to control cyberspace due to the growing number of local users, who would disseminate investigative reports online. The use of the internet, thus, would lead to the democratisation of closed societies.

In other words, many pundits and commentators alike anticipated that the internet, given its decentralised structure, could not be controlled by governments and thus would enhance representative democracy and liberate authoritarian countries,

[21] My goal is not to review all effects of the internet but those that (arguably) led to internet control. Other studies, for example, extensively cover the internet's impact on electoral politics (Anstead and Chadwick 2009, Davis et al 2009), the peculiarities of global internet governance (Mueller 2002, 2010, DeNardis 2014), and cybersecurity issues (Stevens 2015, Lacy and Prince 2018, Cavelty 2009) and the interplay between new technologies and security (Lacy 2014).

bringing freedom to oppressed societies. Politicians, too, held similar views. US President Bill Clinton, for instance, believed that control over the internet would be useless, famously comparing it to attempts to "nail Jell-O to the wall" (The Economist 2013). In addition to theoretical deliberations though, there have been more empirically grounded studies of the democratising agency of the internet. For example, Howard (2010) conducted a comparative analysis of the role of information and communication technologies (ICTs) in democratic transitions and entrenchment of seventy-five countries with a considerable Muslim population. He concluded that the diffusion of technologies contributes to the democratisation.

Relatedly, pundits studied how digital technologies such as the internet and mobile phones can solve collective action problems and enable political activism, contributing to the expansion of freedom in the world. In particular, Diamond (2010, 2012), emphasising the liberating potential of digital technologies, argues that the internet has become associated with the promotion of democracy by empowering opposition movements worldwide. Diamond states that ICTs allow individuals "to report news, expose wrongdoing, express opinions, mobilize protest, monitor elections, scrutinize government, deepen participation, and expand the horizons of freedom" (2010: 70-71). Although the author acknowledges that authoritarian regimes can exploit the same technologies for repression and control, activists still can depose dictators with the help of ICTs. In other words, nothing would stop protesters from swaying oppressive regimes if a liberation technology were used in a proper and smart way.

Similarly, Deibert and Rohozinski (2010b) and Howard (2010) contend that ICTs played an important role in coordinating and mobilising protesters – mobile phones during the post-Soviet "colour revolutions"[22] and social media applications in the 2009 Iran protests, respectively. For instance, Howard maintains that in 2009 – when social media platforms were relatively popular – protesters in Iran, dissatisfied with the results of the presidential elections, "had access to an information infrastructure largely independent of the state" and equipped with ICTs were able to "spread the news of electoral fraud and escalating tensions" (2010: 3). As a result, the user-generated content was distributed between citizens and reached the international community.

Furthermore, the concern over the potential of information and communication technologies to promote democracy and combat dictatorships has been boosted after the 2011 Arab Spring. For instance, according to Howard and Hussain (2013: 120), the Middle East uprisings were empowered through the use of digital media. The authors state that unrests extended over the Arab countries "largely because digital media

[22] The "Orange revolution" in Ukraine in 2004 and the "Tulip revolution" in Kyrgyzstan in 2005.

allowed communities to realize that they shared grievances and because they nurtured transportable strategies for mobilizing against dictators" (Howard and Hussain 2013: 3). Tufekci and Wilson (2012), drawing from 1 050 surveys, also concluded that social media significantly contributed to the 2011 street protests in Egypt. They found that more than half (51%) of surveyed participants used Facebook for communicating about the protests and more than a quarter (28%) had initially learnt of the protests on Facebook.

As a result, following the numerous protests, new digital technology was dubbed a liberation technology (Diamond 2010) while the Middle East uprisings were called in the press the Twitter or Facebook revolutions (Reed 2014: 126). The role of social media platforms in oppressed societies was perceived to be exceedingly crucial, even leading to the suggestion to award Twitter the Nobel Peace Prize (Pfeifle 2009). Nevertheless, not all scholars and observers shared an optimistic view of the internet's potential to undermine the authority of governments. There have been more sceptical considerations of new technology, which are reviewed in the following sub-section.

2.2. Cyber-pessimism

The internet since its advent was widely believed to hold the potent democratising potential that would bring about positive changes in society, empowering citizens and diminishing the role of governments regardless of the geographical location. This faith in the internet as a democratiser originated partly from the libertarian culture[23] that surrounded the internet's development in the 1990s (Kalathil and Boas 2003). Besides, a belief that big powers' (such as the Soviet Union) failure to shape and limit "the flow of electronic information" (ibid, 2) led to the decline of their influence also contributed to the optimistic perception of technologies. Yet, despite the widespread conviction about the liberating agency of digital technologies, there have been less optimistic voices, seeing the internet's role as exaggerated.

Sceptical views were expressed from the beginning of the internet's expansion across the world. Wu and Weaver (1996), for instance, claimed that new possibilities facilitated by the internet at the time were not necessarily beneficial for democracy. In particular, they identified several flaws of online polls in the US, which were deemed to expand democratic practices, concluding that such methods "cannot, however, measure general public opinion or preference in any reliable or valid manner" (Wu and Weaver 1996: 82). Lipow and Seyd (1996), concerned with the internet-determinist direction of

[23] Libertarianism is a philosophy, rooted in anarchism, that argues against the expansion and intervention of government into various spheres of life, including cyberspace, and promotes liberty as a crucial principle. This view was incorporated in "A Declaration of the Independence of Cyberspace" (Barlow 1996).

scholarly debate, also argued against electronic democracy. Their main argument was that the advent of online political participation would undermine the centrality of political parties, which are a crucial part of the democratic system. In addition, Kalathil and Boas' (2003) analysis of internet politics in eight authoritarian countries demonstrated that early hopes about the democratising impact of the internet were not completely justified as governments had been able to adapt to a new environment, resorting to numerous tactics to control information flows.

Morozov, in turn, calls all this dispute surrounding internet's powers cyber-utopianism – "a naïve belief in the emancipatory nature of online communication that rests on a stubborn refusal to acknowledge its downside" (2011: xiii). Cyber-utopianism, according to Morozov, "overstates the positive role that corporations [such as Twitter, Facebook, Microsoft, and Google] play in democratizing the world without subjecting them to the scrutiny" (2011: 21). Instead, he doubts political power of the internet, questioning the transparency of business-oriented tech giants that own social media websites. Similarly, Siapera (2018), also sceptical about the internet's democratising potential, argues that political entities "use the internet for their own purposes, such as promotion, persuasion, campaigning, administration and so on, rather than to allow citizens to communicate and participate directly in the political process" (2018: 49).

With regard to internet-empowered political engagement, Gladwell (2010) maintains that activism requires strongly motivated participants, that is, those with strong connections with each other and to the cause. Social media is, in contrast, based on weak ties (when Facebook "friends" and Twitter "followers" and the "followed" might not ever meet in person). Another flaw of networks enabled by the internet is a lack of hierarchy and leadership that, according to the author, are needed to organise effective opposition movements. Thus, weakly connected and leaderless social media activism might be great for low-risk activities (e.g. finding a donor or fund-raising) that do not ask for great sacrifices but would be inappropriate for highly risky actions of political change.

Although the formation of groups has become much easier in the internet age (Shirky 2008), Morozov (2011: 188) also argues that, due to the lack of both strong ties between the members and true commitment to the cause, it is a difficult task to ask people for sacrifices on behalf of those groups. Thus, the participants' and groups' number can be high but a political impact is negligible. In addition, another flip side of internet-enabled political activism is "clicktivism" (Siapera 2018: 60). The latter refers to users' superficial actions that are merely reduced to clicking on a link to demonstrate the adherence to the cause of digital activism but leading to no significant results outside cyberspace.

Meanwhile, Esfandiari (2010) holds that there was no Twitter revolution in Iran in 2009 as many protest-related posts in English were authored by people from the West. Also, although social media helped bring international attention to the post-election events, it led to the spread of rumours while the Iranian government managed to use the same web platform to arrest oppositionists. Esfandiari's conclusion is thus that Twitter's role in Iran was significantly overrated. Instead, she argues, "word of mouth" was the main communication tool to influence opposition movements. Morozov (2011), too, argues that it is challenging to conclusively establish the causality between Twitter and the 2009 protests in Iran. This is because it is hard to precisely identify the number of posts published from Iran itself (as those who sympathised with protesters were changing their location to Tehran) and whether Twitter was indeed used for organising opposition forces or simply to inform about events.

In the same manner, Lynch (2011: 303) is careful with the assessment of the internet's role in the Arab Spring, stating that "political anger over heavily manipulated elections … [and] a rapidly deteriorating economic situation" were more crucial factors. Also, the author maintains that the main weakness of social media-mobilised movements is the absence of leaders that are much needed to negotiate and arrange the transition and post-regime affairs. That is, protesting organisations of citizens empowered by the new information technology do not always evolve into governing political parties. Curran et al (2016) are also less optimistic, asserting that digital technologies did not significantly contribute to the "explosion" of the Middle East in 2010-11 since internet access was low in the region at the time. Instead, other factors such as increasing opposition to existed regimes fuelled by "deep-seated political, economic, cultural and religious causes" (Curran et al 2016: 68) mostly instigated protests[24].

Consequently, it can be seen that the perception of the internet varies from highly optimistic to very sceptical. Nevertheless, regardless of the real impact of digital technology, many governments appeared to be suspicious of the internet's liberating potential. For instance, political leaders in Iran bought into the bluff created by western media and policymakers about Twitter's and, respectively, bloggers' powers to bring about political changes (Morozov 2011: 25-26). As a result, the authorities began considering the internet in a more precarious way, adapting to a new information environment. One of the consequences could be the decision to boost the sentiments in support of the regime as "two weeks after the protests began, the number of pro-

[24] Curran et al (2016: 203) also argue that the internet's impact and role are context specific. That is why the early hopes that the new information technology would transform society and promote democracy across the world did not come true as those predictions did not account for a context in which the internet has been used (ibid).

government messages on Twitter increased two-hundred-fold compared with the period immediately after the election" (Morozov 2011: 135).

In Russia, the internet after the Arab Spring was referred to by the leadership as a threat to national security (Vendil Pallin 2017: 19) while the Russian president mentioned the internet as a CIA project (Rayman 2014). Moreover, Russia, too, suffered from the mass street anti-government protests in December 2011, in which social media was credited with the organisation and coordination of protesters (Moore 2018: 86-87, Oates 2013). In addition, Moore (2018: xi) contends that Russia, China, and Iran after the Arab Spring "sought to tame and domesticate the net". Other scholars (Deibert et al 2010, Morozov 2011) have similarly argued that the internet is not uncontrolled and apart from empowering people can be exploited by governments for their own purposes (for example, for surveillance and propaganda) (all these tactics are discussed below).

Yet, the fact that governments have eventually opted to control a new technology is not novel. Every breakthrough technology has in the end come under the state's close supervision. Before the internet's emergence, for instance, other technologies such as the printing press, telegraph, radio, and television were deemed to challenge the status quo, diminishing the governments' authority[25] (Spar 2001). Similarly, these innovations, like the internet, seemed to be uncontrollable. Although challenging governments for some time, all these technologies eventually found themselves under the rules of governments (ibid). In this regard, the internet appears to be no exception as many countries have sought to control information online within their borders. In what way they have attempted to achieve that goal and what has led them to control the internet in the first place are discussed in the following section.

3. INTERNET CONTROL

Scholars (Deibert 2015, Roberts 2018, Singer and Brooking 2018) have provided numerous classifications, which outline how states seek to control digital information[26]. Despite being divided into various generations, mechanisms, and categories, it is possible to distinguish the same cohort of state-employed tactics of internet control (sub-

[25] In chapter 3, I discuss in more detail how various technological innovations were deemed to challenge the state.

[26] I do not focus on regulation and control of all information distributed over the internet. This is because it is a normal practice that "[e]very state regulates the flow of information within and across its borders to some degree ... The United States, for example, regulates content it deems harmful to society, such as child pornography and online gambling. It also regulates the sharing of copyrighted materials" (Powers and Jablonski 2015: 5). Similarly, Diamond (2012: xi-xii) agrees that "regulation should [not] be absent, but rather that it should be carefully constrained – used to protect intellectual property rights and shield vulnerable groups such as children". Consequently, I do not consider control and censorship of content related to (child) pornography and copyrights protection issues as part of state control of information flows.

section 3.1.). It is also possible to recognise a common approach in the literature, which is a tendency to address the issue of internet control through strict lines between political systems (sub-sections 3.2. and 3.3.). Scholars (e.g. Deibert 2015, Roberts 2018) conclude that it is authoritarian regimes that employ different tactics to control the online flow of information, though the same scholars also provide examples of how democracies resort to internet control. Although practices of internet control in democracies are thus acknowledged, they are omitted in the following analyses and conclusions. Instead, the authors focus on implications and consequences of state interference with digital information *for* democracies but, with few exceptions (discussed in sub-section 3.3.), do not study information controls employed *by* democracies.

In addition, there is a lack of studies of conditions leading to state control of the internet (sub-section 3.4.). Nevertheless, as I argue below, it is possible to suggest that the logic of political survival appeared to be the main factor leading to the implementation of numerous tactics to shape and limit information distributed over the internet. In the following sub-sections, I provide further details, reviewing first how scholars classify numerous tactics of internet control. After that, I proceed to the discussion of limitations and gaps in the literature.

3.1. Classifications of internet control

One of the often-cited classifications of internet control has been advanced by Deibert (2015). He identifies four generations of information controls, which have evolved from basic to more advanced and subtle ones, that states employ (not necessarily in chronological order). The first generation of internet control is tools of filtering information by blocking access to undesirable foreign websites; these measures are seen as defensive by states (Deibert 2015: 65). The Chinese government, for example, bans access to many western websites through a system known as the “Great Firewall” (Deibert and Rohozinski 2010a: 4). Many other countries (e.g. Kazakhstan and Uzbekistan) also practice what might be called politically motivated censorship of information, systematically restricting access to the opposition and critical materials[27].

The second generation of internet control is aimed at society through the implementation of restrictive laws and rules that may require, for instance, internet providers (ISPs) to store data on users or ask users to sign up before commenting or posting on a website (Deibert 2015: 68). For instance, in Kazakhstan, 2017 amendments to legislation on information and communication banned anonymous commenting on the

[27] Freedom House, for example, provides a systematic and comparative analysis of internet freedom – including content filtering – in sixty-five countries.

internet (Zakon 2017). Currently, Kazakh users can comment on online news and articles only after the authorisation by providing their personal data. Such measures leave little room for manoeuvre for civil society as “registration, licensing, and identity requirements [are used] to control what people do online and to create a climate of self-censorship” (Deibert et al 2012a: 11). In other words, the restrictive legal framework helps many governments shape and restrict the dissemination of digital information.

The third generation of information controls, seen as offensive, encompasses state-employed secret surveillance and disruption of internet connectivity. Such tools are especially used during political events (e.g. elections and opposition demonstrations) (Deibert 2015: 68-70). For instance, the internet became temporarily inaccessible in Kazakhstan in December 2016 when a political dissident was broadcasting from abroad; the minister of information later referred to technical errors on the network (Forbes Kazakhstan 2016). In another case, the Russian authorities disconnected the internet in Moscow during the August 2019 protests (Fokht 2019). Such “just in time” interruptions are quite regular among authoritarian states, according to Deibert (2015: 69-70). Besides, electronic armies such as Russian and Chinese pro-government trolls and bots, who manipulate and influence public opinion on social media, are included in the third generation of internet control. For instance, it is estimated that Chinese paid-for commentators write around 450 million posts per year to promote “the state, symbols of the regime, or the revolutionary history of the Communist Party” (King et al 2017: 497).

The fourth generation moves from the domestic to the international stage, where some countries appeal for a greater role of states in global internet governance, preferably under the UN guidance (Deibert 2015: 70). China, for instance, promotes the concept of “internet (information) sovereignty”, emphasising the priority of states to manage the internet within their sovereign borders. In this regard, China, referring to the state’s integral right to protect its sovereignty and criticising the established order of global internet governance, actively advances a view that the government has legitimate rights and responsibilities to regulate information (including one coming from abroad) on its territory (Powers and Jablonski 2015: 14-16). Consequently, China, along with Russia, used the concept of internet sovereignty to justify their attempts to align cyberspace with national jurisdiction (Mueller 2019: 9). Deibert (2015) also emphasises often neglected regional cooperation meetings on cybersecurity (for example, under the Shanghai Cooperation Organisation or the Collective Security Treaty Organisation), where tools of internet control can be shared.

Singer and Brooking (2018) address similar tactics of internet control, though classifying them differently. The authors maintain that (authoritarian) countries tame the technology through “control of the signal” by dominating the internet infrastructure and “control of the body” by arresting and putting pressure on internet users (Singer and Brooking 2018: 87, 90). Also, governments resort to the “control the spirit” and “daze and confuse” tactics (ibid, 95, 103). The former tactic is referred to Chinese practices of filtering online content and organising and paying the army of pro-governmental commentators. The latter tactic is based on Russian digital disinformation campaigns and the role of the RT (Russia Today) news agency and the Internet Research Agency (IRA) in manipulating information. The IRA, a well-structured and well-financed group of Russian trolls (about 600 participants) located in St Petersburg, advances the pro-Kremlin narrative on the internet with the main goal of shaping public opinion (Moore 2018: 94-95). The agency, taking roots from the “Nashi” pro-government nationalist youth organisation, has also been credited with meddling into the 2016 US elections via social media platforms (Singer and Brooking 2018: 112-114).

Sanovich et al (2018) also offer a typology of similar tactics. The authors distinguish between “offline responses”, “online restriction”, and “online engagement” tools at the state’s disposal, drawing evidence from Russia. The first tool, “offline responses”, covers the legal framework and prosecution along with state’s efforts to “change ownership infrastructure of online media” (Sanovich et al 2018: 438-439). One of the examples can be a requirement for bloggers to register with a respective ministry. Another example is the change of ownership of VKontakte, a popular Russian social media website, from a disobedient owner (Pavel Durov) to a group close to the Kremlin. The second tactic, “online restriction”, includes filtering and censorship techniques ranging from the DDoS attacks to the systems such as the Chinese Firewall (ibid, 440-441). The last tool, “online engagement”, includes exploitation and co-optation of the third party, pro-governmental bots/trolls, bloggers, and/or celebrities, to shape public opinion (ibid, 441-442). Relatedly, Hussain et al (2013: 8) recognised the following main tactics of internet control: “online” (blockage or closure of websites), “offline” (arrests of digital activists), and “by proxy” (pressure on internet intermediaries). The fourth, most radical tactic, is to switch off the whole network.

Roberts (2018), too, presents a classification of similar tactics of internet control. The author, by drawing evidence from China, distinguishes between three main mechanisms of control over information flows: “fear”, “friction”, and “flooding”. The first tool (fear) is designed to infuse a sense of self-censorship, which can be achieved through implementing censorship laws limiting what can be said on the internet, through intimidating users (specifically journalists) for publishing online, and through rewards, for example, by encouraging a journalist not to criticise a government (Roberts 2018: 45-49). Thus, the aim of the “fear” mechanism is to deter people from spreading or producing particular types of information.

The second tactic (friction) refers to throttling and, if necessary, blocking access to the undesirable website(s). This is what China did in retaliation to the Google's decision in 2010 not to filter information (Roberts 2018: 56-57), leading to a significant fall of the tech giant's share of the Chinese market. Thus, the government "can impose small or large taxes on information" (ibid, 58) with the purpose to divert people away from the undesired content. The key difference between "fear" and "friction" is that the former needs to be performed publicly so that the people can see consequences of internet activities, whereas the latter tactic "does not have to be observed to be effective" (ibid, 59). In China, for instance, the blocked internet page or website displays a technical error, thus making users guess whether the denial of access was due to technical issues or was politically motivated (Goldsmith and Wu 2006: 94).

The last tactic (flooding) in Roberts' classification is to shift attention from undesirable for the government topics by spreading and emphasising other, more neutral, information. This is usually done by means of state-owned news agencies. State media propaganda and paid online influencers who can write positive posts are thus forms of "flooding" with the aim to distract people's attention from negative information (Roberts 2018: 83-85). Consequently, people need "to spend more energy to sift through available information" (ibid, 43) that most individuals, as the author argues, would not do. Also, less visible "friction" and "flooding" partly reduce the possibility of backlash compared to the observable mechanism of "fear".

Although internet control has been this time organised into three complementing (that is, they are not mutually exclusive and can operate in concert) mechanisms of fear, friction, and flooding, Roberts' (2018) information controls are not substantially different from other scholarship. The "fear" mechanism, for instance, is similar to the abovementioned tactics of "control of body" and "control of signal" (Singer and Brooking 2018), the second generation of internet control (Deibert 2015) and "offline responses" (Sanovich et al 2018). The "friction" mechanism can be respectively compared to "control the spirit", "online restriction", and the first generation of state interference with digital information. Likewise, "flooding" closely parallels the "daze and confuse" tactic, "online engagement", and the third generation of internet control. In brief, tactics to shape and limit the online flow of information are similar but categorised in different ways.

Yet, regardless of how they are classified, it is possible to extract the following main information controls. These are censorship of online content, disruption of internet and mobile access, implementation of restrictive internet legislation, arrests of and encroachment on digital users and journalists, co-optation of bloggers and/or organisation of paid commentators who manipulate public opinion, covert surveillance of communications, and dominance of internet actors. In addition to identifying a similar cohort of internet control tactics, I also found common limitations in the literature, which are discussed in the following sub-sections.

3.2. Authoritarian nature of internet control

Many classifications of information controls distinguish between similar state-employed tactics. However, notwithstanding how these tactics are classified, the main limitation of internet studies is that scholars tend to attribute internet control solely to authoritarian countries. Although the same authors also discuss how democracies resort to information controls, they conclude that it is authoritarian regimes and the authoritarians who limit the dissemination of information online.

For example, Deibert (2015) constantly emphasises authoritarian countries as those that employ various tactics of internet control, dubbing this tendency “cyberspace authoritarianism”. All four generations of internet control are attributed to authoritarian regimes: “authoritarians have developed an arsenal that extends from technical measures, laws, policies, and regulations, to more covert and offensive techniques such as targeted malware attacks and campaigns to coopt social media” (Deibert 2015: 65). However, although Deibert defines authoritarianism[28], it is unclear how the author distinguishes between political systems as he also refers to some democratic countries while discussing digital authoritarianism. For instance, Deibert includes Pakistan, India, Indonesia, Malaysia, Venezuela, and Kenya in his examples of authoritarian cyberspace, control, and resurgence. Yet, at the time these countries were not commonly perceived as being authoritarian[29]. Thus, the author undermines his conclusions about the

[28] Deibert defines authoritarianism as “state constraints on legitimate democratic political participation, rule by emotion and fear, repression of civil society, and the concentration of executive power in the hands of an unaccountable elite” (2015: 64).

[29] In the discussion of the first, second, and third generations of authoritarian cyber control, Deibert (2015) refers to Pakistan as one of the examples of authoritarian resurgence. Yet the country at the time was a hybrid regime, according to 2014 Democracy Index (the Economist Intelligence Unit 2015), and a democracy by Polity IV data (Marshall et al 2018). Similarly, in the discussion of the second generation of controls, the author refers to Turkey as a country that imposes restrictive internet laws, though Turkey at the time was not authoritarian (ibid). In addition, the author refers to Tunisia, Indonesia, and India (the largest democracy in the world) as examples of what he calls “cyberspace authoritarianism”. Yet again, it is challenging to name all three countries authoritarian at the time (and now) as they were democracies in line with both 2014 Democracy Index and Polity IV. Also, Deibert, by arguing that “[a]uthoritarian policy makers looking to channel industrial development and employment opportunities into paths that reinforce state control can be expected to support local innovation” (2015: 74), refers to examples of Malaysia (that was a flawed democracy) and India. Other examples of cyber authoritarianism include Venezuela and Kenya (as those resorted to social media manipulation), which were hybrid regimes by 2014 Democracy Index; and Kenya was considered a democracy by Polity IV. In short, in all these cases of “cyberspace authoritarianism”, countries considered by Deibert (2015) did not appear to be authoritarian.

authoritarian nature of internet control by conflating authoritarian states with democracies (and hybrid regimes).

Additionally, in the discussion of the third-generation tactics that include covert surveillance, Deibert does not refer to some western liberal democracies such as the US and UK, focusing instead on China. Moreover, mass communications surveillance by the National Security Agency is considered contributing to the resurgence of authoritarian regimes (Deibert 2015: 65). That is, covert surveillance by the US (according to the author) helps autocrats justify their own secret spying on their population, but the act of surveillance by the US itself – which can be seen as an authoritarian practice (Glasius and Michaelsen 2018) – is not discussed by Deibert in his analysis of "authoritarian controls over cyberspace" (2015: 65). It is of note that the Snowden leaks in 2013 contributed to the promotion of the internet sovereignty concept – a right and priority of states to regulate the online flow of information within their borders. However, these calls to strengthen state control over cyberspace came not only from authoritarian regimes but also from democracies (Mueller 2017: 13-14). Consequently, Deibert's conclusions about digital authoritarianism appear to be inaccurate as the same author also provides, and in the case of US mass surveillance neglects, examples of how democracies sought control of the internet.

However, the trend to split internet control between authoritarian and democratic states is not uncommon in the scholarly literature. A similar narrative of internet control with similar limitations has also been offered by Singer and Brooking (2018). Although Singer and Brooking (2018) constantly refer to authoritarian regimes, they do not provide the definition of authoritarianism. In addition, it is (again) unclear how the authors distinguish between political systems. For instance, Singer and Brooking, claiming that authoritarian countries distorted and turned "[t]he web's unique strengths … toward evil ends" (2018: 87) such as oppression and control, nevertheless provide democratic India as one of the examples. Also, in the discussion of how "authoritarians haven't hesitated to use their own unique powers" (Singer and Brooking 2018: 90) to "control the body", the authors refer to Pakistan among other countries. Yet, Pakistan at the time was considered a hybrid regime, according to Economist Intelligence Unit's Democracy Index (2018), and democracy by Polity IV data[30] (Marshall et al 2018). In other words, the authors, maintaining that India attempted to control information flows by cutting off communication networks in one of the regions and Pakistan sentenced to death an

[30] Pakistan had the +7 Polity score in the range from -10 (full autocracy) to +10 (full democracy).

internet user for online speech, have nevertheless concluded that it is the autocrats[31] who control the internet.

Likewise, in the discussion of the "daze and confuse" tactic that has given "authoritarians a tool that has never before existed" (Singer and Brooking 2018: 103), the authors again refer to India as one of the examples of state-organised manipulation and propaganda on the internet. Furthermore, Singer and Brooking (2018: 116) refer to a 2017 study[32] by Bradshaw and Howard (2017), stating that 29 countries resorted to manipulation of public opinion on social media (there are 28 countries in the original report). Most importantly, though, the cited original study also summarises that "almost every democracy in this sample has organized social media campaigns that target foreign publics, while political-party-supported campaigns target domestic voters" (Bradshaw and Howard 2017: 3) and that "[a]uthoritarian regimes are not the only or even the best at organized social media manipulation. The earliest reports of government involvement in nudging public opinion involve democracies" (ibid, 3). This part, however, has not been mentioned and discussed by Singer and Brooking (2018). Instead, the authors conclude their analysis of internet control tactics by stating that "a new breed of authoritarians tighten their grip on the world" (Singer and Brooking 2018: 116). In other words, we again see that the scholars, despite being aware of practices of state interference with information online within democratic settings, have not accounted for democracies while making conclusions about authoritarian control of the internet.

Roberts (2018) also provides examples of information controls employed by democracies, yet (explicitly) emphasises the authoritarian resilience towards the growing role of the internet and authoritarian control of new technologies. In the discussion of the fear mechanism of information control, for instance, Roberts (2018: 47) mentions defamation laws that restrict freedom of expression in South Korea, Indonesia, and the US. Also, the author emphasises intimidation of journalists in "democracies such as Mexico and Brazil" along with India and Ukraine (Roberts 2018: 49). Yet, she concludes that "findings in this book speak to a growing literature that puzzles over the resilience of authoritarian governments in the face of the third wave of democratization and the expansion of the Internet" (ibid, 227).

In addition, Roberts admits that along with democratic Israeli and Mexican governments "[e]ven political parties in the United States are beginning to employ online

[31] To underpin this statement, Singer and Brooking (2018) provide examples of Russia, China, Iran, Turkey, Saudi Arabia and other ostensibly autocratic regimes that, following the logic of authors, also include Pakistan and India. However, the authors, as already mentioned, do not provide the definition of authoritarianism.

[32] Interestingly, Singer and Brooking (2018: 321) cite a Bloomberg article but not the original report from the Oxford Internet Institute.

armies that defend their candidates" (2018: 84). Nevertheless, she concludes that the friction and flooding mechanisms, directed to distract and divert people from undesired information, strengthen the "authoritarian resilience" (Roberts 2018: 228). Although the latter sentence might be correct, the author, despite admitting the fact that democracies employ the same mechanisms of information control, refrains from discussing consequences and implications of using them by democracies. Besides, Roberts (2018: 229) argues that the development of surveillance technologies would help the authoritarians target and spy on dissidents in a more able way. However, as some scholars (Hintz and Milan 2018) suggest, unlimited surveillance does not extend only to authoritarian regimes and is already a problem in democracies.

Furthermore, the author notes that people in "democracies recently have been shown to be susceptible to flooding as well" (Roberts 2018: 17) and, therefore, "more research needs to be done to study how censorship extends to democratic environments on the Internet" (ibid). Nevertheless, accepting that censorship might take place in a democratic context, Roberts offers a theory based only on practices of one authoritarian state (China)[33]. Given that the author was aware of "flooding" in democracies, internet control occurring within democratic settings was not, however, counted when building a theory. Accordingly, we can yet again see the repeating pattern of noting internet control practices in democracies (however entrenched the extent of control can be) but overlooking them in the following analysis and conclusion.

In another analysis, Sanovich et al (2018) explicitly attributed options of internet control to the authoritarians. The scholars focused solely on authoritarian regimes, though not defining them, whereas democracies were omitted. Yet, as we already know, the 2017 study by Bradshaw and Howard showcased that democracies have been resorting to public opinion manipulation on the internet – what Roberts (2018) classifies as "flooding" and Sanovich et al (2018) as "online engagement" – as much as autocracies. In other words, the classification by Sanovich et al (2018) designed purposefully for authoritarian regimes can, in practice, suit many democracies.

However, there has been a study of internet control that focused on both democracies and autocracies. Hussain et al (2013) traced known cases of internet control across the world between 1995 and 2010[34]. Altogether, the authors identified 566 cases of state intervention with the internet. Remarkably, they found that democratic governments between 1995 and 2010 interfered with digital networks almost as often as

[33] Besides, the question to be raised is the applicability of Roberts' theory to other contexts and whether it is correct to call evidence derived from one country a theory.

[34] The authors defined cases as those "where a government intervened in a digital network by breaking or turning off connections between national sub-networks and global information networks" (Hussain et al 2013: 6).

authoritarian ones. Democracies did not significantly lag behind autocracies and in some instances were even ahead of them. For example, among all available options, democratic states used the pressure on and manipulation of internet service providers more often than authoritarian regimes (47 vs 41 incidents) (Hussain et al 2013: 9).

Nevertheless, although the authors discovered instances of state control over the internet in democracies, they excluded them in the following analysis and case studies. Thus, despite revealing that democratic states resorted to internet control almost on the same scale as autocracies, conditions and consequences of such behaviour of democratic governments were not discussed. Instead, Hussain et al (2013) analysed state intervention with networks in authoritarian countries such as Iran, Egypt, Kuwait, Morocco, Vietnam, and Russia. Another issue is that the study has not been updated, covering incidents of internet control up to 2010.

Consequently, it is reasonable to suggest that classifications of information controls are viewed and analysed through a division between autocratic and democratic political systems. Above, I discussed the works of Deibert (2015), Singer and Brooking (2018), Roberts (2018), Sanovich et al (2018), and Hussain et al (2013) – all experts of internet politics. The list is, however, not comprehensive as the goal was not to review all typologies of internet control but to demonstrate a common pattern inherent to many studies. This pattern also extends to other scholars: for example, Tucker et al (2017), Morozov (2011), MacKinnon (2012), Wright (2018), Guriev and Treisman (2015).

All in all, the authors, despite providing examples of democratic states, maintain that it is authoritarian regimes that employ various tools to control the dissemination of digital information and reason about the authoritarian resilience, authoritarian cyberspace, and digital authoritarianism. This is not to say that authoritarian countries do not shape and restrict information distributed over the internet, but that democracies should not be excluded from a (comparative) analysis of practices (and origins) of internet control. Focusing only on authoritarian states can reduce the scope of internet scholarship. Nevertheless, as I discuss in the following sub-section, despite some exceptions in the literature, the tendency to attribute information controls to the authoritarians is also evident in recent studies.

3.3. Authoritarian control of the internet as a rule

A possible explanation for why scholarship generally focuses on authoritarian regimes is that the internet has been widely seen as a liberation technology, which would enhance democratic practices (Diamond 2010). The emphasis on the liberating potential of the internet only grew after several dictators were overthrown allegedly with the help of ICTs. When some governments managed to resist and adapt to the development and use of digital technologies, scholars (e.g. Deibert 2015: 64, Roberts 2018: 227) began discussing the authoritarian resilience and resurgence. Consequently, given the democratising agency of the internet, it was naturally taken that internet control occurs mainly within the autocratic context. Numerous cases of how Iran, Russia, China, and other ostensibly authoritarian states interfere with networks have underpinned that claim. As a result, practices of internet control in democracies were largely disregarded and not analysed[35]. Also, as I discuss in sub-section 3.4., another consequence of such approach is that possible conditions of state control have not been scrutinised.

Nevertheless, there have been exceptions in the literature as few internet control tactics have not been attributed solely to authoritarian regimes. These are covert surveillance and its implications for human rights and sway of public opinion on social media. The former tactic has received wider attention after the 2013 Snowden revelations of mass surveillance by the US and UK security agencies and the latter tactic has come under more scrutiny after the 2016 US presidential elections in which reportedly a third party interfered. In both cases, scholars (Greenwald 2014, Hintz and Milan 2018, Bradshaw and Howard 2017) do not draw a strict line between political systems (autocracy and democracy), admitting that both tactics take place within the democratic context, too.

For instance, Hintz and Milan (2018) study how authoritarian and illiberal practices of covert and pervasive surveillance are found in western democracies. Also, surveillance-related issues of privacy and big data (Dencik et al 2016) have been examined. Similarly, Bradshaw and Howard (2017, 2018) found that democratic governments and institutions (as much as authoritarian ones) have opted to manipulation of public opinion on social media. That is, censorship through noise is common in democracies. Nonetheless, these studies have focused on only one of internet control tactics; there have not been recent analyses of all main tactics within both authoritarian and democratic polities[36].

One of the exceptions is the study of the internet fragmentation debate by Mueller (2017). In the discussion of states' attempts to align cyberspace with local jurisdiction and sovereignty, Mueller identifies three main methods of control over the internet. These are "national securitization" (control under the grounds of providing national security), "territorialization of information flows" (censorship of content from abroad, data localization legislation, geolocation-based restriction of internet access, and international

[35] As mentioned above, I do not consider censorship of online content related to (child) pornography and copyrights issues as part of internet control.

[36] As noted in Chapter 1, studies of internet control by Deibert et al (2012b) and Hussain et al (2013) have not been updated.

promotion of the information sovereignty concept), and “alignment of critical Internet resources” (nationalisation of the global domain name system and internet protocol addresses) (Mueller 2017: 74-84). Most importantly, Mueller provides examples of democratic states in his classification and, consequently, does not attribute the methods of cyberspace control exclusively to the authoritarians and does not reason about the authoritarian resilience and digital authoritarianism.

Nevertheless, despite these exceptions, the tendency to divide countries that control information on the internet between authoritarian and democratic ones continues and is evident in recent studies. Kendall-Taylor et al (2020), for example, following assumptions of Deibert (2015) and Roberts (2018), also attribute all tools of internet control to autocrats. According to the scholars, it is the prerogative of solely “digital autocracies” to disrupt internet and mobile access, to organise paid-for brigades who spread disinformation and pro-government messages manipulating public on social media, to filter online content, and to deploy covert surveillance of communication networks. Rosenberger (2020), too, is resolute in her judgements about internet control. The author, like Kendall-Taylor et al (2020), extensively discusses cases of Russia and China, assigning control of information flows to the authoritarians. The latter, according to Rosenberger (2020: 146), resort to “surveillance, censorship, and the manipulation of information” whereas democracies happened to be merely the victims of these practices.

Clarke and Knake (2019) are even more radical in their (perceived) division between democracies and autocracies, also ascribing the command of information flows to the latter. The authors suggest to the US and its allies to take full control of the internet by creating the Internet Freedom League, install their own rules, and if needed to cut “bad actors” such as Russia and China off the network (Clarke and Knake 2019: 186-188). In other words, the United States should unilaterally regulate and control the internet, imposing its own wills on others. The authors, however, do not discuss the existing system of global internet governance and the role of international organisations (such as the Internet Corporation for Assigned Names and Numbers, the Internet Engineering Task Force, the United Nations), and whether such an extreme method would instead lead to a divided internet.

In another recent study, Weidmann and Rød (2019) solely focus on authoritarian states in their examination of the internet’s effects on protest movements. The authors excluded democratic countries from the study on the assumption that the latter do not and would not control the internet. Similarly, Diamond (2019: 236), in his discussion of how governments vie for control of cyberspace, repeatedly concludes that it is “authoritarian governments [that] are using the internet as a vast web for political surveillance, repression, and control”, leaving aside democratic states. Yet most importantly, all these narratives, focusing on the engagement of authoritarian countries with the digital domain, omit democratic states by default by assuming that they shall not control information online. As a result, the authors discuss implications of internet control *for* democracies, taking no notice of (known) similar activities *in* democracies (regardless of how entrenched the extent of internet control in democracies can be).

Besides, researchers studying information controls and arguing about the "authoritarian wave/breed" and "cyberspace/digital authoritarianism" tend to forget to provide the definitions of political regimes they examine and refer to. Yet, it is important for scholars to explicitly clarify how they define and conceptualise political systems in their studies as there exists no universal definition of both democracy and authoritarianism. The definitions vary[37]. Frantz, for instance, states that "the bulk of mainstream research on authoritarian politics" (2018: 6) operates with a minimalist definition of authoritarianism as the one where a government is not selected through fair and free elections. Similarly, Berman (2019: 4) contends that most pundits currently use a minimalist definition, according to which a key feature of democracy "is the selection of leaders through competitive elections by the people they govern".

On the other hand, there exists a more extended definition that also "explicitly incorporates a wide variety of liberal rights" (Berman 2019: 6). In this regard, Polity IV focuses on three elements such as electoral procedures, institutional constraints on the executive authority, and protection of civil liberties in the evaluation of political systems (Marshall et al 2018: 14). Economist Intelligence Unit's Democracy Index (2020), for another example, measures political regimes by assessing five aspects in each country. These are electoral process, civil freedoms, government's functionality, political participation, and political culture. Thus, given the possible range of political regimes' definitions, the lack thereof can lead to further confusion over the indexation of countries. However, in addition to the definitions, as I discuss in the following sub-section, there is also a lack of studies of conditions of state control over the digital flow of information.

3.4. Conditions of internet control

Although the significant body of the literature concentrates on numerous information controls (albeit viewing them through a democracy-autocracy dichotomy), few pundits have sought to analyse underlying conditions of governments' attempts to control information online in the first place. Scholars tend to focus on *how* states shape and restrict information on the internet; the main reference in these studies is authoritarian

[37] The goal here is not to discuss an ongoing debate over the definitions of democracy and authoritarianism, but to demonstrate that there has been a range of definitions thus far.

states. There is a lack of research analysing *what has led* governments to control information flows as authoritarianism is usually assumed as the main (and only) origin of state control. However, despite this gap in the literature, it is possible to suggest the logic of political survival as the main driver of internet control.

Hussain et al (2013) shed some light on why states interfere with the internet, identifying two broad reasons: protection of political authority and preservation of public good. The former includes “protecting political leaders and state institutions; election crisis; eliminating propaganda; mitigating dissidence; and national security” (Hussain et al 2013: 11). The latter covers “preserving cultural and religious morals; preserving racial harmony; protecting children; cultural preservation; protecting individuals’ privacy; and dissuading criminal activity” (ibid, 11). Surprisingly, the study found that democracies cited “protection of political leaders and institutions” and “national security” reasons for internet control almost as often as authoritarian regimes.

Although Hussain et al (2013) identified the common reasons for internet control, they did not address the causes leading to state intervention in digital networks. The authors suggested that “[b]anning access to social media websites, powering down mobile phone towers, or disconnecting the Internet exchange points in major cities are an authoritarian government’s desperate strategies for asserting control” (Hussain et al 2013: 15), though they did not extend further on this proposition. Similarly, although the scholars found that democracies systematically resorted to internet censorship (between 1995 and 2010), they did not study what motivated democracies to control cyberspace. In other words, Hussain et al (2013) identified the main cited reasons for state intervention but the causes that lead some governments to control information online to protect leaders’ political authority and preserve the public good were not analysed.

The study of Deibert et al (2010) is one of the few studies that covered the possible origins of internet control. The authors, despite studying primarily how governments control the internet, have provided some insights into why states may employ information controls. The authors assert that the non-Baltic post-Soviet states after the “colour revolutions” in Ukraine, Georgia, and Kyrgyzstan between 2003 and 2005 started considering critically the internet’s ability to undermine national security and specifically to empower possible social disorders (Deibert et al 2010: 20). On the other hand, governments were aware of the opposite side of the internet that can be directed to disable opposition movements by filtering information (ibid, 8). Thus, the authors imply that the post-Soviet leaders’ fear of mass protests and demonstrations, strengthened by examples of successful regime change in the region, has eventually led to the implementation of information controls; the leaders have also recognised the internet’s potential to be used against opposition movements.

Also, Deibert et al named “the state of Internet access and infrastructure, the level of economic development, and the quality of governance institutions” (2010: 111), in addition to laws and decrees regulating the internet, as key factors “determining which countries resort to filtering and how they choose to implement Internet content controls” (ibid, 111). However, the authors did not study these factors, providing only a table at the beginning of each case study but not connecting them to the extent of internet control. In other words, possible underlying conditions of state control over digital information have been proposed but have not been scrutinised.

Another explanation for internet control tactics was offered by Deibert (2015). He suggested that the main cause of digital authoritarianism is the need for cybersecurity, given the growing dependence of people on the internet. As the author states, “a major driver of this [authoritarian] resurgence has been and likely will continue to be the growing impetus worldwide to adopt cybersecurity and antiterror policies” (Deibert 2015: 71) and that “[t]he headlong rush to guard against extremism and terrorism worldwide, in other words, could end up providing the biggest boost to resurgent authoritarianism” (ibid, 71).

By following Deibert’s line of reasoning, states seek control of the internet by resorting to four generations of tactics (discussed above) because of the need to “guard against extremism and terrorism”. The problem is, however, that it is uncertain how the necessity of cybersecurity drives some governments to employ various information controls such as, for example, the organisation of a trolls army or censorship of online content. That is, the state-orchestrated sway of public opinion on social media platforms is hardly driven by security concerns but rather arguably by political calculations of those in power. Similarly, the Chinese government filters and blocks information online not because to strengthen cyber-defence of the country but rather to secure the political authority of the ruling party. In other words, the need for cybersecurity lacks the explanatory power for why states apply numerous tactics of internet control.

Nevertheless, despite the lack of analysis of conditions, it is possible to distinguish a common denominator behind information controls, which appears to be political survival. Deibert et al (2010), as mentioned above, argued that political leaders fear internet-enabled opposition movements and protests. Similarly, Roberts maintains that “information can act as a tool to facilitate coordination and protests that can threaten political entities’ survival” (2018: 22), thus leading to state control over information on the internet. (In addition, Roberts mentions that internet control depends on “the political structure, level of economic development, and technological capabilities of the regime” (2018: 236), though without providing any further details or analysing these factors.) Also, according to Powers and Jablonski (2015), all states endeavour to control information, albeit with different fervour, for the purpose of self-preservation, that is, political survival.

Likewise, Wagner (2018: 3929) claims that the government of Pakistan tended to resort to communications disconnections during anti-government demonstrations so that to prevent coordination of efforts by political opponents. Thus, after examining numerous cases of internet shutdowns in Pakistan between 2012 and 2017, Wagner concludes that communications disruptions are politically motivated, being used "within the context of a political struggle" (2018: 3933). Sanovich et al (2018), drawing from the case study of Russia, similarly explain the preference for internet control tactics as a result of political contest between those in power and those in opposition. The authors contend that the choice of controls is "a complicated process of choosing the optimal strategy, directly reflecting … the political struggles inside the regime" (Sanovich et al 2018: 442).

Soldatov (2019) echoes the abovementioned claims, maintaining that the desire to preserve the existing political regime led Putin's government to control first what is communicated via TV and later on the internet. Consequently, independent TV channels starting from the 2000s were eventually shut down or acquired by more loyal owners. The internet, for its part, after the 2003-2005 "colour revolutions" in the post-Soviet countries, the 2011 Arab Spring, and especially the 2011 demonstrations in Russia itself, was regarded as a potential tool that can trigger protests and thus instigate regime change. Therefore, according to the author, Putin's administration, as a countermeasure to substantially diminish the digital technologies' potential to start a revolution, resorted to information controls. In other words, the logic of political survival resulted in a strict approach to content distributed over cyberspace.

Thus, there seems to be a (broad) consensus that political survival tends to lead to state control of digital information. That is, some governments (regardless of their political ideology) when feel threatened by, for instance, political opposition are tempted to employ information controls. However, as can be seen, those of the scholars who have addressed potential conditions did not study them in detail: most of them either briefly mentioned what might lead to internet control without in-depth (or comparative) analysis or drew their propositions from one case study. Pundits have listed some possible drivers of internet control but did not scrutinise or test them. The assumption of political survival, therefore, needs to be verified. Consequently, in chapter 3, I discuss the logic of political survival that takes roots from institutional theory in more detail, and in chapter 5, I test the proposition by conducting a comparative analysis.

4. CONCLUSION

In this chapter, I reviewed the body of literature that addresses tactics and conditions of internet control. The chapter started with the background information on the interplay between the internet and information structure, summarising that irrespective of the digital technologies' impact and potential (be it real or exaggerated) many governments have appeared to seek control of information distributed over the internet.

After considering the context, I discussed the literature on internet control. Overall, there have been many ways to classify how governments shape and limit information online (Deibert 2015, Roberts 2018, Singer and Brooking 2018). Yet these classifications address similar tactics such as censorship of online content, internet shutdowns, crackdown on internet users, disinformation campaigns on social media platforms, adoption of legislation that expands state powers in the digital domain, cyberattacks and covert mass surveillance, and dominance of internet infrastructure and intermediaries. These tactics facilitate state control over information on the internet[38].

Also, throughout the literature review, I found a few common patterns and limitations inherent to many studies. One of these is a tendency among scholars to conclude that it is authoritarian countries that control digital information. Although the same authors also provide examples of how democratic states interfered with the internet, they overlook democracies in the following analyses and conclusions. The focus is instead on the "authoritarian resilience", "authoritarian cyberspace" and other authoritarian issues (and their implications for democracies). As a result, known cases of internet control that took place in democracies are neglected. This, however, does not mean that authoritarian states do not control information online, but rather that democracies should not be excluded from the analysis. Meanwhile, the existing approach adopted in the literature does not offer a full grasp of the issue under consideration.

Some pundits (Hintz and Milan 2018, Bradshaw and Howard 2017, Mueller 2017), who do not attribute internet control solely to authoritarian governments, have examined cases of democracies that opted to control information online. Yet most of them focus predominantly on one of several tactics such as covert surveillance of communication networks or manipulation of public opinion on social media. Thus, notwithstanding that we have learnt that democracies resort to information controls[39], the

[38] For instance, by arresting users for their digital activities (e.g. publication of critical posts) some governments try to infuse a sense of fear into society. As a result, self-censorship of citizens limits the amount of critical information. Similarly, by pressuring internet intermediaries (such as service providers) governments can block access to websites that hold negative (opposition) information.

[39] As noted above, I do not consider censorship of content related to (child) pornography and copyrights protections as state control of information online.

extent of their engagement with the internet (that is, how many tactics they employ) has not been explored. So far, based on known cases discussed above, the implementation of internet control tactics by democratic countries is considered to be selective[40].

In other words, we have recognised that authoritarian regimes control information distributed over the internet and that democracies also can apply some of internet control tactics. Yet it is unknown whether internet control by democracies is *a rule or an exception*. What is lacking here is a comparative analysis of all main information controls (not just one) within both the authoritarian and democratic context (not just within one political system). Such an approach is important as democracies can, and do, control information online.

Another pattern identified in the literature is a lack of studies of possible conditions of internet control. Above, I suggested that this gap is due to the scholars' conclusions that it is the authoritarians who control digital information within national borders. As a result, authoritarianism is thought of as the main origin of internet control. Another interrelated reason is that the internet was (and still is) viewed as a technology with the potent democratising potential that promotes democracy and combats dictatorships. The attention of many scholars was naturally directed to non-free societies, for example, the post-Soviet "colour revolutions", the 2009 protests in Iran, the Arab Spring. Thus, factors leading countries to control information online have not been scrutinised. Those scholars who addressed the issue propose political survival as the main motivation behind information controls (Wagner 2018, Roberts 2018).

Consequently, I build on these gaps in the literature in the following chapters. In particular, I contribute to knowledge by studying the main tactics of internet control in both authoritarian and democratic countries in a comparative manner (chapter 5). I also contribute to the literature by thoroughly addressing conditions of state interference with digital information, testing and refining the main proposition (the logic of political survival) (chapters 3-5). Another interrelated contribution of my study is that it sheds light on internet politics in the post-Soviet region (chapters 6 and 7). I conduct two case studies, examining how survival strategies of political leaders in Kazakhstan and Ukraine have affected the extent of internet control in their respective countries.

In brief, my study emerges from the gaps in the scholarly literature: the lack of focus on democracies and the lack of studies of underlying conditions of internet control. In the following chapter, I discuss the interplay between the assumption of political survival, which originates from institutional theory, and control of information on the

[40] For example, mass surveillance of communications in the US or internet shutdowns and social media manipulation in India.

internet in more detail. The main argument is that the nature of political institutions (a proposed condition) affects the choice of survival strategies of those in power, thereby shaping the extent of internet control (an expected outcome).

CHAPTER 3. THEORETICAL FRAMEWORK: THE INSTITUTIONALISM AND CONTROL OF INFORMATION

1. INTRODUCTION

In the previous chapter, I inferred that the logic of political survival appeared to affect state control of digital information (Wagner 2018, Roberts 2018). In this chapter, I discuss the interplay between survival strategies and control over information flows in more detail, drawing insights from institutional theory. I maintain that the (new) institutionalism (Lowndes and Roberts 2013, Scott 2014) is the appropriate theory to apply to the study of internet control[41] as political institutions shape the logic of political survival, which, in turn, affects the choice of information policies (Bueno de Mesquita et al 2003, Acemoglu and Robinson 2013). That is, political leaders operate within political institutions ("the rules of the game") that structure their incentives and survival strategies, subsequently having an impact on their actions and decisions including in the information domain.

First, I discuss institutional theory, reviewing how the dominant theoretical approaches define and see institutions[42]. After that, I study how institutions, shaping survival strategies of political actors, affect the choice of governance policies including in the information domain (Bueno De Mesquita et al 2003, Acemoglu and Robinson 2013). For example, Acemoglu and Robinson (2013) distinguish between two types of political institutions: inclusive and extractive. In the first case, institutions are more democratic, serving the needs of a large part of the population, the executive authority is constrained, and a political landscape is more competitive. Consequently, under inclusive institutions, control of information flows tends to be less extensive. In the second case, institutions are more authoritarian, serving the interests of a small number of those in power, while political opposition is fragmented and society's participation in political processes is considerably restricted. As a result, the dissemination of information tends to be controlled under extractive institutions.

In addition, I also discuss how information flows and new technologies of the day were historically controlled in countries with extractive institutions. Before the internet, for instance, the introduction of the printing press, telegraph, radio, and even steam

[41] Although the explicit use of political theory is uncommon in internet studies, there have been some exceptions. Choucri (2012), for example, applied the lateral pressure theory to study international relations in the digital age. Brown and Marsden (2013) built their study of internet regulation on the premises of rational choice theory. Similarly, the theory of information censorship advanced by Roberts (2018) draws insights from rational choice theory. Valeriano and Maness (2015) utilise a theory based on cyber restraint and issue-based perspective. Another exception is Mueller (2010), who used institutional theory (network organisations) in his study of internet governance.

[42] Although institutional theory begins the argument with institutions, it does not necessarily prioritise them.

railways was often opposed by authoritarian political leaders. This was due to the logic of political survival. Many leaders feared that the free dissemination of information and fast communication between citizens enabled by new mediums could undermine the balance of political power, which was in favour of those in power. As a result, in countries with extractive institutions, the extent of control over the press and new technologies was substantial. In contrast, in countries with inclusive institutions, institutionally constrained executives could do little to control the media and technologies (even if they wanted). The institutional context was thus important for the extent of control over information distributed via the mass media and new technologies.

Consequently, drawing insights from institutional research, I argue that political institutions, by shaping survival strategies of political leaders, affect the choice of policies in general and in the digital domain in particular. The proposition, thus, is that the distinct nature of institutions leads to different extents of internet control. In countries with more extractive institutions, government engagement with digital information is expected to be more thorough – more information controls are implemented. Meanwhile, in countries with more inclusive institutions, information distributed over the internet is assumed to be selectively controlled[43].

2. BACKGROUND: INSTITUTIONAL THEORY

There are two schools of thought in the scholarly literature on institutionalism (Lowndes 2018, Peters 2019, Scott 2014): old (traditional) institutionalism and new institutionalism. Old institutionalism focused on a (comparative) analysis of formal structures and organisations within the government. The main emphasis of old institutionalism was on legalism (law and its role in governance), structuralism (structures largely conditioned behaviour of individuals), holism (study of political systems as a whole), historicism (national history and historical development of countries), and importance of norms and values (what constitutes a good government) (Peters 2019: 8-13). However, after the advent and ensuing dominance of behavioural approaches in political science after the 1950s, which argued that individuals instead of organisations should be studied to explain political outcomes, old institutionalism was eclipsed. Only in the 1980s, in response to the proliferation of behavioural and economic methods of inquiry in political science, institutionalism re-emerged, though in a somewhat different form.

The main shift in the theoretical discussion was driven by the seminal article of March and Olsen (1984) who coined the term “new institutionalism”. By moving the focus

[43] As discussed in chapter 2, democracies also can exercise control over the online flow of information. Therefore, internet control in democracies is not completely absent.

of debate in political science from individual-based approaches to political processes such as behaviouralism and rational choice theory to more structural features such as institutions, March and Olsen reanimated institutional theory, bringing not just a new name but also adding new meaning. In particular, March and Olsen (1984) argued that the role of institutions was underestimated in political theory, which at the time tended to focus on individuals as the main political actors. They stated that institutions, too, are autonomous political actors that can affect the main political processes such as the development of individuals' incentives, the balance of political power, and constraints on actions set by rules and laws (March and Olsen 1984: 738-740).

Importantly, almost at the same time (the 1980s), in addition to the March and Olsen's version (normative institutionalism), another two approaches to institutions – historical and rational choice – have appeared. Below, I briefly review how each approach defines institutions and considers institutional effects on political behaviour and outcomes. The main point is that, despite some differences, there are many similarities between the dominant strands of institutional theory.

2.1. What do institutions mean?

Normative institutionalism sees institutions not only as formal organisations and structures of government but also as a collection of norms, rules, and practices that define the behaviour of political actors (March and Olsen 1989). Rules and practices, according to March and Olsen (2008: 3), prescribe the appropriate conduct to individuals in particular circumstances. Appropriate behaviour is of "ancient origin" and grounded on collective and sometimes implicit considerations of "what is true, reasonable, natural, right, and good" (March and Olsen 2011: 479). The logic of appropriateness thus indicates proper behaviour for actors whose actions are expected to conform to norms and constitutive rules of institutions they belong to (though, it is accepted that those norms can be interpreted differently by members of an institution). Consequently, this logic of appropriate behaviour, guided by institutional rules and norms, affects political outcomes.

Another main strand of theory is rational choice institutionalism, which sees institutions as a collection of incentives and rules that set constraints on the behaviour of political actors (Weingast 1998). Despite the assumption of rational choice theory (in its purest form) of the full autonomy of individuals, rational choice institutionalists accept that political institutions constrain the agency of individuals[44]. The utility maximisation is

[44] Rational choice and normative approaches, although offering a structural explanation for political behaviour, accept that individuals can shape institutions as well. For example, this can

still assumed as the main motivation of actions but the autonomy of actors is bound since they need to operate within institution-determined incentives. Thus, the goals of individuals remain to be the same but the means of achieving these goals have been changed under the impact of political institutions[45].

The third dominant approach to institutions is the historical version. Historical institutionalists define institutions as “the formal or informal procedures, routines, norms and conventions embedded in the organizational structure of the polity” (Hall and Taylor 1996: 938). The key point is that initial choices, ideas, and procedures woven in the formation of an institution are crucial as they affect consequent (future) decisions and policies taken within this institution by its members. Historical institutionalists contend that institutions will persist once formed unless strong political pressure (for example, a revolution) emerges and changes the institution. Thus, the main focus is on the historical development of an institution as political outcomes in this version of institutionalism appear to be path dependent (Peters 2019: 80). Similarly, historical institutionalism also focuses on critical junctures that have caused shifts in the institution’s evolution (ibid, 90), though contingency is also taken into account when studying institutions.

In some cases, historical institutionalism can be interrelated with the rational choice approach when a historical element is combined with the rational choice version (Hall and Taylor 1996, Lowndes and Roberts 2013: 37-38). In other cases, historical institutionalism can be related to the normative approach due to emphasising the importance of ideas and norms that often lead to the creation and persistence of an institution (e.g. Levitsky and Ziblatt 2018). Proponents of rational choice theory also have become more acceptable of other (ontologically different) theoretical paradigms (e.g. North and Thomas 1973, Acemoglu and Robinson 2019, Bueno de Mesquita et al 2003). In this regard, Lowndes and Roberts maintain that critics of rational choice approach to institutions tend to see the latter “as interchangeable with rational choice theory in its original and purist form” (2013: 35) without considering that rational choice institutionalists have recognised the importance of institutions and institutional norms in political life[46].

happen through non-compliance with established norms and rules, by actions of (exceptional) leaders, or by the way of recruiting different categories of members into institutions (Peters 2019: 45-46).

[45] In this regard, it is also no overstatement to advocate that the rational choice approach, although itself explicitly agency-centred, is implicitly, if not paradoxically, structure-determined (Hay 2002: 103).

[46] For instance, North, arguing that institutions “structure incentives in human exchange, whether political, social, or economic” (1990: 3), have also recognised that “the governing structure [of human interaction] is overwhelmingly defined by codes of conduct, norms of behavior, and conventions” (ibid, 36).

All of the above mean that practitioners of new institutionalism can incorporate ideas from other approaches. Although three dominant strands within institutional theory are distinct and define the role of institutions differently, the boundaries between them are not clearly specified and eclectic approaches to research problems contribute to the blurriness of lines. This became possible because some key features of institutions are shared by all institutionalists (Lowndes 2018: 60-64). One of them is to consider institutions not only as formal organisations but also as a collection of rules that shape the behaviour of political actors. Another common characteristic is to study informal institutions in addition to formal ones. New institutionalists (in comparison to representatives of old institutionalism) appeared to clearly understand the importance of unofficial and unwritten rules that guide political life. Other shared features of new institutionalism are related to the stability of institutions (stable patterns of behaviour), shared values (meaning and power entrenched in institutions), impact on actors' behaviour (constraints on individual actions), and the importance of context (space and time of institutions and their interplay with other related institutions) (Peters 2019: 22-23, Lowndes 2018: 60-64).

In other words, although institutional approaches see institutions from somewhat different angles, they all consider institutions as key aspects of political life, overlapping in many theoretical and methodological components[47]. Also, explanations of political outcomes offered by practitioners of different political theories are not necessarily mutually exclusive and, depending on a research problem's context, can supplement each other. In some cases, the combination of various theoretical approaches can produce a more satisfactory and complete explanation for political phenomena[48]. Such an eclectic institutional approach is also evident in theoretical and empirical considerations of institutionalists, whose research I discuss in the following section.

3. POLITICAL INSTITUTIONS AND CONTROL OF INFORMATION

After reviewing institutional theory, I discuss how institutions affect the extent of information control. Before studying conditions leading governments to control information flows, it is important to appreciate (or assume) that high-office politicians

[47] However, such a synthesis of different theoretical paradigms to address a research problem is not novel in political science. Since at least the end of the 1980s, many scholars have begun to see different institutional versions as complementary rather than competing and utilise them to study political issues (Weingast 1998: 183, Hall and Taylor 1996: 955-956). In a similar fashion, Peters argues that the boundaries between institutional approaches should be loosened and rather complement each other, given that in isolation no version is in a position to "fully explain all political actions" (2019: 2).

[48] The mixture of various institutional versions in political analyses has allowed an advancement of unified theory of institutionalism (Lowndes and Roberts 2013).

have to remain in power to be able to pursue any goals, including promises to voters (Ames 1987). Given this, the principal aim of executives, irrespective of their political stance, is to stay in office. Importantly, executives operate within political institutions ("the rules of the game") that shape their incentives (to hold onto power). These institutional incentives, in turn, affect the choice of policies (Geddes 1994). In other words, executives pursue policies, keeping in mind that they need to remain in power, which sequentially depends on institutional settings. (Although the executive can shape institutions as much as institutions shape her/his behaviour, s/he first needs to get to office.)

In sub-section 3.1., I discuss how institutions affect the behaviour of political leaders and the consequent choice of policies in more detail, drawing insights from institutional research (Bueno de Mesquita et al 2003, Acemoglu and Robinson 2013). The main claim is that the institution-structured logic of political survival shapes the available set of policies. In sub-section 3.2., I discuss how particularly distinct institutional setups affect the extent of information control. The key point is that the nature of institutions historically mattered in control of information distributed via the mass media and new technologies. Institutional divergence led to different approaches to the dissemination of information.

3.1. Institutions and political outcomes

In this section, I examine how institutions affect political outcomes by discussing the works of Bueno de Mesquita et al (2003, 2011) and Acemoglu and Robinson (2013). Their main argument is identical: institutions are crucial in politics. For instance, Bueno de Mesquita et al (2003) study how political institutions, defined as "the mechanisms that determine how leaders are chosen or deposed" (2003: 26), affect outcomes in economic, social, and political spheres. The authors have developed the selectorate theory that holds that the size of the selectorate is crucial for the political survival of leaders, thus having an impact on their behaviour and actions. The selectorate is seen as a group of all citizens enfranchised to vote and choose leaders of the country[49] (Bueno de Mesquita et al 2003: 42). The selectorate's most important subgroup is the winning coalition (or essentials) – a minimum number of vital supporters necessary for chief executives to stay in office[50].

Bueno de Mesquita et al (2003) and Bueno de Mesquita and Smith (2011) contend that political institutions, defining the size of the winning coalition, put constraints

[49] The original meaning of the selectorate was narrower, implying only "the group within a [British] political party that has effective power to choose leaders" (Shirk 1993: 71).

[50] In authoritarian countries, the winning coalition is usually a small group of the elite. In the US, for instance, it is "the minimal number of voters who give the edge to one presidential candidate … over another" (Bueno de Mesquita and Smith 2011: 5-6).

on what political leaders can and cannot do. According to the authors, the larger the winning coalition, the more institutionally constrained the executive, and vice versa. Thus, the executive who is dependent on a small size of the coalition – a small-coalition leader – is less limited in the choice of policies to pursue. In comparison, the executive who is dependent on a large number of essentials – a large-coalition leader – is more constrained in the set of available actions. This is because in the first case the leader needs to take care of a small number of people whose support is essential for her/his political survival, whereas in the second case the leader has to keep royal a large group of supporters.

Consequently, Bueno de Mesquita and Smith (2011: 7) argue that the coalition size, having an impact on chief executives' political survival, affect the choice (and quality) of governance policies. The authors found that, as a result of institutional constraints, large-coalition leaders seem to provide public goods whereas small-coalition leaders tend to deliver private rewards[51] – in both cases to keep the winning coalition royal so that to stay in office. Large-coalition leaders "tend to emphasize spending to create effective public policies that improve general welfare" (Bueno de Mesquita and Smith 2011: 11), since by having a large winning coalition it is "too costly to buy royalty through private rewards" (ibid, 11). In contrast, for those dependent on a small number of essentials, private rewards allocated to their small coalitions to gain political support are a more effective way to hold on power. In this case, however, "the mix of public goods is slimmer and trimmer" (ibid, 125). In both cases, political leaders merely pursue the most effective way to secure political survival.

Bueno de Mesquita et al (2003: 93-95, 103) also discuss the role of norms in politics. In particular, the authors argue that the norm of loyalty (affinity) is higher within small winning coalitions since the price for the defection is high. In contrast, within large winning coalitions, the loyalty norm is lower as the price for the defection of essentials from the leader is also low. As a result, there is a relatively distinct allocation of public and private goods. When the number of essentials is small, political leaders provide less public goods (such as the rule of law, social security, and civil liberties) compared to countries with a large winning coalition. In countries with small-coalition leaders, human rights and freedoms are thus not assured and secured. Therefore, according to the authors, institutions-structured political calculations of leaders, which include the coalition size and royalty norms, cause leaders to choose particular governance

[51] The authors consider education, health care, social security, economic growth along with the rule of law and civil liberties as public goods and black market rates, general corruption, and cronyism as private goods (Bueno de Mesquita et al 2003: 104, 179-199, 200-205).

strategies. As I discuss in the following sub-section, this logic of institutional arrangements also extends to the information sphere.

Lake and Baum (2001) also argue that institutional setups affect the quality of public services available to citizens. After conducting a cross-sectional analysis, the authors found that more democratic institutional settings (such as political competition and participation) are conducive to a greater value of public goods such as education and public health, compared to other political systems[52]. In addition, Lake and Baum (2001) similarly contend that politicians, keeping in mind the main aim to stay in power, do not differ in kind but institutional constraints on their autonomy. Therefore, “we should not assume that democratic politicians are innately different from autocratic rulers” (Lake and Baum 2001: 618) as both “differ not in their goals but in the institutional contexts” (ibid, 618). Likewise, D’Anieri (2011: 29) contends that the main goal of politicians, notwithstanding their political ideology, is to stay in office by winning in re-elections, echoing the proposition of the “electoral connection” advanced by Mayhew (1974, 2004).

Acemoglu and Robinson (2013) similarly hold that the nature of political institutions (by structuring incentives of people) tends to influence political and economic outcomes, leading to different approaches to governance – including in media and technology spheres. The authors distinguish between the inclusive and extractive nature of political and economic institutions. Inclusive economic institutions are those that provide a broad segment of society with “secure private property, an unbiased system of law, and a provision of public services that provides a level playing field in which people can exchange and contract” (Acemoglu and Robinson 2013: 74-75). In contrast, extractive economic institutions feature the opposite characteristics, being devised to extract the fortune and capital from one (large) part of society to enrich another (small) part (ibid, 76).

Political institutions, in turn, “determine how the government is chosen and which part of the government has the right to do what. Political institutions determine who has power in society and to what ends that power can be used” (ibid, 79-80). Thus, in societies where political power is distributed in favour of a small group with a few constraints on their authority, political institutions are extractive. On the other hand, inclusive political institutions are those where political power is dispersed more evenly, that is, “rests with a broad coalition or plurality of groups” (ibid, 80), and the chief executive’s authority is circumscribed. Leaders operating under extractive and inclusive

[52] In this regard, Frantz (2018) maintains that economic development is also associated with more democratic systems: “[r]icher countries are more likely to be democratic, and poorer countries are more likely to be authoritarian” (2018: 17), albeit there exist some exceptions such as oil-rich states. The main statement is, however, that democracies tend to perform better in terms of economy and public goods provisions than autocratic regimes.

institutional settings closely match small-coalition and large-coalition leaders, respectively[53]. It is also of note that institutionalists, in general, tend to define political institutions in a very similar fashion, seeing them as directly related to the balance of political power and allocation of resources. As Lowndes states, political institutions are seen as the rules of the game that “distribute power, because they specify who has access to resources and decision making” (2018: 61, 63).

According to Acemoglu and Robinson (2013), some countries have become prosperous, developed, and industrialised with greater respect for freedoms and rights, including in the digital domain, due to having inclusive political and economic institutions[54]. On the other hand, extractive institutions lead to inequality, underdevelopment, and poverty with less effective rule of law and more constrained civil liberties – and therefore less freedom in cyberspace. This happens because extractive and inclusive institutions create different incentives, which in turn lead to different political and economic outcomes[55].

This line of thought concurs with the arguments of Bueno de Mesquita et al (2003) who similarly contend that small-coalitions leaders, due to having to retain the loyalty of only a small number of supporters, do not provide core public goods. The situation with regard to public policies improves, however, when the size of the winning coalition becomes larger as in this context “the prospects of political survival increasingly hinge on successful policy performance” (Bueno de Mesquita et al 2003: 263). In addition, both Bueno de Mesquita et al (2003) and Acemoglu and Robinson (2013) resort to historical case studies to test their propositions. For instance, Acemoglu and Robinson (2013) argue that the goodwill of leaders is seldom the main reason why some nations have inclusive institutions while others have extractive ones. The development of institutions is mainly tied to historical critical junctures that slowly but gradually paved a path to the emergence of either inclusive or extractive institutions[56].

[53] Consequently, in the following chapters, I use both concepts (extractive/inclusive institutions and small-/large-coalition leaders) interchangeably.

[54] Acemoglu and Robinson (2013) maintain that political institutions determine economic institutions.

[55] Although there can be exceptions when countries experience the economic growth under extractive institutions, the development can only be temporal, according to Acemoglu and Robinson (2013). One of the examples is the economic growth in the Soviet Union, between the 1930s and 1970s, under extractive political (strong grip of the Communist Party over society) and economic (state-commanded economy policies) institutions. The authors argue that the Soviet economy progressed because resources were allocated into industry at the expense of the agricultural sector. However, the growth could not be sustained as extractive institutions did not foster investments, technological development, and innovation, leading eventually to economic stagnation.

[56] For instance, critical junctures such as the 17th century Civil War and Glorious Revolution in England. According to Acemoglu and Robinson (2013), these historical events were crucial for

In this regard, the authors found that in nations where the ruler's authority was not defied or civil society's resistance against the existed political order failed, more extractive institutions persisted. On the other hand, inclusive political institutions have gradually taken roots in societies where a broad part of people was eventually mobilised and empowered, challenging the political order that was not in their favour. As a result, the large section of society that managed to defy the status quo has acquired more rights and freedoms and enabled a fairer redistribution of political power. The media and new technologies, as I discuss in the following sub-section, can significantly contribute to the empowerment of society.

3.2. Institutions and information control

The media, including its new forms, can facilitate the coordination between people, informing and motivating many citizens to demand changes of extractive structures, which might lead to protests and more importantly to regime change. The mass media can thus become an explosive tool in the hands of people, subjecting political leaders and organisations to accountability and transparency. It is thus unsurprising that the media appeared to be specifically controlled in countries with extractive political institutions[57], given that (small-coalition) leaders are well aware of media's potential to empower people to rally against the existing state of affairs (Acemoglu and Robinson 2013: 461-462). The chief executives, feared for their political life, have eventually resorted to control of the media and the free flow of information in their countries. In contrast, the media tends to thrive under inclusive institutions as the latter provide for the rule of law and fair rules of the political game[58] (ibid, 309, 325).

Different survival strategies and corresponding policies with regard to the media (and new technologies) are therefore pursued *depending on* institutional contexts in which executives operate. The mass media theories (Siebert et al 1956) support this statement, claiming that the media is a "servant of the state" functioning "from the top down" (1956: 2-3) in the authoritarian context. Crucially, Seibert et al similarly contend that institutional settings affect control of the mass media: "the press always takes on the form and coloration of the social and political structures within which it operates" (1956: 1). Thus, within authoritarian (extractive) arrangements, the mass media is controlled by

the development of inclusive political and economic institutions in England since the existed political order was challenged and the autonomy of the Crown was significantly undermined while the parliament was empowered. As a result of more evenly distributed political power, a broader part of society eventually received more rights and freedoms than they used to have.

[57] I use extractive/inclusive political institutions interchangeably with small-/large-coalition leaders.

[58] Bueno de Mesquita et al (2003) also contend that the logic of political survival extends to such public goods as freedom of speech and freedom of media (including in cyberspace).

the state, being merely an instrument of the government. On the other hand, freedom of speech and freedom of the press are secured in states operating under liberal (inclusive) principles[59].

Djankov et al (2003) also found that more authoritarian states exercise greater control over the media. This tendency happens because the authoritarians – those reigning over extractive institutions – fear the potential power of the media (McMillan and Zoido 2004). The news outlets and TV channels can expose the wrongdoings of politicians to a mass audience, serving as a check on governments and their policies. As a result, leaders of authoritarian countries, according to McMillan and Zoido (2004), put more efforts (and money) to co-opt the media rather than representatives of political opposition and judiciary. The media, thus, is of more priority for authoritarians' survival in office. That is why the mass media is recognised as the fourth estate that performs watchdog functions whereas its freedom is associated with a democratisation process (Lawson 2002). Moreover, with the rise of digital technologies and the consequent transformation of the media into the "networked fourth estate" (Benkler 2011), the internet, too, appeared under control in countries with extractive institutions. However, as I discuss below, the internet was not the first and only new technology that became opposed or controlled by political leaders.

In addition to the mass media, technological change was also often feared and opposed by those in power as new technologies could disrupt the existed political order. For example, long before the internet, the invention of the printing press in the middle of the 15th century shook the balance of political power at the time (Naughton 2012: 15). Unsurprisingly, the Catholic Church opposed the innovation in printing since its authority in interpreting the Bible significantly decreased (ibid, 17-18). The Church "was not subject to deviant secular interpretations", continuously limiting the probing on religious canons by individuals outside of its hierarchy (Seibert 1956: 17), whereas the printing press facilitated a faster exchange of opinions opening a door to alternative views. If previously the Catholic Church was able to silence its critics (for example, Jan Hus) without great consequences for its authority, then after the invention of the printing press it became much more difficult to do since critical writings (for example, of Luther) were distributed in a faster fashion (Briggs and Burke 2017: 63).

Rulers of the Ottoman Empire reacted in a similar way, banning Muslims to print in Arabic (Acemoglu and Robinson 2013: 213). The logic of Ottoman rulers' decision to

[59] Also, Seibert et al (1956), resorting to historical examples, argue that the expansion of political representation and participation was a crucial factor in the centuries-long process of turning the printed media into a relatively independent and free from the state's involvement. The change of political institutions, in other words, mattered in the freedom of media.

resist the printing press was also an attempt to preserve the existed political order. The distribution of books could mobilise and empower people, threatening the status quo – those in power simply did not want to share their political and economic power. "Books spread ideas and make the population much harder to control" (ibid, 215). Although some ideas could contribute to economic progress, the Ottoman leaders feared that other ideas might become rebellious. Hence, the printing was prohibited. Later, in the 18th century, one printing household was allowed to operate, though the issue of books was limited and was subject to prior censorship (Savage-Smith 2003: 658). The cause for the strict regulation of the printing process was (again) the fear "that more social unrest would result from this inexpensive means of communication" (ibid, 658). Consequently, the printing enterprise did not last too long and was eventually shut down.

Beyond the Middle East, many states in western Europe, between the 16th and 18th centuries, also sought to control the printed media after the advent of the printing press and consequent increase in books' publications (Seibert 1956: 19-25). For that reason, they resorted to three main methods. The first one was a selective issue of monopoly patents to favourable publishers and printers. The second was the licencing system of the press in the form of censors to keep "privately owned printing and publishing establishments under official control" (ibid, 21). The third instrument in the state's arsenal was a prosecution of individuals distributing anti-governmental materials and opinions. In addition, at that time the authorities resorted to more subtle methods such as co-optation of writers and secret state-funding of independent newspapers (ibid, 25). As can be seen, mostly all of these methods of the post-Gutenberg era are still in action in many modern nation-states, having been effectively applied to the mass media and internet.

The main point is that those in power, who operate under extractive institutions, fear technological innovations. This is because new technologies could bring about a "creative destruction", introduced and defined by Schumpeter (2010: 73) as "the organisational development … that incessantly revolutionizes the economic structure *from within* [cursive in original], incessantly destroying the old one, incessantly creating a new one". The creative destruction could undermine not only commercial privileges of the elite but also the balance of political power. Political leaders, frightened of such consequences, largely opposed the development of inclusive institutions in general and the introduction of new technologies in particular. As a result, technological change – that, like the mass media, was believed to empower a large number of people and lead to the revision of the political game's rules – was often resisted within extractive institutional settings. This was a case with the printing press invented in the 15th century;

the reluctance to build steam railways by the Austro-Hungarian and Russian governments was another example.

In the 19th century, the economic and political order in both Austria-Hungary and Russia was largely based on feudalism and serfdom. Consequently, leaders in both states opposed the introduction of steam railways as they feared that technological innovation "would bring a socially dangerous mobility" of citizens (Acemoglu and Robinson 2013: 230), which could result in revolution. The leadership in both the Habsburg and Russian empires understood that the new technology could thus destabilise the support of the elite needed for their political survival. As a result, until the mid-19th century, in Austro-Hungary under the rule of Emperor Francis I, horses were still used to pull rail cars (ibid, 226). Similarly, the Russian government, frightened of the creative destruction that industrialisation could bring, also opposed the development of steam railways[60]. Under the rule of tsar Nicholas "policies were aimed at strengthening the traditional political pillars of the regime, particularly the landed aristocracy" (ibid, 228). In countries with extractive institutions, a new technology of the day could have led to the opening of political institutions, endangering leaders, and thus was often resisted[61].

In addition, the logic of political survival played a significant role in the initial decision to oppose the telegraph in Russia. The tsar refused to fund the telegraph project advanced by Morse because he considered it a subversive technology (Spar 2001: 68). Thus, the introduction of the telegraph and steam railways was not initially approved in the Russian Empire due to the fear that new technologies would empower citizens and undermine the government. It is of note that American, English, and French governments also did not support the telegraph in the beginning but due to commercial reasons. At the outset, a new technology of the day "was evidently not regarded as a useful form of communication" by politicians, the public, and the press (Standage 1999: 50). The attitude toward the telegraph was, however, slowly shifting and by the middle of the 19th century it already operated in all main European countries. Yet the latter, ostensibly for security reasons, used to censor and intercept messages sent across their lines (Spar 2001: 81, Standage 1999: 114).

The pretext of national security also resulted in control of radio, which was deemed a disruptive innovation since messages could be broadcast across borders,

[60] The importance of railways in Russia was reconsidered after defeat in the Crimean war (1853-1856).

[61] A more modern example is Sierra-Leone. In the post-colonial period, in the 1960s, the then ruler of the country (Siaka Stevens) ordered to disassemble railways to disrupt the trade and exports of his political rivals (Acemoglu and Robinson 2013: 336-337). Although, as a result, Stevens managed to eventually centralise political power in his hands, the negative effects of that decision on Sierra-Leone's economy were huge.

challenging state control over information flows (Spar 2001: 126-127). While the printed press could be checked at the state border if needed, radio signals were passing through and over physical objects, being obviously intangible, representing a novel potential threat to state security. As a result, the protection of national interests and welfare led many European countries to heavily regulate radio services at the beginning of the 20th century. England, France, Germany, Russia, and Italy considered the emerging radio a crucial mass communication tool, especially at the time of war, and therefore decided to control it from the outset (Spar 2001). Consequently, the wireless radio by the end of WWI "was seen not just as a vital naval technology, but also as a vital security technology – an instrument of power and of war" (ibid, 144). (As I demonstrate in chapters 5-7, many modern states resort to internet control tactics also ostensibly on the grounds of providing national security.)

However, in other instances, the promotion of national interests and safety also led to information control. For instance, Germany during the first half of the 20th century – in the midst of the global geopolitical contest – increasingly invested in wireless telegraphy so that to distribute international news from the German point of view to the rest of the world, according to Tworek (2019). As the author contends, the German government, keeping in mind the aim to shape the world information landscape like its Anglo-American counterparts, also subsidised the main domestic news outlets, becoming able to control their agenda and narratives. In that way, control of the communication infrastructure (wireless telegraphy) and leverage over the means of news production (local newspapers) allowed the country to follow its imperialistic ambitions, albeit at the expense of freedom of information – world news made in Germany were manipulated by its government.

In essence, the mass media and new technologies – and information distributed through their mediums – were deemed instruments that could jeopardise the leader's hold on power and (ostensibly) national security and interests of the country, resulting in their consequent control. That the fast exchange of information and communications is crucial for political survival can also be seen from Vladimir Lenin's actions in the wake of the 1917 October Revolution. Shortly before the revolution, Lenin urged to take control of the telephone and telegraph lines so that to mobilise protesters to rally against the existed regime (Soldatov 2019). After the Bolsheviks seized the power, the first orders of Lenin "were to close down the non-Bolshevik press" (Volkogonov 1999: 74) in order to suppress the opposition. In other words, Lenin perspicuously understood the advantages and disadvantages of mass communication and media for the survival of political leaders and institutions. When Lenin opposed those in power in 1917, he sought to seize the communication channels for better coordination and organisation of the revolution; when Lenin himself took the power, he immediately restricted the circulation of opposition press as he sought to consolidate his and the Communist Party's authority in the country.

Eventually, in the Soviet Union, the press and later the broadcasting systems such as radio and TV became state-owned, being an instrument and continuation of the Communist Party (Schramm 1956). The latter was the chief regulator, censor, and controller of media and technology spheres. The newspapers and radio largely promoted and propagated the political line of the party to a respective audience. In addition, radio signals of foreign stations were jammed, albeit not always successfully, so that the Soviet people could not learn of the alternative interpretation of political and social issues (Kotkin 2001: 41). Moreover, personal "telephones were kept to a minimum – twenty-five million, fewer than one for every ten people – and typewriters had to be registered with the police" (ibid, 42). Control of communication technologies and information flows was extensive in the Soviet Union since their role in the empowerment of civil society vis-à-vis the government was perfectly understood by Lenin's successors.

The logic of political survival of those in power also played its role in the destiny of Soviet cybernetics politics. The Soviet engineers tried to build a national network of interconnected computers – under the name of All-State Automated System – that would facilitate the management of the Soviet command economy (Peters 2017, Gerovitch 2008). Yet despite numerous attempts, the project was not successful as the extractive nature of institutions did not encourage the development of the "Soviet Internet". Military leaders, along with government bureaucrats, feared that the implementation of a new interconnected network for the economy management would threaten their (privileged) positions and jobs making them superfluous, whereas the Party leadership became indifferent to the initiative (Peters 2017: 191-192, 194). In due course, the Soviet Union drastically lagged behind its main global competitor, the United States, in designing information systems as well as in possessing computers. The manufacturers in the Soviet Union became merely unable to produce competitive communication technologies (Kotkin 2001: 63). In the 1980s, there were only "200,000 microcomputers, leaving aside their quality, while the US already had 25 million, and that number was about to skyrocket" (ibid, 63-64).

Yet, it shall not be surprising that the Soviet leaders and institutions feared and tightly controlled all means of communication and information production, given that the nature of political institutions in the Soviet Union was irrevocably extractive. The ultimate power rested in the Communist Party's Politburo and primarily the General Secretary (small winning coalition), whereas the extended number of committees and party rank-and-file merely executed orders already made on the top of the political hierarchy (Lewin

2016: 46). Thus, due to extractive institutional settings and because political leaders of the Soviet Union were absolutely reluctant to “envisage any permanent sharing of power” (Kennan 1947: 569), which the free press and communications technologies could otherwise have enabled, the media and technology fields were closely supervised and controlled. The only Soviet political party, like the Church in the 15th century, was intolerant to alternative voices, allowing “no substantial deviations in ideology” (Schramm 1956: 118).

Although there can be numerous examples of a strict approach to the media and new technologies, the tendency is clear. The institutional context dictated executives whether to regulate information distributed with the help of the media and new technologies in a rigorous manner, becoming the main source of extensive control. The distinct nature of political institutions led to various extents of control over the mass media and information and communication technologies. As can be seen, the press and new technology of the day threatened the political survival of leaders, specifically those reigning within extractive political institutions. As a result, those in power attempted to control the mass dissemination of information and communications as extensively as institutional settings allowed.

In this regard, the internet, like its predecessors and the printed media, also targets the political survival of leaders, providing inclusivity to a large part of society. Due to its many-to-many structure, the internet can challenge those in power, specifically under extractive institutions, allowing citizens to quickly share information and instantly communicate with one another. The internet extends demands for a wider representation and (alternative) voices, subjecting political entities and actors to accountability and transparency. Furthermore, the internet has become associated with the democratisation, being perceived as an instrument that significantly facilitates and coordinates (anti-government) protests and uprisings, empowering civil society vis-à-vis a state apparatus (discussed in chapter 2). The remaining autocrats are perfectly aware of numerous ostensibly internet-enabled regime changes. If not in the form of revolutions, negative information distributed over the internet can affect the popularity and rating of politicians, costing them votes in elections[62]. In other words, there are many reasons for political leaders to treat the internet with suspicion.

It is thus no exaggeration to suggest that the internet’s advent into the masses in the 1990s and the ensued growth of internet users’ number have become another challenge for many governments, especially those with extractive institutions. Like the

[62] Enikolopov et al (2011), for instance, found that in democracies negative information can cost votes to pro-government parties while the independent mass media may strengthen the stance of opposition parties.

19th-century rulers who initially opposed the development of telegraph and steam railways fearing that it could empower society and result in revolution, their 21st-century counterparts similarly fear the internet's potential to mobilise citizens against the existing political order, which is not in favour of the latter. Given that leaders within the extractive institutional context do not share political power with the rest of the population so that they can keep a privileged position and secure survival, they oppose or control new technologies. That is why many leaders have already opted to control the internet. Otherwise, they risk losing everything.

Although information and communication technologies evolved throughout the centuries, the government's attitude toward them did not substantially change. Leaders operating within extractive institutional arrangements controlled (and continue to control) the flow of information enabled by new mediums within their countries, whereas leaders presiding over inclusive institutions were restricted in their authority to exercise control over the media and technology sphere. The internet, following the logic of political survival, is destined to repeat the path of its predecessors and the mass media. Thus, the initial propositions are that the internet is controlled in countries with extractive institutions (or small-coalition leaders) while the extent of internet control is expected to be limited in countries with inclusive institutions (or large-coalition leaders)[63].

4. CONCLUSION

In this chapter, I discussed the interplay between the logic of political survival and information control, drawing insights from the new institutionalism. First, I reviewed how normative, rational choice, and historical institutionalism see institutions. The normative approach argues that the logic of appropriate behaviour affects the political conduct of actors and consequent political outcomes through institutional norms. The rational choice version maintains that institutions structure incentives, influencing the choice of policies. Historical institutionalism considers the initial ideas and values that have been embedded in the creation of institutions as determining the political behaviour of individuals. Notably, these three key institutional versions overlap in many theoretical aspects, having more similarities than differences. As a result, institutionalists tend to apply the eclectic approach in their political analyses.

Next, I discussed the effects of institutions on political outcomes and the role of institutions in the media and technology domains, following institutionalists (Bueno de

[63] I do not hold that control of information on the internet is absent in countries with inclusive institutions as we have learnt that democracies (countries with inclusive institutional settings) also resort to information controls (chapter 2). However, given the lack of studies in this direction, the initial proposition is that the extent is limited.

Mesquita et al 2003, Acemoglu and Robinson 2013) who also adopt the eclectic approach in their studies. Bueno de Mesquita and Smith (2011), for instance, argue that, as a result of political institutions, there can be either small-coalition or large-coalition leaders. The former need to take care of a small number of supporters and thus are less constrained in their actions. The latter must consider a bigger number of supporters to stay in power, thus being more restricted in their authority. Likewise, Acemoglu and Robinson (2013) distinguish between two types of institutions: extractive and inclusive. Overall, extractive institutions closely match small-coalition leaders whereas inclusive institutions are similar to large-coalition leaders. In both cases, the political authority of those in power is either unconstrained or significantly limited. Thus, institutional settings determine what political leaders can and cannot do, affecting their choice of policies.

Importantly, institutions affect the extent of control over information, including on the internet. Executives presiding over extractive institutions (small-coalition leaders) are in a position to control the internet as the free flow of digital information can pose a great threat to their hold on power (that is, threaten their political survival). Whereas the set of actions available to executives operating within inclusive institutions (large-coalition leaders) is more constrained. In this case, the extent of state engagement with the internet is expected to be less extensive (though not completely absent). Thus, drawing insights from institutional research, the proposition is that distinct sets of political institutions (extractive/inclusive), differently generating survival strategies, have a various impact on the extent of internet control (extensive/limited).

Previous examples of how governments historically treated the mass media and new technologies of the day underpin the claims. Political leaders operating within extractive institutions opted to resist the introduction of innovative products such as the printing press, telegraph, radio, and even steam railways due to the fear that the new would substitute the old. That is, new technologies could challenge the existed status quo – the privileged position of a small group of people – by empowering a large segment of society. Small-coalition leaders, in other words, did not want the change of extractive institutions. The institutional logic of political survival led to the rejection or extensive control of technologies; the same logic is applied to the internet.

Consequently, after having elaborated the theoretical framework, the next step is to consider an appropriate method to explore the proposed causal relationship between the institution-structured logic of political survival and internet control. Thus, in the following chapter, I discuss a qualitative comparative analysis (QCA) (Ragin 2008), which is applied to study the causal interplay between research variables. In addition, I formulate the research questions, aims, and hypotheses and provide the definitions of the main research concepts. Also, a model of internet control that incorporates main information controls is offered in the following chapter.

CHAPTER 4. METHODOLOGY: A QUALITATIVE COMPARATIVE ANALYSIS

1. INTRODUCTION

In the previous chapter, I discussed institutional theory and how it can be applied to the study of internet control. Drawing insights from prior research and theory, the main proposition was that the nature of political institutions, shaping the logic of political survival, affects the extent of internet control. In this chapter, I provide a methodology to study the effects of institutions on the course of state control over digital information. Consequently, I first discuss the research questions, aims, and hypotheses, and then proceed to the method of the qualitative comparative analysis (Ragin 2008), a tool that helps unveil the causal relations between independent (a condition) and dependent (an outcome) variables.

Following previous research and institutional theory, the main question of my study is related to conditions of state control over digital information, specifically the (expected) relationship between the nature of political institutions (the main condition) and the extent of internet control (the outcome). In case the causal relations between variables are established, the question is how and to what extent political institutions affect the implementation of information controls. On the other hand, if I fail to identify any patterns and regularities between the condition and the outcome or if causation is too weak, I raise a question of other additional conditions of internet control, apart from or in addition to political institutions.

Consequently, I hypothesise that there is a connection between political institutions and control of information on the internet: extractive institutional settings lead to significant control, whereas inclusive institutions lead to limited state interference with digital information. To test my hypotheses, I first conduct a comparative analysis of sixty-five countries to identify any patterns and regularities between variables (chapter 5). After that, I narrow down my focus to two case studies to refine the findings drawn from the comparative analysis (chapters 6 and 7). In this regard, the aim is to explore and explain the impact of political institutions, along with other possible additional conditions (if there are any), on the dissemination of digital information.

To unveil the causal relations between the hypothesised condition (the nature of political institutions) and the outcome (the extent of internet control), I resort to the method of the qualitative comparative analysis (QCA) advanced by Ragin (2000, 2008) (section 3). The QCA provides necessary tools to explore the interplay between research variables. To apply the method, I first conceptualise and calibrate the key concepts employed in the study (sections 4 and 5). I provide the definitions of, and the way I measure, the extent of internet control and the nature of political institutions. For instance, to study the former, I develop a model of internet control that incorporates main information controls. After that, a calibration of variables to gauge sufficiency, necessity, consistency, and coverage of condition in relation to the outcome is provided. Finally, I explain how I conduct two case studies (section 6).

2. RESEARCH QUESTIONS, AIMS, AND HYPOTHESES

In the previous chapter, drawing insights from institutional theory, I proposed that the nature of political institutions affects the extent of internet control. Countries with more extractive political institutions (small-coalition leaders) are expected to control information on the internet to a greater extent than countries with more inclusive institutions (large-coalition leaders). To test this proposition, I examine the causal relations between political institutions and state control over digital information. In other words, I study whether and, if so, how political institutions affect the extent of internet control.

Accordingly, the research questions of my study are as follows. Under what conditions do states control the digital flow of information? In particular, what is the relationship between the nature of political institutions and the extent of internet control? How (and to what extent) do political institutions shape the extent of internet control? If political institutions have no (or minor) impact, what are other possible conditions of state control over digital information? Consequently, my research hypotheses, based on prior research and institutional theory, are that political institutions affect internet control: countries with extractive political institutions (small-coalition leaders) have extensive control of information on the internet (H1), whereas countries with inclusive political institutions (large-coalition leaders) have limited control of digital information[64] (H2) (figure 2).

My research aim, as mentioned above, is to explore and explain the effects of political institutions (and other possible conditions) on the course of internet control. That is, whether the distinct nature of institutions leads to different extents of control over information on the internet. To reach the research aim, I identified two main objectives of my study. The first is to examine political institutions and the extent of internet control in sixty-five countries to identify general patterns and regularities (if they exist) between the former and the latter. Consequently, in the following chapter, I conduct a comparative

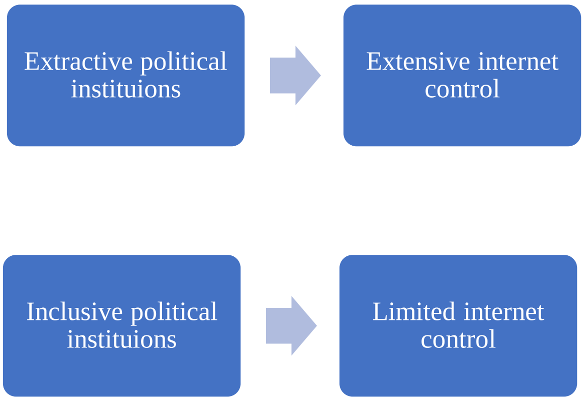
[64] As noted in chapter 2, it is known that democracies (that is, countries with inclusive institutions) tend to resort to information controls. However, the extent of their interference with the internet has not been recently studied. Consequently, the initial proposition is that internet control within inclusive institutions is limited but not absent.

analysis to explore the causal relations between the hypothesised condition (the nature of political institutions) and the outcome (the extent of state control over the internet).

After identifying possible generalisations between political institutions and internet control, the second objective is to further analyse and refine the impact of institutions (and additional conditions) on state control over digital information. To broaden the study of whether and, if so, to what extent political institutions shape the extent of internet control, I resort to the case studies[65]. I study the development of domestic political institutions and their influence on the course of control over information flows in two countries. In chapter 6, I analyse the interplay between extractive institutions and the dissemination of digital information (Kazakhstan), and in chapter 7, my focus is on internet control within inclusive institutional settings (Ukraine).

Consequently, these two steps help to identify and study conditions of state interference with digital information and also conclude whether the institutional context is crucial for internet control.

Figure 2. Research hypotheses


Extractive political instituions
Extensive internet control
Inclusive political instituions
Limited internet control

3. QUALITATIVE COMPARATIVE ANALYSIS

My research seeks to explore and examine conditions of internet control. The main proposed condition is the nature of political institutions. To study the causal interplay between various institutional settings (such as extractive and inclusive) and the extent of control over digital information, I apply a method of the qualitative comparative analysis (QCA) as it is more appropriate for the outlined research aim.

[65] In addition, the case studies appeared to be necessary as the comparative analysis of sixty-five countries (chapter 5) only partly confirmed the research hypotheses. I found that extractive political institutions lead to significant control of digital information (79% of consistency), whereas the inclusive nature of institutions does not necessarily lead to the limited extent of internet control (53% of consistency).

Statistical techniques also allow the identification of potential causal relations within a large number of cases but they are less appropriate to study causal paths in detail. Meanwhile, small-N case studies allow the examination of detailed causal mechanisms but they are less suitable to make broad generalisations of findings. The QCA, however, provides a middle ground between in-depth small-N studies and quantitative large-N studies as it enables an analysis of causal relations between independent and dependent variables (a condition and an outcome) beyond one or few cases. The comparative method mitigates the limitations of conventional case-oriented qualitative and variable-oriented quantitative approaches, combining case-based and cross-case nature of social research (Ragin 1987, 2000).

Consequently, based on Boolean algebra, the QCA makes it possible to examine the complex causal relations and identify whether a condition (or a combination of conditions) is a sufficient or necessary aspect of the outcome within a small, middle, or large number of cases (Ragin 2008). Only after identifying the causal interplay between political institutions and internet control, I conduct two case studies to deepen and strengthen the findings of the comparative analysis (section 6). In this section, I outline the main aspects of the comparative method.

Overall, there are three important characteristics of the QCA that define how it works. First, it operates under membership sets, in which a concept (condition and outcome) has a membership score of 0 or 1 such as in crisp sets (dichotomous range of variables), or a score from 0.0 to 1.0 such as in fuzzy sets (continuous gradation of variables). In the latter case, a score of 0.0 means full non-membership of the concept in a set, a score of 1.0 displays full membership, and a score of 0.5 indicates neither full membership nor full non-membership (indifference point). Accordingly, fuzzy sets are more detailed as they have three qualitative anchors: full membership (1.0), full non-membership (0.0), and a point of indifference (0.5), whereas simpler crisp sets are dichotomous with only full membership (1) and full non-membership (0) (Schneider and Wagemann 2012: 31). In addition, there can be a different number of values in a membership score of fuzzy sets: three, four, six, seven, or continuous values (Ragin 2008: 31). Thus, fuzzy sets are able to provide “difference-in-kind between cases (qualitative difference) and add to this the ability to establish difference-in-degree (quantitative difference) between qualitatively identical cases” (Schneider and Wagemann 2012: 27).

Crisp and fuzzy sets can also be translated into a truth table, which is a key tool of the QCA. The truth tables are aimed at exploring “explicit connections” of configurations of conditions with an outcome by listing all “logically possible combinations of causal conditions and the empirical outcome associated with each configuration”

(Ragin 2008: 23-25). After studying the various possible configurations of conditions related to the outcome, the next step is to reduce these recipes to the smallest possible number of configurations by applying the Boolean logic (Halperin and Heath 2012: 220). Thus, the truth tables provide "a framework for comparing cases as configurations of similarities and differences while exploring patterns of consistency and inconsistency with respect to case outcomes" (Ragin, 2008: 25).

The second characteristic of the QCA is that a condition or combination of conditions can be either a subset or superset of the outcome (figures 3 and 4). That is, whenever a condition occurs, the outcome also takes place, meaning that the condition is a subset of the outcome; and vice versa (Schneider and Wagemann 2012: 76). For example, if I hypothesise that the extractive nature of political institutions (a condition) leads to extensive control of information distributed over the internet (an outcome), then I assume that the former is a subset of the latter. Another consequence of the condition being the subset of the outcome is that this condition (extractive institutions) is not the only factor leading to the outcome (extensive internet control); there might be other factors prompting extensive control, in addition to political institutions. Thus, the condition in this example can be sufficient but not necessary for the outcome to appear. Necessary conditions, in contrast, are supersets of the outcome: whenever the outcome occurs, the condition takes place as well (Schneider and Wagemann 2012: 69).

Consequently, in the causal relations, a condition or combination of conditions leading to a particular outcome can be either a sufficient or necessary attribute of the result. The QCA, by applying a fuzzy-set data matrix and truth table analysis, allows for the identification of sufficiency and necessity of conditions for the outcome. In other words, the identification of set-subset relations is important for the analysis of the causal relationship between variables.

Figure 3. Condition is a subset of the outcome

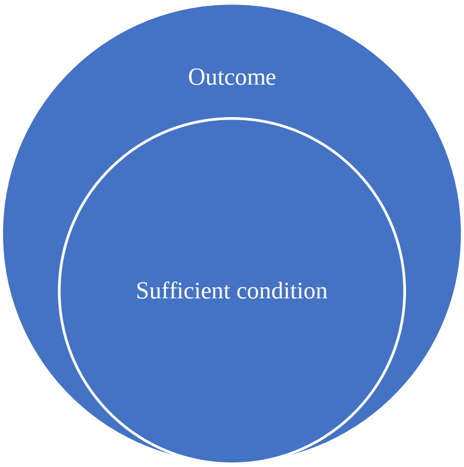


Figure 4. Outcome is a subset of the condition

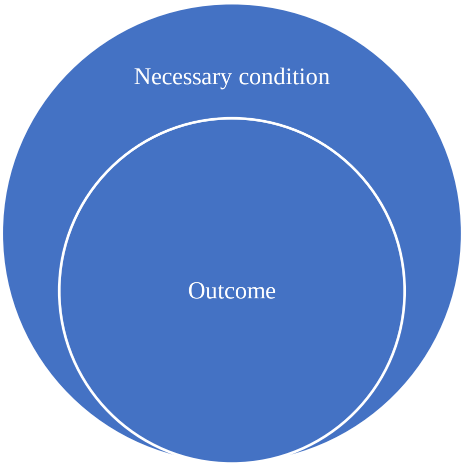
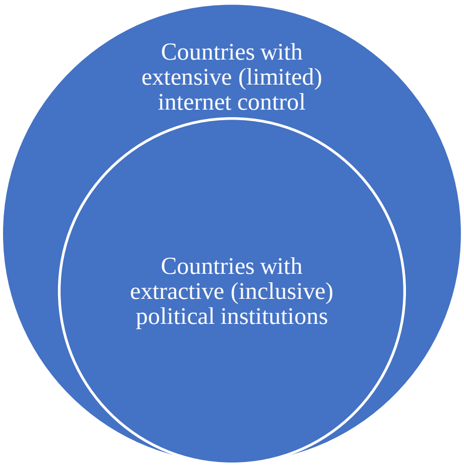


Figure 5. Nature of political institutions (condition) is a subset of internet control (outcome)


Countries with extensive (limited) internet control
Countries with extractive (inclusive) political institutions

The third characteristic of the QCA is the asymmetrical nature of causal relations (Ragin 2008). For example, the assumption that all states with extractive political institutions exercise substantial control of digital information (sufficient condition) does not *necessarily* imply that all countries with significant internet control have extractive institutions. The fact that there might be a country with inclusive institutions that exercises extensive control of digital information will not undermine my hypothesised argument that all countries with extractive institutions regulate information on the internet with a heavy hand. This is because the set of countries with extractive institutions is a *subset* of the set of countries with extensive control of digital information (figure 5). Also, I cannot claim that all states with inclusive institutions *automatically* have insignificant (that is, limited) internet control, in case extractive institutions lead to extensive control. This is because asymmetrical relations imply that "the explanation of the occurrence of an outcome does not necessarily help us much in explaining its non-occurrence", requiring to analyse both the occurrence and non-occurrence of the outcome separately (Schneider and Wagemann 2012: 81, 89).

As Ryan (2018: 273) maintains, “[w]e study politics so that we can better understand and explain political outcomes. One important way of explaining an outcome is to identify causation”. One of the strategies to identify potential conditions of an outcome is to find whether cases with the same or similar conditions also share the same outcome; the second strategy is to identify similarities between cases with the same outcome as they may suggest significant empirical connections (Ragin 2008: 17-18). In terms of my research, I argue that countries with more extractive political institutions (the same or almost same condition) share the same or similar outcome, which is the substantial extent of internet control. Whereas countries with more inclusive political institutions have more limited control over information online.

In order to identify whether the differences in political institutions lead to either extensive or limited internet control, I first need to establish whether conditions are *necessary or sufficient* for the outcome. According to the fuzzy-set logic (Ragin 2000, 2008), a condition is sufficient if membership scores of the condition are repeatedly equal or lower than membership scores of the outcome (scores of all cases that range from 0.0 to 1.0 are compared). In that case, the condition is a subset of the outcome. The condition is necessary for the outcome if membership scores of the condition are mainly equal or higher than membership scores of the outcome. In that case, the condition is a superset of the outcome. Thus, the sufficient condition means that when it is present, then the outcome is present too. The necessary condition means that when the outcome is present, then the condition is present too.

After establishing necessity or sufficiency, I assess the *consistency and coverage* of conditions. The consistency of sufficient condition measures to what extent cases with same or similar conditions display the outcome (the extent of internet control), demonstrating its significance. The coverage of sufficient condition assesses to what extent “a cause or causal combination “accounts for” instances of an outcome” (Ragin 2008: 44), demonstrating its empirical weight. The consistency of necessary condition, in contrast, measures to what extent cases with the same outcome display the condition or (a combination of conditions). The coverage (empirical relevance) evaluates to what extent “instances of the condition are paired with instances of the outcome” (Ragin 2008: 45).

The consistency is expected to be as close to 100% as possible; in case the rate is less than 75% (0.75), then “maintaining on substantive grounds that a set relation exists, even a very rough one, becomes increasingly difficult” (Ragin 2008: 46). Thus, I consider the research hypotheses to be confirmed when the consistency is equal to or higher than 75%. To calculate necessity, sufficiency, consistency, and coverage of conditions, I use “fsQCA 3.0” software specifically designed for the QCA computations[66].

Finally, it can be noted that the qualitative comparative analysis has been widely employed within social science (e.g. Vis 2009, Pennings 2003) and beyond (Jordan et al 2011). The comparative method was also used in internet studies. For instance, Howard (2010) applied the QCA to explore the causal relations between information and communication technologies and the democratisation process in Muslim countries. In addition, Hussain and Howard (2013) used the method of the QCA to identify causes of the Arab Spring in 2010-2011, in which digital technologies were credited with the organisation and coordination of street protests.

4. CONCEPTUALISATION AND OPERATIONALISATION

4.1. Model of internet control

In this sub-section, following how countries control information online within national borders (discussed in chapters 1-2), I present a model that incorporates the main tactics of state interference with digital information (table 1). The model is used to study the extent of state control over the internet in general and in relation to political institutions in particular. Overall, I have six main tactics employed by countries to shape and limit the dissemination of digital information[67]. These are censorship of online content through filtering and blocking (censorship due to pornography and copyrights issues is not included in this category); disruption (or shutdown) of communication networks; manipulation of public opinion via social media; the punishment of users for internet activities (for example, arrests, prosecution, fines, detainment); restrictive internet legislation that expands state powers in the digital sphere; and dominance of internet infrastructure. The main actor in my study is the “core executive”: a government and state agencies.

To conduct a comparative analysis of internet control, I collect data from numerous secondary sources. The main, but not the ultimate, source is reports of Freedom House, one of a few organisations that systematically studies freedom of the internet[68]. Freedom House’s annual and country reports provide evidence of internet

[66] Software is available from http://www.socsci.uci.edu/~cragin/fsQCA/software.shtml

[67] I refrain from including state-organised cyberattacks and covert surveillance in the model as it is not possible to definitely identify the state’s role in all cases. However, in two case studies (chapters 6-7), I collect evidence in an attempt to explore the state’s participation in cyber operations.

[68] I do not use the final scores of internet freedom by Freedom House because the measurement of these scores includes issues (such as barriers to internet access, variety of online media outlets, internet activism, and issues of self-censorship) that are not directly related to state-employed tactics of internet control. Also, the final score is usually given by one expert.

control practices across the world that can be accordingly applied to my model. Although other organisations (e.g. Reporters without Borders) also report on governments' interference with digital information, they do not provide reports in a systematic way (that is, every particular period of time) nor cover they a large number of countries.

The advantage of Freedom House is that it has been publishing annual and country reports on internet freedom since 2011, covering sixty-five states. In other words, data from Freedom House is more relevant and allows for a comparison. In addition, I also resort to numerous additional sources of information. For instance, I use the findings from the study of manipulation of public opinion on social media (Bradshaw and Howard 2018) to supplement the respective category. In the case studies, I also scrutinise primary sources such as constitutions, laws, official regulations, statutes, and programs that directly or indirectly deal with the digital domain.

Table 1. Model of internet control

Main tactics	Censorship of online content[69]	Internet shutdowns and disruptions	Manipulation of public opinion on the internet[70]	Punishment of users for internet activities	Restrictive internet legislation	Dominance of internet infrastructure
Country	Employed / Not employed	Employed / Not employed	Employed / Not employed	Employed / Not employed	Employed / Not employed	Employed / Not employed

The coverage period for all categories, apart from restrictive laws that expand the state authority in the digital sphere, spans from June 2016 to May 2018. The coverage period for internet-related laws is wider and includes five years (June 2013 – May 2018) as the adoption of new legislation takes more time compared to other forms of control. Another feature of internet laws is that they can be applied at any time since their adoption. For example, a law passed in 2014 can be equally employed in 2018 – therefore I extend the coverage period for the respective category. The number of countries is identical to the Freedom House ranking: sixty-five countries altogether comprising 87% of world internet users[71]. In this regard, the comparative analysis of

[69] Filtering and blocking of content and websites because of (child) pornography and copyrights issues is not included in this category. This is because censorship of such content is a norm in almost all countries (Powers and Jablonski 2015).

[70] The focus is on control of information distributed over the internet by countries within their territories. Consequently, I do not consider social media manipulation of one country employed in another country.

[71] These countries are Angola, Argentina, Armenia, Australia, Azerbaijan, Bahrain, Bangladesh, Belarus, Brazil, Cambodia, Canada, China, Colombia, Cuba, Ecuador, Egypt, Estonia, Ethiopia, France, the Gambia, Georgia, Germany, Hungary, Iceland, India, Indonesia, Iran, Italy, Japan, Jordan, Kazakhstan, Kenya, Kyrgyzstan, Lebanon, Libya, Malawi, Malaysia, Mexico, Morocco,

sixty-five countries serves as a preliminary step in studying conditions of internet control, which is sufficient to identify general patterns in the interplay between research variables.

It is also of note that the model to study the extent of internet control is not all-inclusive, though is still efficient as there a priori cannot be total or all-encompassing control of information on the internet (unless an intranet such as in North Korea is created). States do not need the total command over the digital space because it is simply impossible to achieve – the quantity of materials produced and generated on the internet is too enormous to grasp. Second, it can be very costly for states to control everything. Yet, by employing various tactics, governments across the world thus far have been able to exercise comprehensive control over digital information. For example, China, which is arguably the most sophisticated regime in controlling the internet, does not attempt to shape and limit all information online. Rather, China tries "to create an Internet that is free enough to support and maintain the world's fastest growing economy, and yet closed enough to tamp down political threats to its monopoly on power" (Goldsmith and Wu 2006: 89).

In short, the model includes main information controls, allowing for a study of state control of digital information within national borders. The main logic is as follows: the higher number of employed tactics, the more controlled information online. Altogether, I identified the following extents of internet control (table 4). The first one is extensive internet control – when a country employs between five and six out of six available tactics. The second extent is significant internet control. The number of employed tactics is between three and four. I consider the employment of minimum half of main information controls to be significant as, although the extent is less extensive than in the first category, it is still sufficient to considerably limit the dissemination of digital information. The last extent is limited internet control, which is when no more than two tactics are employed. This number of tactics is of a limited impact as two tactics are insufficient to effectively control information on the internet.

4.2. Defining the nature of political institutions

In addition to the extent of internet control, I also identify the nature of political institutions. Based on the definitions of political institutions by Bueno de Mesquita et al (2003), Acemoglu and Robinson (2013), and other institutionalists (e.g. Lowndes and Roberts 2013, North 1990), I define political institutions as formal and informal rules, practices,

Myanmar, Nigeria, North Sudan, Pakistan, Philippines, Russia, Rwanda, Saudi Arabia, Singapore, South Africa, South Korea, Sri Lanka, Syria, Thailand, Tunisia, Turkey, Uganda, Ukraine, United Arab Emirates, United Kingdom, United States, Uzbekistan, Venezuela, Vietnam, Zambia, and Zimbabwe.

and other processes (e.g. narratives) that regulate executive recruitment and distribute political power by stipulating who has the admission to decision-making and the allocation of resources. Thus, specifics of executive selection and whether the executive authority is constrained or not, along with the extent to which a large part of the population is able to participate in political processes (such as elections) and influence political outcomes (for example, by voting), determine the nature of political institutions.

Consequently, countries have *extractive* institutions when there are unfair and unfree elections (or no elections at all), no or slight limitations on the executive authority, and political participation and competition are restricted, that is, political power is located in the hands of a small group of people. In contrast, political institutions are *inclusive* when elections are free, fair, and regular, when there are constraints on the political authority of the executive, and when the political landscape is competitive and open for a large segment of society. I summarise the definitions of the key concepts of my study in table 2.

To identify the nature of political institutions in sixty-five countries, I use data from Polity IV (Marshall et al 2018). The advantage of Polity IV is that it evaluates “authority characteristics” such as the regulation, openness, and competitiveness of executive selection, institutional constraints on the executive authority, and the regulation and competitiveness of political participation, which are the integral parts of political institutions.

Democracy Index by the Economist Intelligence Unit (EIU) is also widely used to measure polities, though, it should be noted that my focus is on political institutions. The nature of political institutions is closely associated with the types of political systems but the assessment of the latter concept is often wider. For example, the EIU in its assessment includes additional indicators such as political culture, the functioning of government, and civil liberties that are not directly relevant to the nature of political institutions. Similarly, the World Bank provides data on political institutions but its focus is on formal organisations such as political parties and the president. Meanwhile, I define political institutions not only as formal but also as informal processes related to the distribution of political power. Thus, the EIU index and World Bank data are not fully compatible with political institutions under my consideration.

Accordingly, Polity IV data is more relevant to measure the nature of political institutions. Also, it is of note that the comparative analysis, in which I largely but not exclusively use data from Freedom House and Polity IV, is a preliminary step to explore general patterns in relations between institutions and internet control. After the comparative analysis, I conduct two case studies to be able to refine the findings and draw more valid generalisations about specifics of internet control. In this regard, I resort to numerous additional primary and secondary sources.

Table 2. Political institutions and internet control

Concept	Conceptualisation	Operationalisation	Indicator
Political institutions	Formal and informal rules, practices, and processes that regulate executive recruitment and distribute political power by stipulating who has the admission to decision-making and the allocation of resources. Specifics of executive selection, whether the executive authority is constrained or not, and the extent to which a large part of the population is able to participate in political processes (such as elections) and influence political outcomes (for example, by voting) determine the nature of political institutions.	1) Regulation, openness, and competitiveness of executive recruitment 2) Institutional constraints on the executive authority 3) Regulation and competitiveness of political participation	Polity IV data on "authority characteristics" (ExRec, ExConst, and PolComp)
Extractive political institutions	Countries have extractive institutions when there are unfair and unfree elections, no or slight limitations on the executive authority, and political participation and competition are restricted. That is, political power is located in the hands of a small group of people.	1) Unfree and unfair elections 2) No constraints on the executive authority 3) Restricted political participation	
Inclusive political institutions	Countries have inclusive institutions when there are free, fair, and regular elections, significant constraints on the political authority of the executive, and the political landscape is competitive and open for a large segment of society. That is, political power is fairly distributed.	1) Free and fair elections 2) Constraints on the executive authority 3) Open and competitive political participation	
The extent of internet control	Internet control is defined as the implementation by states of censorship, disruption, propaganda, and/or other means to shape and/or limit the digital flow of information within national borders. The extent of internet control is defined by the number of state-employed information controls.	1) censorship of online content and websites 2) disruption of communication networks 3) manipulation of public opinion on the internet 4) punishment of users for internet activities 5) restrictive internet legislation 6) dominance of internet infrastructure	Freedom House (2017-2018 annual reports; and 2017-2018 country reports), Bradshaw and Howard (2018), and other secondary sources

5. CALIBRATION

One of the strategies to identify causation is to establish whether cases with the same or similar conditions also share the same outcome. In my case, whether countries with extractive political institutions extensively control information online. On the other hand, I also examine whether countries with inclusive political institutions exercise limited control over the dissemination of digital information. However, before proceeding to a comparative analysis, I need to calibrate both the extent of internet control (the outcome) and the nature of political institutions (the condition) to be able to identify the causal interplay between the former and the latter. Otherwise, without the calibration, the application of the QCA method will be unmanageable (Ragin 2008: 8).

5.1. Calibration of the outcome

In my study, I apply a seven-value calibration (table 3) as it allows a more comprehensive analysis of the concepts under my consideration. There are three qualitative anchors of 1.0, 0.0, and 0.5 that accordingly mean full membership, full non-membership, and neither membership nor non-membership (point of indifference) in a set. In addition, there are further gradations such as 0.83, 0.66, 0.33, and 0.17 that indicate whether a concept is more in or more out of the set. In the seven-value calibration, there is a slight yet important distinction between 1.0 and 0.83, and 0.17 and 0.0, where 0.83 means that a country is mostly but not completely in a set while 0.17 means that a country is mostly but not fully out a set[72].

By applying the seven-value calibration to internet control, I can distinguish between various gradations of state control over the online flow of information. Altogether, as discussed above, I identified the following extents: extensive, significant, and limited internet control. In terms of the calibration value, the stricter control of digital information within national borders, the higher the membership score (table 4). Thus,

[72] For example, this logic of calibration can be applied when one discusses democracy, comparing two countries such as Colombia and Canada (randomly taken examples). It can be said that both states are democratic, yet they are not alike. By applying the method of the QCA we can have a finely gradated set of democratic countries that would allow us to see the different degrees of the same concept (democracy). Consequently, by calibrating democracy, Colombia and Canada will have different membership scores. We can see, referring to, for instance, Polity IV data, that Canada is more democratic than Colombia – 10 out of 10 points (full democracy) versus 7 out of 10 (almost full democracy), respectively. As a result, both countries will have different positions in the set of democratic countries, in which the membership score of 1.0 means the most democratic country while 0.0 means that the country is fully out of the set, that is, not democratic at all; 0.5 (crossover point) means that a country is neither democracy nor non-democracy. Canada would have a membership score of 1.0 (fully in the set of democratic countries) and Colombia of 0.83 (mostly but not fully in the set of democratic countries). Both membership scores mean that both countries are democratic (as both scores are higher than the crossover point of 0.5), though we can see that Colombia is less democratic than Canada. Accordingly, the same logic of calibration is applied to all concepts used in my study.

countries that employed five and six information controls have membership scores of 0.83 and 1.0, accordingly. For example, Kazakhstan employed all six internet control tactics during the coverage period. Therefore, its membership score is 1.0 – Kazakhstan extensively controls the dissemination of digital information.

Table 3. Seven-value calibration

Seven values in fuzzy sets	**Description of membership in a set (categories)**
1.0	Fully in a set
0.83	Mostly in (but not fully)
0.66	More in than out
0.5 (crossover)	Neither fully in nor fully out
0.33	More out than in
0.17	Mostly out (but not fully out)
0.0	Fully out a set

Countries that used three and four tactics (significant internet control) have membership scores of 0.5 and 0.66, respectively. Although this extent cannot be attributed to the camp of either extensive or limited internet control, I consider the extent significant as the minimum number of employed information controls equals to half of the available ones. The employment from three to four tactics is tangible as the dissemination of digital information is restricted under such circumstances. Finally, countries that applied no more than two tactics have membership scores of 0.0, 0.17, and 0.33, indicating that the country has a limited extent of internet control. For example, Japan used only one out of six tactics during the coverage period, thus having a 0.17 membership score.

Table 4. Calibration of the extent of internet control

Extent of internet control	**QCA score**	**Number of employed tactics (out of 6)**
1. Extensive	1	6
	0.83	5
2. Significant	0.66	4
	0.5	3
3. Limited	0.33	2
	0.17	1
	0.0	0

5.2. Calibration of the condition

The main proposition of my study is that the nature of political institutions affects the extent of internet control. Consequently, I identified three integral components such as specifics of the executive election, constraints on the executive authority, and restrictions on political participation that define political institutions. Political institutions, as a result of various extents of these three integral aspects, can be either more extractive or more inclusive.

To identify specifics of executive selection, I use the Polity IV concept of "executive recruitment" that defines "how institutionalized, competitive and open are the mechanisms for selecting a political leader" (Marshall et al 2018: 48). There are eight categories, starting from "ascription" (category 1), which is hereditary succession to the chief executive position, to "competitive elections" (category 8). Consequently, the calibration of the concept utilises the following logic: the more competitive and open the selection process of the executive, the smaller the membership score of the country in this set. Thus, competitive elections equal to 0.0 whereas the absence of elections equals to 1.0. The six in-between categories are calibrated accordingly (table 5). For example, Saudi Arabia, which is an absolute monarchy with no elections, has a membership score of 1.0 whereas Australia, having competitive elections, has a 0.0 score in the set of executive recruitment.

Table 5. Calibration of executive recruitment
(the higher the score, the less open and competitive executive recruitment)

QCA score	**Polity IV "Executive recruitment" (exrec)**	
	Categories	Description of categories
1.0	Concept 1	"Ascription"
0.83	Concept 2	"Dual executive: ascription+designation"
0.66	Concept 3	"Designation"
0.5	Concept 4	"Self-selection"
	Concept 5	"Gradual transition"
0.33	Concept 6	"Dual executive: ascription+election"
0.17	Concept 7	"Transitional or restricted elections"
0.0	Concept 8	"Competitive elections"

Table 6. Calibration of constraints on the executive authority
(the higher the score, the less constrained political authority of the executive)

QCA score	**Polity IV "Executive constraints" (xconst)**	
	Categories	Description of categories
1.0	Concept 1	"Unlimited executive authority"
0.83	Concept 2	"Intermediate category #1"
0.66	Concept 3	"Slight to moderate limitation on executive authority"
0.5	Concept 4 (and -0.77)	"Intermediate category #2" (and "failed authority")
0.33	Concept 5	"Substantial limitations on executive authority"
0.17	Concept 6	"Intermediate category #3"
0.0	Concept 7	"Executive parity or subordination"

To measure the second aspect of political institutions – the agency of chief executives, that is, whether their political authority is constrained or not – I refer to the concept of “executive constraints”. According to Marshall et al (2018: 24), the concept “refers to the extent of institutionalized constraints on the decision-making powers of chief executives, whether individuals or collectivities”. The concept has seven hierarchical categories, starting from “unlimited executive authority” (category 1) and ending by “executive parity or subordination” (category 7). Accordingly, the calibration is applied in a similar hierarchical sequence: the higher membership score reflects the more unconstrained executive authority (table 6). For example, the political authority of the executive in Uzbekistan is defined as unlimited. Thus, the membership score of Uzbekistan is 1.0.

Similarly, I use data from Polity IV, particularly the concept of “political competition and opposition”, to measure the regulation of and constraints on political participation. The concept has ten categories, starting from “suppressed competition” (category 1), going through “factional competition” (category 7), and ending by “institutionalised electoral participation” (category 10). The sequence of the hierarchy is the same: the concept starts from the severest settings (first categories) and proceeds to the less strict ones (last categories). The calibration is as follows: the higher membership score means the more restricted political competition (table 7). For example, political participation in Armenia is defined as factional, thus the membership score is 0.66.

Table 7. Calibration of political participation
(the higher the score, the more restricted political participation)

QCA score	**Polity IV “Political competition and opposition” (polcomp)**	
	Categories	Description of categories
1.0	Concept 1	“Suppressed competition”
	Concept 2	“Restricted competition”
0.83	Concept 3	“Imposed transition: loosening or tightening restrictions”
0.66	Concept 6	“Factional / Restricted competition”
	Concept 7	“Factional competition”
0.5	Concept 4 (and -0.77)	“Uninstitutionalized competition” (and “failed authority”)
	Concept 5	“Gradual transition from uninstitutionalized competition”
0.33	Concept 8	“Electoral transition: persistent conflict/coercion”
0.17	Concept 9	“Electoral transition: limited conflict/coercion”
0.0	Concept 10	“Institutionalized electoral participation”

Finally, after identifying country’s membership scores in all three sets (executive recruitment, executive constraints, and political participation), I can identify the nature of political institutions (whether they are more inclusive or more extractive). Following the logic of Boolean algebra, on which the method of the QCA is based, the country's smallest membership score among all three sets (that together comprise political institutions) indicates the country's overall position in combined sets – the operation called "set intersection" (Ragin 2008: 36-37). For instance, Belarus scores 0.66 in the set for executive recruitment, 0.83 for executive constraints, and 1.0 for political participation. The membership score in the combined set of executive recruitment, executive constraints, and political participation would be the minimum one, which is 0.66. Thus, the membership score of Belarus in the nature of political institutions (that combine all three discussed above aspects) is 0.66. Consequently, I consider all scores equal to or above 0.5 as indicating more extractive political institutions, whereas all scores below 0.5 as belonging to more inclusive institutions (table 8).

Table 8. Calibration of the nature of political institutions
(the higher the score, the more extractive political institutions)

QCA score	**The nature of political institutions (executive recruitment, executive constraints, and political participation)**
1.0	More extractive
0.83	
0.66	
0.5	
0.33	More inclusive
0.17	
0.0	

5.3. Calibration of the additional condition

After conducting a comparative analysis of sixty-five countries, I did not find evidence to confirm the second hypothesis that a more inclusive nature of institutions leads to more limited internet control (details are provided in chapter 5). Thus, since research is a back-and-forth process between theory and data, after probing political institutions as the main condition of internet control, I proceeded to the identification of additional condition(s) leading to differences in the outcome. The condition that I identified in the following chapter is political instability[73]. In particular, I found that many (large-coalition) leaders operating within inclusive political settings consistently resort to information controls in the wake of political instability, which can be provoked by, for instance, street protests, ethnic conflicts, or regional tensions.

[73] The second condition is an upcoming leadership contest. In the following chapter, I provide the rationale for using these conditions. Also, the selection of the case study (chapter 7) is related to the refined proposition. As I identified that most countries with inclusive political institutions considerably control information online, I study one of the deviant cases (Ukraine) in more detail. This case has more inclusive institutions but substantial control over digital information.

Thus, to assess the level of political instability in case countries, I refer to the World Bank's Governance Indicator that "measures perceptions of the likelihood of political instability and/or politically-motivated violence, including terrorism" across the world (World Bank 2018). The indicator ranges from -2.5 to +2.5, where a lower score means a higher level of political instability. Consequently, the calibration of the additional condition is as follows: the lower the World Bank score, the higher the QCA membership score (table 9). For instance, Ukraine has a political instability score of -1.9. As a result, the calibration score is 1.0: Ukraine is fully in the set of politically unstable countries. Estonia, in another example, has +0.66 score according to the World Bank data. Hence, the calibration score is 0.33: the country is more out than in the set of politically unstable countries. In other words, Estonia is a relatively politically stable country.

Table 9. Calibration of political instability
(the higher the score, the higher level of political instability)

QCA score	**The World Bank Worldwide Governance Indicator of "Political stability and absence of violence, including terrorism"** (measurement from -2.5 to +2.5)
1.0	from -1.75 and lower
0.83	from -1.74 to -1.05
0.66	from -1.04 to -0.35
0.5	from -0.34 to +0.35
0.33	from +0.36 to +1.05
0.17	from +1.06 to +1.75
0.0	from +1.76 and higher

6. CASE STUDIES

The first objective of my study is a qualitative comparative analysis, a preliminary but important step in establishing the effects of the proposed condition on the extent of internet control. In this regard, the study of sixty-five countries is appropriate to test the hypotheses by confirming or disconfirming them (Gerring 2011: 1141-144). However, one of the possible weaknesses of the QCA method is a lack of in-depth analysis of identified causal paths. Thus, the second objective, with the focus on two cases, is to study the findings of the comparative analysis in more detail. For this reason, I examine internet politics in two post-Soviet countries, Kazakhstan and Ukraine. The case studies allow for a thorough analysis of underlying conditions, deepening the study of internet control.

In addition, both case studies follow the findings of the comparative analysis, elucidating peculiarities of state control over digital information within extractive and inclusive political institutions, respectively. As George and Bennet (2005: 24) argue, case selection bias is lower if selected cases represent various interplays between variables. In the context of my research, this means the different nature of political institutions:

extractive and inclusive. In broad terms, Kazakhstan characterises a country with extractive institutions whereas Ukraine exemplifies a country with inclusive institutions.

To analyse the impact of political institutions on the extent of internet control in the case studies, I first trace the development of institutions since both countries' independence, covering the period between 1991 and 2019. Especially, attention is paid to crucial turning points and junctures that affected the evolution and change of institutional settings in Kazakhstan and Ukraine. Such an analysis of historical processes – known as process-tracing (George and Bennet 2005) – helps observe and explain the causality between research variables (a condition and an outcome). Besides, to explore and examine the effects of political instability, the identified additional condition, on the course of internet control in Ukraine, I study the 2014 geopolitical crisis brought about by Russia's annexation of Ukraine's Crimea.

After studying the institutional context in both countries, I proceed to the discussion of internet control. Similar to the comparative analysis, the focus is on following information controls. First, internet-related legislation is thoroughly examined. Second, I study state actors (such as ministries of information and security services) who, empowered by the legal framework, also affect the extent of internet control. Next, numerous cases of systematic targeting of online content via censorship and blocking are discussed. Other analysed tactics of internet control include state capacities and practices of communications surveillance and state-organised manipulation of public opinion on social media. I also trace cases of internet shutdowns. Finally, the focus is on a crackdown of internet users, bloggers, and online journalists for their publications on the internet.

I resort to primary (constitutions, internet-related laws, regulations, policies, and programs) and secondary (news, media reports, scholarly literature, and analytics) sources to trace and study the development of political institutions and specifics of internet control in both Kazakhstan and Ukraine. In this regard, knowledge of the Russian language was a crucial asset in gathering and analysing data on case countries. It should also be noted that there is a lack of studies of internet politics in the post-Soviet countries, except for Russia, in scholarship in English and Russian languages.

All in all, the comparative analysis of many cases (chapter 5) helps explore general patterns in the interplay between research variables. Meanwhile, the main advantage of a case study is that it deepens the analysis by focusing on one of the cases in detail (chapters 6-7). Furthermore, case study selection and analysis based on the findings of the already conducted study – that is, if a case study follows the cross-case study – strengthen the research design (George and Bennet 2005: 24). Eventually, this combination of levels of analysis allows for a more comprehensive exploration and scrutiny of political phenomena and more valid conclusions, unfolding causal paths leading to state control of digital information.

7. CONCLUSION

In this chapter, I provided and explained the research design of my study. I discussed the research questions, hypotheses, and objectives that were set in order to examine conditions of internet control. The research questions, following the discussion of institutional theory in the previous chapter, are related to the expected relationship between political institutions (the condition) and the extent of state control over digital information (the outcome). The proposition is that the extractive nature of institutions (small-coalition leaders) leads to substantial control over digital information, whereas the inclusive nature of institutions (large-coalition leaders) leads to limited state interference with information on the internet.

In this regard, to unravel the causal interplay between independent and dependent variables, I resort to the qualitative comparative analysis (QCA) (Ragin 2000, 2008). Accordingly, in this chapter, I discussed how the method works and can help to explore the proposed causal connection between political institutions (along with other possible conditions) and internet control. I also provided the definitions and calibration of the key concepts used in my study. Both conceptualisation and calibration are needed to clarify how I define and measure research variables so that I can analyse the causal relations between them; otherwise, the application of the QCA is not possible. In addition to the comparative method, I also discussed how two in-depth case studies are conducted.

Consequently, in the following chapter, I apply the method of the qualitative comparative analysis to study the causal relations between the proposed condition and the outcome. I identify whether the nature of political institutions is a sufficient or necessary (if any) condition of internet control. Importantly, I focus on all main information controls in countries with extractive (authoritarian) and inclusive (democratic) institutions. Also, building on the findings of the comparative analysis, I proceed to the examination of two cases in detail. In chapters 6 and 7, I examine the interplay between political institutions, along with other possible conditions, and the extent of internet control in Kazakhstan and Ukraine, respectively. In brief, such a combination of levels of analysis can strengthen the findings and warrant more refined and valid conclusions about conditions of state control over digital information.

CHAPTER 5. POLITICAL INSTITUTIONS AND INTERNET CONTROL: A COMPARATIVE ANALYSIS

1. INTRODUCTION

In this chapter, I conduct a comparative analysis of sixty-five countries to explore the (causal) relationship between political institutions and internet control. In the previous chapters, I proposed that the distinct nature of political institutions leads to different sets of control over digital information. In particular, countries with inclusive political institutions are supposed to have a limited degree of internet control. Meanwhile, countries with extractive political institutions are expected to substantially control the online flow of information. To test these propositions, the interplay between the proposed condition and the outcome is examined.

The main motivation to implement information controls is the logic of political survival. That is, executives resort to control of digital information in order to stay in office, though the nature of political institutions within which executives operate shapes the set of available survival strategies. Under the settings of more extractive institutions, executives depend on a smaller number of supporters (small-coalition leaders) to maintain power and thus, being less limited in their authority, are expected to exercise a stricter approach to the dissemination of digital information. While in the context of more inclusive political institutions, executives rely upon a larger size of the winning coalition (large-coalition leaders) to stay in office and, consequently, are less autonomous in the choice of actions. Hence, the extent of internet control is supposed to be less substantial. In other words, executives follow various policies toward information on the internet, depending on the institutional context needed for political survival.

Nevertheless, following the comparative analysis of the relationship between political institutions and internet control, only one of the propositions was confirmed. Specifically, I found that small-coalition leaders, operating within more extractive institutional setups, exercise significant and extensive control over digital information. Out of sixty-five analysed countries, *twenty-three* have a more extractive nature of political institutions and none of them has a limited extent of internet control. On the other hand, I did not find sufficient evidence to confirm the proposition that control of digital information is limited within inclusive institutions. This is because, out of the remaining *forty-two* countries with more inclusive institutions, twenty-nine have either significant or extensive control of information on the internet. Only thirteen countries from the sample have limited internet control.

As a result, given new findings, I identified additional intervening conditions such as political instability and an upcoming leadership contest that also lead governments to employ information controls under the settings of more inclusive institutions. Under these two conditions, large-coalition leaders employ numerous tactics to affect the online flow of information. In other words, I found that the extractive nature of political institutions (small-coalition leaders) is *conducive* to significant and extensive internet control, whereas the inclusive nature of political institutions (large-coalition leaders) is *insufficient* for limited control over digital information. Additionally, I found that information on the internet appears to be substantially controlled within more inclusive political institutions in the wake of political instability and/or forthcoming elections.

Consequently, the structure of the chapter is as follows. First, specifics of internet control in all sixty-five countries are briefly outlined (section 2). Then, the extent of state control of digital information in relation to political institutions is considered. In particular, I discuss the interplay between internet control and extractive political institutions (section 3). In total, I identified twenty-three out of sixty-five countries as having more extractive institutional structures. Next, I proceed to the discussion of internet control in the remaining forty-two countries with more inclusive political institutions (sections 4). Finally, I analyse additional intervening conditions that also tend to affect the extent of state control of information on the internet (section 5).

2. INTERNET CONTROL

I distinguish between the following main tactics of state control over information on the internet: 1) censorship of online content (including blockings of websites)[74]; 2) disruption (or shutdown) of communication networks; 3) manipulation of public opinion on social media; 4) punishment of digital users and online journalists for their internet activities; 5) adoption of restrictive internet laws and regulations that expand the state grip over cyberspace; and 6) dominance of internet infrastructure and actors. Based on the number of tactics employed by countries, I identified the following extents (groups) of internet control: limited (0-2 employed tactics), significant (3-4 employed tactics), and extensive (5-6 employed tactics).

Overall, as demonstrated in figure 6, only thirteen out of sixty-five countries have limited control over digital information (up to two employed tactics). Alarmingly, almost half of analysed countries (thirty-two) has a significant extent of internet control (from three to four employed tactics) whereas the remaining twenty countries exercise extensive control over digital information (from five to six employed tactics). Below, I discuss the extent of internet control in sixty-five countries, outlining the main aspects of each group (extensive, significant, and limited). After understanding general patterns of

[74] Censorship of content related to (child) pornography and copyrights issues is not included.

state interference with information online, in the following sections, I discuss practices of internet control in relation to the nature of political institutions (extractive and inclusive), providing additional details and examples.

Figure 6. Extent of internet control, 2016-2018 (65 countries)

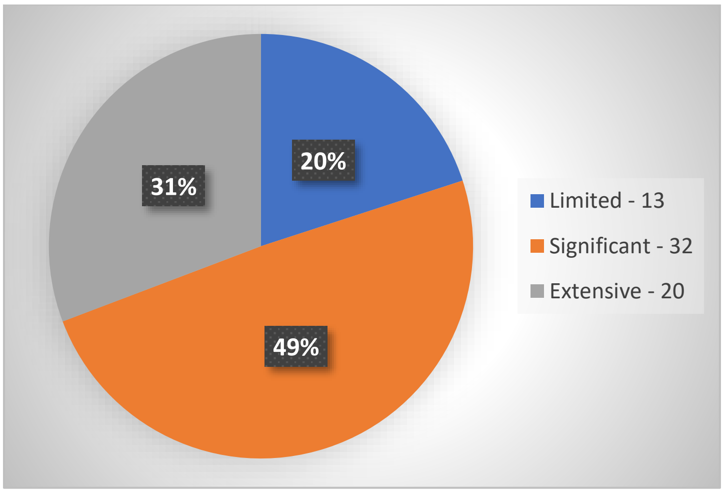


Table 10. Internet control, 2016-2018 (65 countries)[75]

Number of employed tactics	Extent of internet control	Number (and list) of countries
6	Extensive (20 countries)	10 (Azerbaijan, Bahrain, China, Egypt, Ethiopia, Iran, Kazakhstan, Pakistan, Belarus, Vietnam)
5		10 (Russia, United Arab Emirates, Venezuela, Saudi Arabia, Thailand, India, Indonesia, Ukraine, Uzbekistan, Turkey)
4	Significant (32 countries)	15 (Brazil, South Korea, Malaysia, Myanmar, Nigeria, Sri Lanka, Lebanon, Singapore, Zimbabwe, Libya, Rwanda, Uganda, Syria, Bangladesh, Cuba)
3		17 (Argentina, Ecuador, Germany, Hungary, Kenya, Kyrgyzstan, Mexico, Philippines, United Kingdom, United States, Zambia, Tunisia, Angola, Cambodia, North Sudan, Morocco, Jordan)
2	Limited (13 countries)	8 (Australia, France, Georgia, Italy, Gambia, South Africa, Armenia, Malawi)
1		3 (Canada, Colombia, Japan)
0		2 (Estonia, Iceland)

2.1. Extensive internet control

Out of twenty states with overwhelming control over information on the internet, *ten* countries employed all six tactics (table 10). In other words, these cases display the worst scenario of internet control as the local authorities censored online content, disrupted internet connectivity, organised manipulation of public opinion via social media,

[75] Full table of the implementation of internet control tactics by countries is provided in Appendix 1.

penalised internet users, enacted restrictive internet-related laws, and dominated the domestic internet infrastructure and actors during the coverage period.

China, for example, deploys firewall software to block foreign websites deemed threatening to its regime. In addition, internet legislation in China requires internet providers to monitor all content distributed on the internet, making them responsible for the circulated information. The police, if necessary, physically patrols internet cafes; meanwhile, regular users can be arrested for expressing political views online (Kalathil and Boas 2003: 26-27, Freedom House China 2018). There is also an electronic army of paid commentators that advance the pro-government narrative via social media. The government in China has been using all these tools to shape the way information is disseminated online, simultaneously creating a sense of self-censorship, fear, and responsibility among the population.

The remaining *ten* countries also have extensive internet control, applying all but one tactic. Venezuela, Ukraine, and Saudi Arabia, for instance, employed all tactics apart from the disruption of communication networks during the coverage period. India, Turkey, and Indonesia also used five tactics of internet control: all but the dominance of internet actors. Yet, even without cutting off internet access or dominating the internet infrastructure and intermediaries, all ten countries, by utilising five out of six main tactics, managed to substantially shape and limit the online flow of information.

As displayed in table 11, all twenty countries with extensive internet control systematically blocked and filtered online content, punished users by the way of detaining, arresting, fining, or prosecuting for internet activities. In addition, all twenty countries during the coverage period passed restrictive internet-related laws, extending surveillance or censorship capabilities of the government, and were organising disinformation campaigns on social media. The least used type of internet control in this group of states was the disruption of communications: thirteen out of twenty states shut down networks between 2016 and 2018. However, as I discuss below, the most notorious cases of communication shutdowns took place in India and Pakistan.

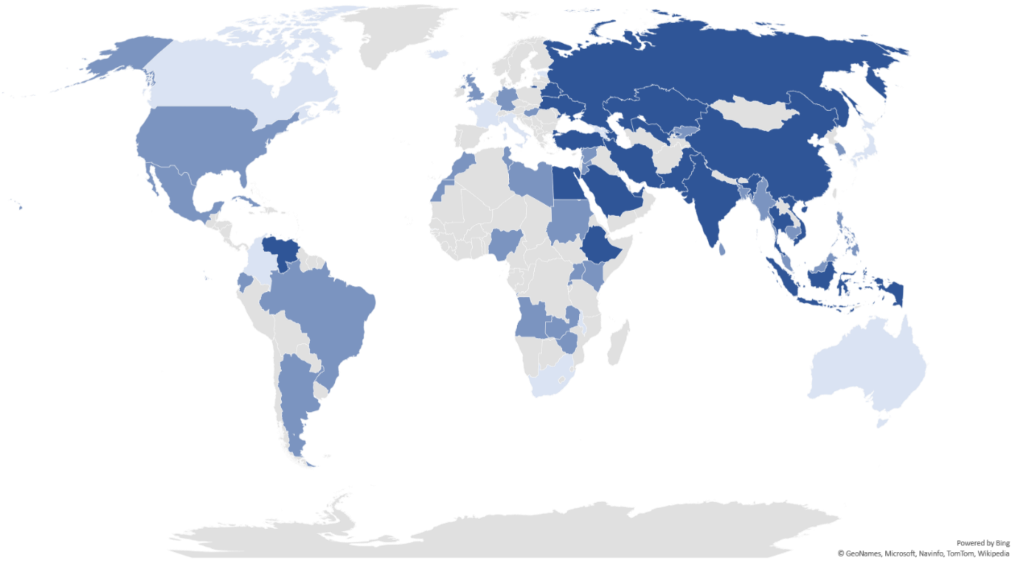
2.2. Significant internet control

Thirty-two out of sixty-five states have significant control of digital information. *Seventeen* and *fifteen* states applied three and four information controls, accordingly. This is not sufficient to define internet control as extensive, yet it is not limited. Overall, the number of employed internet control tactics is smaller and the grip over the digital domain is weaker compared to the countries with extensive control. However, the employment of a minimum half of main tactics telegraphs the government's determined approach toward the online flow of information.

This is also a diverse group of countries, ranging from the United States, the United Kingdom, and Argentina to Zambia, Tunisia, Zimbabwe, and Kyrgyzstan to Brazil, Malaysia, and South Korea (table 10 and figure 7). For example, the authorities of the latter three (democratic) countries, between 2016 and 2018, methodically filtered online content, were involved in the public opinion sway on social media platforms, detained citizens for their internet activities, and adopted restrictive internet legislation. (I provide further details in the following sections.)

Figure 7. Map of internet control, 2016-2018 (65 countries)

(light blue – limited control; blue – significant control; dark blue – extensive control)



Alarmingly, in all countries from this group individuals were punished for their online endeavours through fines, detainments, and/or arrests. The latter tactic, along with state-aligned campaigns to influence the public via social media and adoption of laws that significantly expand government's surveillance or censorship powers, were the three most used information controls among all thirty-two countries (table 11). Similar to the previous group, communications shutdowns were the least "popular" tool to affect the dissemination of information online: only six (Bangladesh, the Philippines, Sri Lanka, Zambia, Lebanon, and Libya) resorted to this tactics during the coverage period. Another two less used information controls were censorship of online content and the dominance of internet infrastructure.

2.3. Limited internet control

Only thirteen out of sixty-five countries employed up to two internet control tactics. *Eight* of them (Australia, France, Georgia, Italy, South Africa, the Gambia, Armenia, and Malawi) resorted to two information controls. Two tools of state interference with information on the internet were the most used in these eight countries. These are the sway of public opinion on social media (Australia, Italy, South Africa, and Armenia) and the implementation of legislation that expands state capabilities in the digital sphere (Australia, France, Italy, South Africa, and Malawi).

In addition, *three* out of thirteen countries employed only one tactic of internet control. Similar to the countries above, the Colombian and Japanese authorities resorted to social media manipulation, and Canada adopted the 2015 Anti-Terrorism Act (Bill C-51) that, according to Freedom House Canada (2018), "permits information-sharing across government agencies for an incredibly wide range of purposes, many of which have nothing to do with terrorism" and was criticised due to privacy concerns. The remaining *two* countries (Estonia and Iceland) did not employ any tactics during the coverage period[76].

Overall, two countries with limited internet control (Armenia and Georgia) denied access to social media platforms; less than one-third of countries punished users for internet activities, and less than half of the group passed restrictive laws and used social media platforms in attempts to influence public opinion. None of the thirteen countries disconnected communication networks between 2016 and 2018 (table 11). In other words, all thirteen countries refrained from implementing most of information controls, having a limited impact on the dissemination of information over the internet.

Table 11. Internet control tactics, 2016-2018 (65 countries)

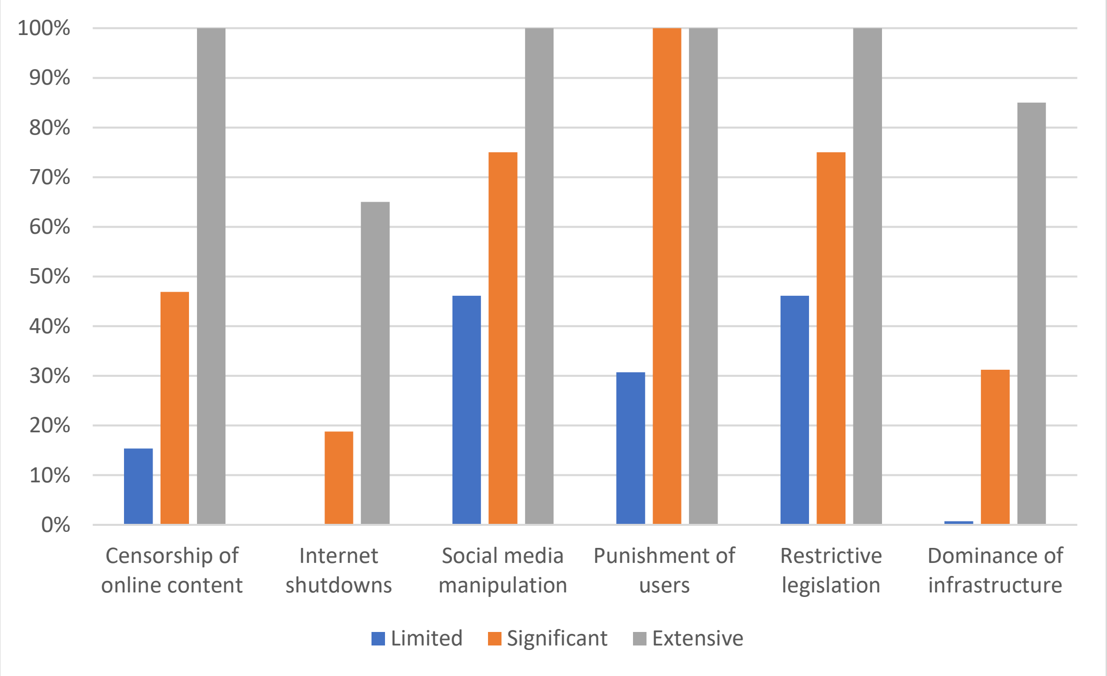
Extent of control	Censorship of online content	Internet shutdowns	Manipulation of public opinion	Punishment of internet users	Restrictive internet legislation	Dominance of infrastructure
Extensive (20 countries)	20/20	13/20	20/20	20/20	20/20	17/20
Significant (32 countries)	15/32	6/32	24/32	32/32	24/32	10/32
Limited (13 countries)	2/13	0/13	6/13	4/13	6/13	1/13
Total	**37**	**19**	**50**	**56**	**50**	**28**

[76] Technically, there was no state control of information on the internet in Estonia and Iceland during the coverage period, though I still relate them to the group of countries with the limited extent of internet control. Also, as noted in chapters 2 and 4, control of information related to (child) pornography and copyrights issues was not considered.

In total (table 11 and figure 8), the most widespread tactic among all three groups of countries was the punishment of users for internet activities: it was reported in fifty-six out of sixty-five states. Another widely used instrument to shape and restrict information online was the adoption of the restrictive legal framework that extends government's powers in surveillance or censorship spheres (fifty out of sixty-five states). The same number of countries was also found to have swayed public opinion on social media with the help of electronic armies of trolls and commentators. Social media manipulation was reported in fifty countries.

Rather surprisingly, the majority of analysed countries (thirty-seven out of sixty-five) resorted to censorship by filtering online content and/or blocking access to websites and applications between 2016 and 2018. Also, a high number of countries, twenty-eight out of sixty-five, dominated the domestic internet infrastructure and actors (such as IXPs, ISPs, and telecommunication companies). Out of all, the least used but still a relatively common tactic was the disruption of communication networks with the goal to limit the dissemination of information online (nineteen out of sixty-five).

Figure 8. Internet control tactics (%), 2016-2018 (65 countries)

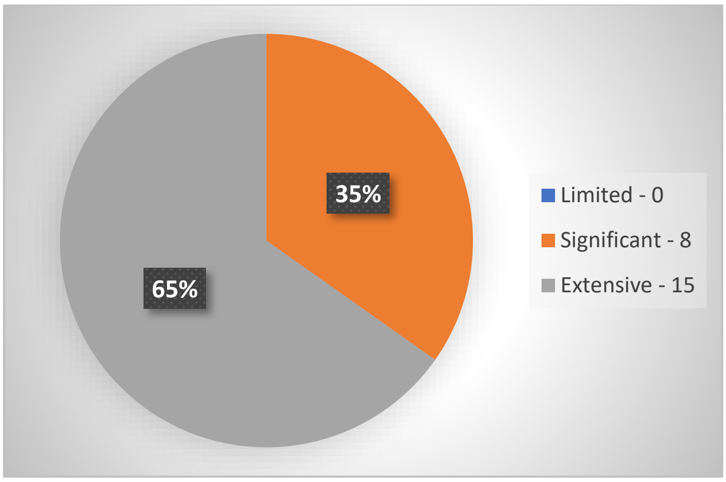


In this section, I outlined main patterns that are specific to extensive, significant, and limited extents of internet control. It can be seen that substantial state control over digital information (the implementation of half and more available tactics) is a common feature in many countries whereas only a minority of states limits its engagement with the internet. In appendix 1, I provide a full table of internet control tactics implemented in sixty-five countries during the coverage period. Also, I identified what tactics are the most used among countries to shape and restrict the dissemination of digital information within national borders. In the following sections, I offer more details while discussing the extent of internet control in relation to the nature of political institutions, which was proposed as the main condition of deploying (or not deploying) information controls.

3. EXTRACTIVE INSTITUTIONS AND INTERNET CONTROL

I identified the nature of political institutions in sixty-five countries in line with Polity IV data (Marshall et al 2018). All countries were divided into two groups: more extractive political institutions (twenty-three countries) and more inclusive political institutions (forty-two countries). In this section, I discuss the interplay between extractive institutions and internet control.

Figure 9. Extractive institutions and internet control (23 countries)



Twenty-three countries have a more extractive nature of political institutions or small-coalition leaders. In these countries, the executive authority is slightly or not constrained, political participation is limited to most citizens, and the electoral process is not transparent and fair. Notably, *fifteen* out of twenty-three states have extensive control of information on the internet, having deployed from five to six tactics. The remaining *eight* states with more extractive institutions have significant control over digital information (from three to four employed tactics). None of the countries from this group has a limited extent of internet control (figure 9).

Nine states from this group employed all six information controls (table 12). Azerbaijan, for instance, filtered online content and restricted access to websites, disrupted communications, penalised users for their internet activities, and organised manipulation of public opinion on the internet between 2016 and 2018. In addition, the government of Azerbaijan dominates over the domestic internet infrastructure and actors and has been passing restrictive internet legislation. There are altogether ten countries with all six main tactics being employed. Nine of them have extractive political institutions (small-coalition leaders). Pakistan, the tenth country, has a more inclusive nature of political institutions and, therefore, is discussed in the following section.

Table 12. Extractive institutions and internet control (23 countries)

Number of employed tactics	Extent of internet control	Number (and list) of countries
6	Extensive (15 countries)	9 (Azerbaijan, Bahrain, China, Egypt, Ethiopia, Iran, Kazakhstan, Belarus, Vietnam)
5		6 (Turkey, Saudi Arabia, United Arab Emirates, Venezuela, Thailand, Uzbekistan)
4	Significant (8 countries)	5 (Cuba, Libya, Rwanda, Uganda, Syria)
3		3 (Cambodia, North Sudan, Morocco)

Six states with small-coalition leaders were found to have resorted to five information controls during the coverage period. Turkey used all tactics save for the domination of internet infrastructure. Uzbekistan, Thailand, Saudi Arabia, the United Arab Emirates, and Venezuela employed all but the disruption of communications. Most notably though, India, Indonesia, Ukraine, and Russia[77], countries that also used five out of six tactics, have more inclusive institutions according to Polity IV data, and thus are considered in the following section. In all these cases, countries, by implementing almost all main tactics, shaped and limited the online flow of information to a great extent.

Eight out of twenty-three countries with small-coalition leaders exercise significant control over digital information. Five of them (Cuba, Libya, Rwanda, Uganda, and Syria) employed four tactics while the remaining three (Cambodia, Morocco, and North Sudan) resorted to three information controls. All of them practised a crackdown on internet users and in all but Morocco and Libya the influence of online opinion via social media was found. Save this, there is no clear pattern in internet control configurations. However, there are altogether thirty-two out of sixty-five countries that exercise significant control over information on the internet and only eight of them have extractive political institutions. Disturbingly, the remaining twenty-four countries have more inclusive political institutions, yet having implemented at least half of main internet

[77] According to Polity IV, Russia in 2017-2018 had: 1) transitional presidential elections, meaning that they are relatively free and the result is not predefined in advance; 2) an intermediate concept of the executive authority (between substantial and slight limitations on the executive authority); and 3) a relatively competitive political landscape, albeit marred by persistent coercion by government. Altogether, these aspects make the nature of political institutions in Russia more inclusive during the coverage period.

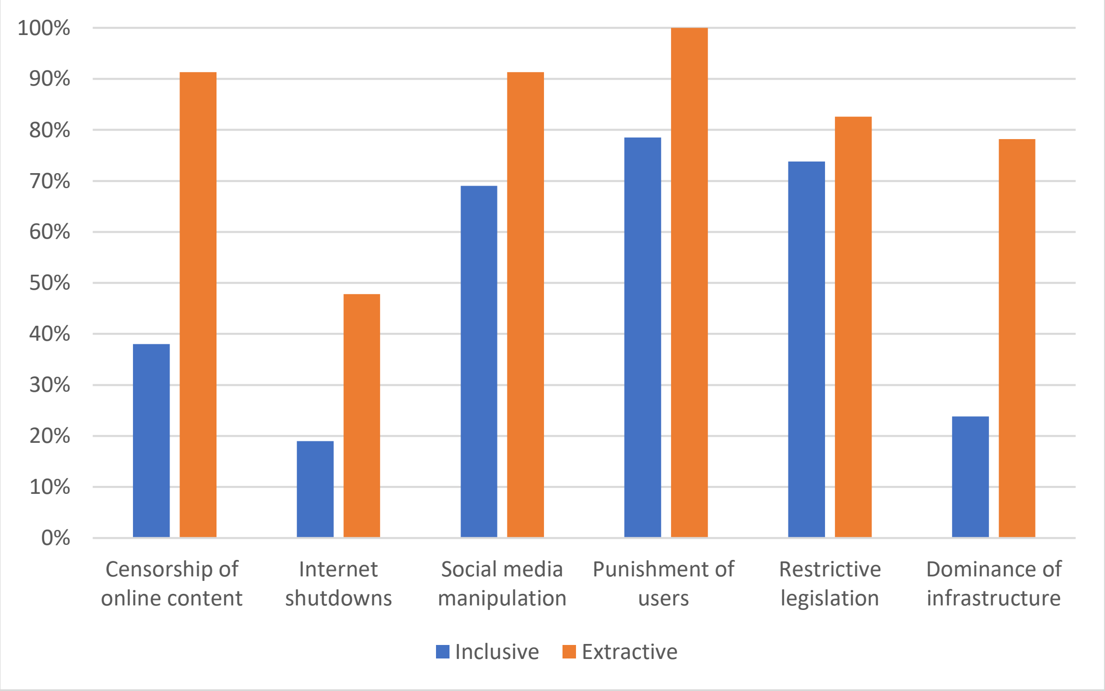
control tactics. Consequently, in the following sections, I discuss a possible explanation for this phenomenon.

Overall, out of six information controls, a crackdown on internet users was the most used (table 13 and figure 10). All twenty-three states with more extractive political institutions punished their citizens for activities in cyberspace. Also, most countries (twenty-one out of twenty-three) resorted to manipulation of the population on social media platforms and censored online content. Similarly, a great number of countries with more extractive political institutions passed restrictive legislation and have been dominating domestic internet actors and infrastructure during the coverage period: nineteen and eighteen countries, respectively. The least employed tactic was shutdowns of communications: less than half (eleven out of twenty-three) disconnected the internet between 2016 and 2018.

Table 13. Political institutions and internet control tactics (65 countries)

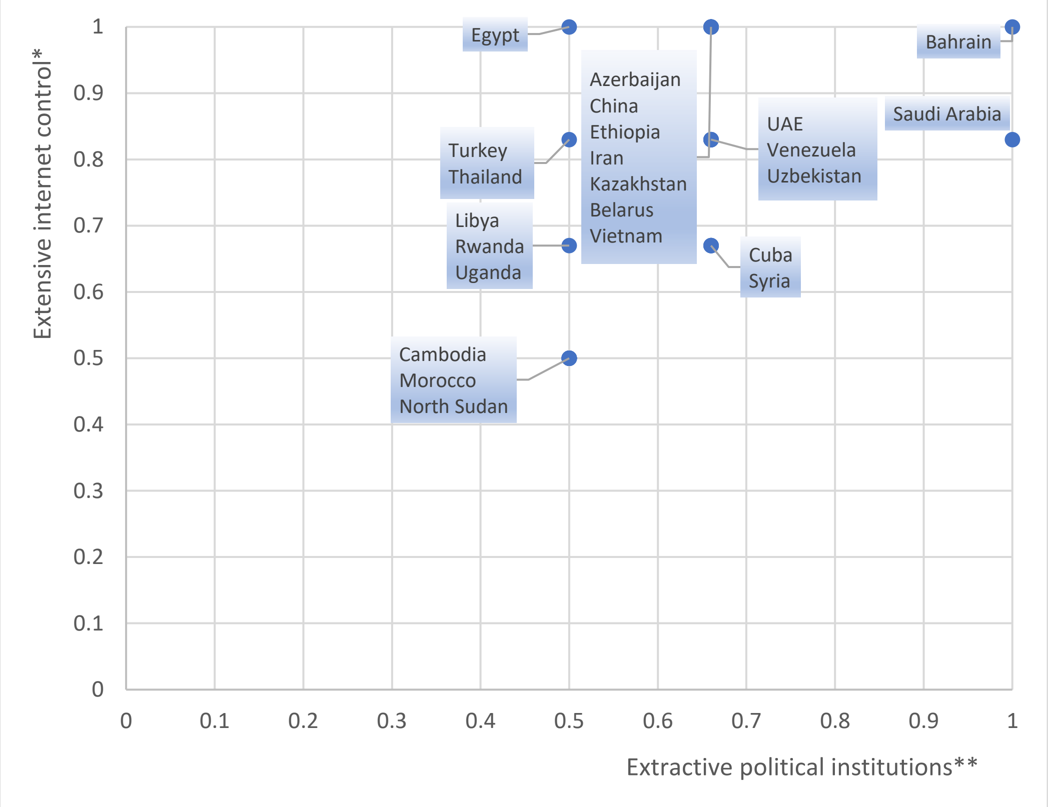
The nature of political institutions	Censorship of online content	Internet shutdowns	Manipulation of public opinion	Punishment of internet users	Restrictive internet legislation	Dominance of infrastructure
Extractive (23 countries)	21/23	11/23	21/23	23/23	19/23	18/23
Inclusive (42 countries)	16/42	8/42	29/42	33/42	31/42	10/42
Total	**37**	**19**	**50**	**56**	**50**	**28**

Figure 10. Political institutions and internet control tactics (%) (65 countries)



To sum up, the extractive nature of political institutions is consistent with the high number of employed internet control tactics (figure 11). Countries with executives with no or slight limitations on their authority, restricted political participation and competition, and unfair election procedures exercised significant (three to four tactics) and extensive (five to six tactics) control over digital information. Thus, with the consistency rate of 79% and the coverage rate of 98%[78], I can confirm the first proposition that the *extractive nature of political institutions is conducive to substantial state control over information on the internet*.

Figure 11. Political institutions and internet control (23 countries)
* the higher the QCA score in the Y axis, the more extensive internet control[79]
** the higher the QCA score in the X axis, the more extractive political institutions[80]



The confirmed proposition is an identified tendency that explains significant and extensive internet control. In most countries, the logic of political survival led governments under the rule of small-coalition leaders to exercise substantial control over the online flow of information. Despite a few exceptions, given the high rate of both

[78] All computations were made in "fsQCA 3.0", software that is specifically designed for the fuzzy-sets qualitative comparative analysis. The calibration of concepts is provided in chapter 4.
[79] According to the calibration of the outcome (chapter 4), membership scores of limited internet control are 0, 0.17, and 0.33; significant – 0.5 and 0.66; and extensive – 0.83 and 1.
[80] According to the calibration of the condition (chapter 4), membership scores of more inclusive political institutions are 0, 0.17, and 0.33; and more extractive – 0.5, 0.66, 0.83, and 1.

consistency and coverage, the pattern of countries with extractive political institutions considerably controlling information on the internet is therefore robust[81].

Thus, the causal relationship between the extractive nature of political institutions and the substantial extent of internet control was identified. In the following chapter, I discuss the interplay between extractive institutions and internet control in more detail, drawing evidence from Kazakhstan. The case study of Kazakhstan represents a relatively common approach of authorities operating within extractive institutional setups to the dissemination of information on the internet. In other words, the logic to stay in power as long as possible motivates small-coalition leaders – from China to Azerbaijan to Kazakhstan – to strictly regulate and restrict information online.

However, the extractive nature of political institutions is a *sufficient* but not a necessary condition of internet control. That is, it is not the only factor leading to significant and extensive state control over digital information. As I discuss in the following sections, there appeared to be additional conditions that also result in a high number of employed information controls.

4. INCLUSIVE INSTITUTIONS AND INTERNET CONTROL

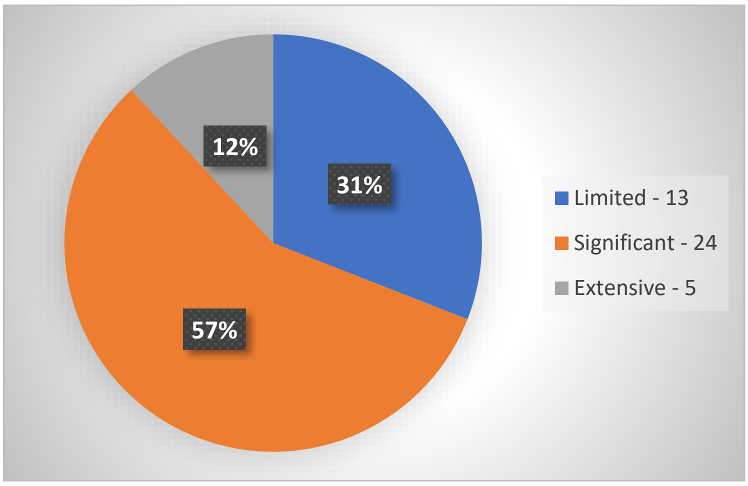
Drawing insights from institutional theory, I proposed that the set of survival strategies of large-coalition leaders is limited due to constraints on their authority. Therefore, they are not in a position to substantially control information on the internet compared to small-coalition leaders whose powers are hardly restricted. One of the propositions, thus, was that the inclusive nature of political institutions (large-coalition leaders) leads to a limited extent of internet control. However, in practice, this was not always the case as many large-coalition leaders, although being institutionally restricted in their powers and actions, managed to shape and restrict information online by employing various tactics. As I argue below, there are additional intervening conditions that affect the extent of internet control within inclusive institutions. Consequently, in this section, I discuss state control over digital information in countries with inclusive political institutions and, given new findings, refine the abovementioned proposition.

Overall, I found that out of forty-two countries with more inclusive political institutions (or large-coalition leaders), that is, fair electoral processes, constraints on the executive authority, and more open political participation, only *thirteen* have limited control of information on the internet (figure 12). Two countries (Estonia and Iceland) did not use information controls during the coverage period; three states (Canada, Colombia,

[81] In three countries (Cambodia, Morocco, and North Sudan), the extent of internet control was less persuasive (three employed tactics during the coverage period).

and Japan) applied only one tactic. The remaining eight countries employed two tactics (table 14). Notably, the Gambian government used to block opposition websites, censor online content, and disrupt communications under the authoritarian rule of the previous president, Jammeh (Freedom House The Gambia 2017). However, since January 2017, when a new president (Barrow) came to power, the nature of political institutions has become more inclusive[82]. Consequently, the Gambian authorities ceased to employ these tactics of internet control.

Figure 12. Inclusive institutions and internet control (42 countries)



Nevertheless, the inclusive nature of political institutions did not always lead to limited state interference with information on the internet as the vast majority of countries (twenty-nine out of forty-two) employed at least half and more information controls. That is, most countries with inclusive institutions adopted a strict approach to the internet, exercising significant (*twenty-four* countries) and extensive (*five* countries) control over digital information.

Out of five states with extensive internet control, Pakistan shapes and restricts information online in the most indiscriminate manner, having used all six tactics during the coverage period. Russia, Indonesia, India, and Ukraine follow suit, having implemented five tactics. India and Indonesia, for instance, used all tactics but the dominance of internet infrastructure. Meanwhile, Ukraine and Russia applied all tactics apart from internet shutdowns between 2016 and 2018. Yet, after the coverage period,

[82] This is one of the cases when an executive (Barrow) initiated the change of political institutions. Before the presidency of Barrow, the nature of political institutions in the Gambia was extractive. After his advent, the rules of the political game have become more inclusive. As I argue in chapter 3, political institutions shape the set of survival strategies and thus actions of political actors. However, actors can affect institutions as well, for example, after getting to office. This is what happened in the Gambia in 2017.

the Russian government resorted to the sixth tactic of internet control: it disrupted communications during the Moscow protests in August 2019 (Fokht 2019).

Table 14. Inclusive institutions and internet control (42 countries)

Number of employed tactics	Extent of internet control	Number (and list) of countries
6	Extensive (5 countries)	1 (Pakistan)
5		4 (Russia, India, Indonesia, Ukraine)
4	Significant (24 countries)	10 (Bangladesh, Brazil, South Korea, Lebanon, Malaysia, Myanmar, Nigeria, Singapore, Sri Lanka, Zimbabwe)
3		14 (Jordan, Angola, Argentina, Ecuador, Germany, Hungary, Kenya, Kyrgyzstan, Mexico, Philippines, Tunisia, United Kingdom, United States, Zambia)
2	Limited (13 countries)	8 (Australia, France, Georgia, Italy, Gambia, South Africa, Armenia, Malawi)
1		3 (Canada, Colombia, Japan)
0		2 (Estonia, Iceland)

As noted above, twenty-four countries with large-coalition leaders exercise significant control over information on the internet (table 14). Ten states out of twenty-four employed four tactics. All ten countries penalised users for internet activities during the coverage period. Besides, most of them passed restrictive internet legislation, swayed public opinion on social media, and censored online content. The remaining fourteen states used three information controls between 2016 and 2018. Although only one of them censored online content, all resorted to the punishment of internet users and online journalists. Likewise, most of these fourteen states, during the coverage period, adopted legislation, strengthening government’s powers in censorship or surveillance and organised disinformation campaigns on social media, manipulating public opinion.

The most used tactic of internet control among the forty-two countries with inclusive institutions was a crackdown on internet users for their activities in cyberspace (table 13 and figure 10). In thirty-three states, the punishment of digital citizens through arrests, detentions, raids, prosecutions, or fines was practised. For example, in Germany, the number of convictions for inciting hatred on the internet has increased. In addition, during the coverage period, the police in fourteen German states raided houses of thirty-six users for assumingly hateful posts on social media platforms (Shimer 2017). In the United Kingdom, there were numerous arrests for posting content associated with terrorism or offences related to race issues. In 2016 and 2017, more than three thousand internet users were detained for abusive posts on the internet (Freedom House United Kingdom 2018). Previously, in the United Kingdom, between 2012 and 2015, about twenty thousand users were investigated for their online comments (Bloodworth 2015). Greenwald (2015), after discussing numerous examples of persecution and prosecution for social media posts in the UK and the US, concludes that increasing control of internet activities encroaches on freedom of speech. The criminalisation of online speech, regardless of where it takes place[83], restricts the free flow of information on the internet.

The second most employed tactic among countries with inclusive political institutions was the implementation of restrictive laws that enhance either censorship or surveillance capabilities of respective authorities. Thirty-one out of forty-two countries implemented such a law between 2013 and 2018. In Germany, for instance, the Network Enforcement Act (NetzDG), in action since the beginning of 2018, requires social media giants (with more than two million users) to remove potentially illegal content that violates the German criminal code (Oltermann 2018). If not complying with the request on time, social media companies can be punished by large fines (up to 50 million euro). In the US, the 2015 USA Freedom Act came to replace some expiring sections of the 2011 Patriot Act that had expanded state surveillance capabilities, though now the National Security Agency needs permission from the FISA court to access communication data of individuals (Freedom House United States 2018, Hintz et al 2019: 71). In addition to internet-related legislation, the tactic of social media manipulation was also in demand in countries with inclusive institutions (twenty-nine out of forty-two countries).

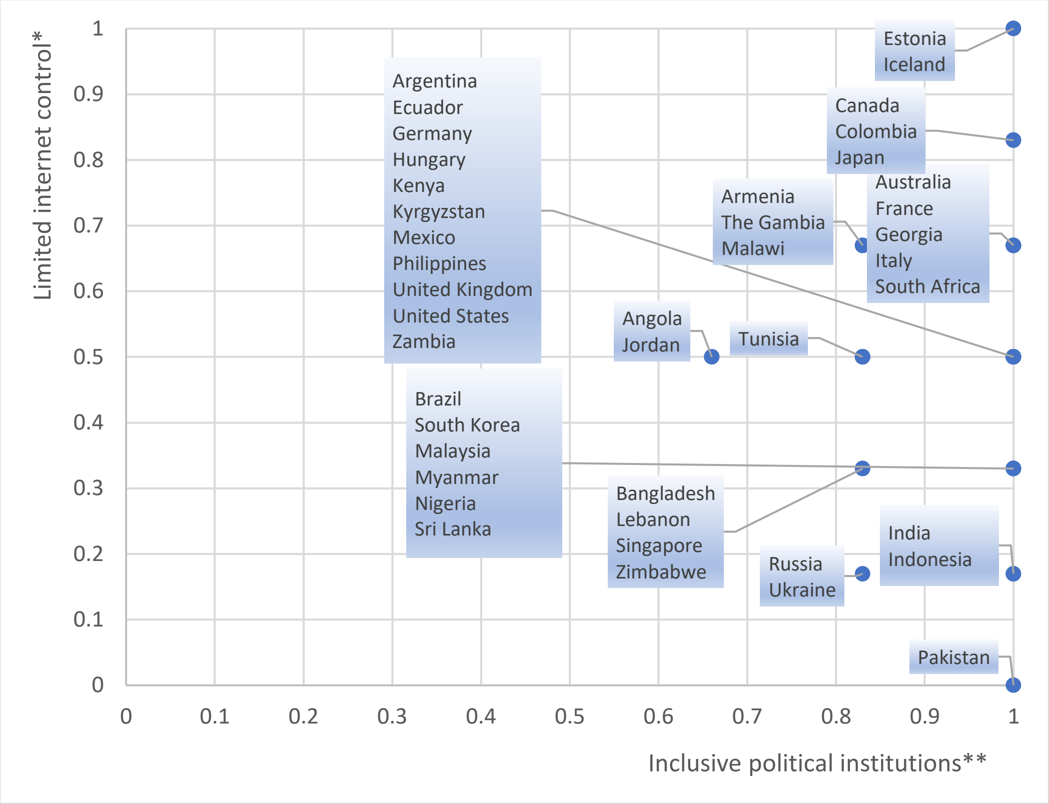
Online content censorship was reported in sixteen countries; this was less widespread than the aforementioned tactics but still included almost 40% of forty-two countries. For instance, the South Korean government systematically censored online content, specifically materials related to criticism of authorities, discussion of conflict or terrorism, and comments on social issues (Freedom House 2017, Freedom House 2018). Similarly, Malaysian state agencies, in addition to criticism of those in power, consistently filtered content related to political opposition, corruption accusations, and blasphemy between 2016 and 2018. Meanwhile, Indonesia blocked content related to social and LGBTI issues and occasionally filtered content, which criticised the government and discussed conflict, corruption, and religious issues. In addition, India, Indonesia, and Sri Lanka blocked social media applications and messengers during the coverage period.

The least employed tactics among countries with inclusive institutions were the domination of internet infrastructure and the disruption of communication services: ten and eight out of forty-two countries respectively resorted to these tools of internet control between 2016 and 2018. Despite the small number of countries involved in communications disruptions, India maintains the leading position in the world, repeatedly

[83] In countries with extractive institutions, detentions and arrests of internet users for terrorism-related posts also take place.

shutting down the internet in the country. Even after the coverage period, in August 2019, India continued the trend, deliberately disconnecting communication networks in the region of Kashmir, leaving several million people without both internet and phone access (Gettleman 2019). The latter is one of the numerous examples of disrupting internet services by the authorities of "the largest democracy in the world".

Figure 13. Political institutions and internet control (42 countries)
* the higher the QCA score in the Y axis, the more limited internet control[84]
** the higher the QCA score in the X axis, the more inclusive political institutions[85]



Although the average extent of internet control in countries with inclusive institutions is less entrenched, in most cases (e.g. India, Pakistan, South Korea, Brazil, Malaysia, Indonesia, or Ukraine) it is considerable (from three to six employed tactics) and can be certainly equalled to countries with extractive political institutions. Thus, in addition to numerous narratives of internet control scholars about "digital authoritarianism" and contrary to their implicit assumption that democracies do not (or will not) restrict the online flow of information, control of information on the internet by

[84] According to the negated calibration of the outcome, membership scores of limited internet control are 1, 0.83, and 0.66; significant – 0.5 and 0.33; and extensive – 0.17, and 0.

[85] According to the negated calibration of the condition, membership scores of more inclusive political institutions are 1, 0.83, and 0.66; and more extractive – 0.5, 0.33, 0.17, and 0.

the same tactics attributed to “digital dictators” was found in countries with inclusive institutions.

Consequently, it is more challenging to conclude with regard to the causal interplay between inclusive institutions and limited state interference with digital information. The inclusive nature of political institutions in most cases (twenty-nine out of forty-two) did not prevent chief executives and their large winning coalitions from exercising substantial control over information on the internet (three and more employed tactics). As can be seen in the top right side of figure 13, only thirteen countries have a limited extent of internet control whereas the remaining majority (all countries between 0.5 and 0 in the Y axis) exercise significant and extensive control of digital information. Thus, with the consistency rate of only 53%, *the causal relationship between inclusive institutional settings and limited control over the online flow of information is too weak to establish*. However, this means that there exists an additional intervening condition (or conditions) that leads to the implementation of numerous internet control tactics under the settings of inclusive institutions.

5. ADDITIONAL CONDITIONS OF INTERNET CONTROL

Based on the comparative analysis of internet control in countries with institutionally constrained executives, a more competitive political landscape, and fair and free selection procedures, I identified two more conditions that, despite the inclusive nature of political institutions, affect the extent of internet control. These factors are political instability and an upcoming leadership contest in the form of elections.

Examples of the first condition are issues such as regional tensions, street protests, ethnic conflicts, and emergency situations, among other things, that can undermine the domestic political stability and support of the chief executive. In the case of upcoming elections, the election process is expected to be freer and more transparent since in the context of inclusive political institutions it is more challenging to fabricate results (or “manufacture consent”) compared to countries with extractive institutions. Thus, when one of these conditions, or sometimes both, transpire, institutional constraints do not always limit the actions of large-coalition leaders as their political survival is specifically at stake at such moments. The main difference from small-coalition leaders is that the political survival of the latter is *constantly* at stake due to the lack of electoral legitimacy (Frantz 2018).

In other words, drawing insights from institutional theory, I initially expected to find the limited extent of internet control in countries with large-coalition leaders. In practice, however, most of the countries, regardless of the inclusive nature of political institutions, experience significant and extensive control over digital information. As it turned out, two additional conditions contribute to the implementation of numerous information controls. Consequently, building on the findings from the comparative analysis, the refined proposition is that in the context of inclusive political institutions, the presence of a politically unstable situation or an upcoming leadership contest (or both) tend to lead to a stricter approach to the internet. In the following sub-sections, I provide evidence that confirms the refined proposition.

5.1. Political instability and internet control

In this sub-section, I discuss the first condition of political instability. Before, during, and after the coverage period, many countries happened to resort to internet control tactics at the time of politically tense moments caused by various internal and external shocks such as regional conflicts, domestic protests, ethnic clashes, or disasters. Below, I demonstrate this tendency among the countries with inclusive institutional setups but substantial control of information on the internet.

The discussion starts with South Korea, a state with inclusive political institutions. According to Polity IV, elections in the country are competitive, the authority of the chief executive is substantially limited, and the balance of domestic political power is dispersed[86]. On the other hand, despite the robust functioning of institutions, the political climate in South Korea is not often stable, given its longstanding military and political conflict with the North Korean regime[87] (Kim 2019, Hancocks 2019). Hence, due to regional tensions, the distribution of North Korean propaganda has been outlawed in the country since 1948 under the National Security Act; violation might lead to lengthy prison sentences (Human Rights Watch 2015).

Consequently, information about North Korea has become a highly delicate topic among the South Korean authorities as they systematically censor online content related to its neighbour (Volodzko 2019). In 2018 alone, about 1 800 websites or pages were blocked or removed under the national security (that is, North Korean) pretext (Freedom House South Korea 2019). In addition to online censorship, individuals were penalised for publishing pro-North Korea materials on the internet (ibid). Furthermore, the punishment of internet users is a constant side effect of difficult relations with North Korea as arrests and imprisonments have occurred during the presidency of both more conservative Park Geun-hye (2013-2017) and more liberal Moon Jae-in (since 2017).

[86] During the coverage period of the comparative analysis, two individuals held the presidential office: Park Geun-hye from 2013 to 2017 and Moon Jae-in since 2017.

[87] The World Bank’s (2018) Global Governance Indicator of “Political Stability and Absence of Violence/Terrorism” also demonstrates that the political climate in South Korea is not always stable. The country scored from +0.11 to +0.42 from 2008 to 2017; the score ranges from -2.5 (fully unstable) to +2.5 (fully stable).

Even before the last two presidents came to power, the extent of internet control in South Korea was tangible under the rule of then-President Roh Moo-hyun (2003-2008)[88]. The testing by OpenNet Initiative in 2006 and 2007 revealed that South Koreans had no “access to a free and unfiltered Internet … [and were] criminally liable for posting “antistate” content” (Deibert et al 2008: 372). A few years later, a similar testing found the same pattern of substantial control over digital information, with North Korea-related content being the main target (Deibert et al 2012b: 360).

Other politically volatile events have also led to state control of information on the internet in South Korea. One such event was the 2014 tragic sinking of the “Sewol” ferry that took lives of 304 passengers. The handling of the catastrophe resulted in wide criticism (including on the internet) of then-President Park Geun-hye, significantly undermining her political support (BBC 2014, Choe 2014). In response to criticism, the South Korean authorities cracked down on online media reports and individuals critical of the government and its actions (Freedom House 2015). As a result, internet users were fined or imprisoned for their posts about the tragedy (Freedom House South Korea 2016). However, in retrospect, all these measures to control the dissemination of information over the internet did not help President Park to stay in office as her popularity fell after the disaster. In December 2016, she was impeached on charges of corruption and abuse of power (not related to the 2014 ferry incident) and in March 2017, was removed from the presidency (Choe 2018).

India is another country with inclusive political institutions that repeatedly resorts to internet control tactics at the time of political instability. India’s authorities during civil unrest indiscriminately cut off internet and mobile access, leaving millions of citizens without communication. The longest shutdown lasted 213 days, from August 2019 to March 2020, in Kashmir (Internet Shutdown Tracker n/d). The practice of disconnecting the internet in India has essentially become a routine in the wake of social or political disturbance, elevating the country to the leading position in the world. In 2019, there were 106 internet shutdowns, considerably more than in any other country (Internet Shutdown Tracker n/d). In 2018, the Indian authorities disrupted communication networks 134 times (Gettleman et al 2019); in 2017, the number of shutdown incidents was seventy (Freedom House India 2018). In addition, in 2017, twenty-two social media websites and messengers including Twitter, Facebook, YouTube, WhatsApp, WeChat,

[88] Interestingly, President Roh Moo-hyun was celebrated as the first “internet president” in the world for his widespread usage of new technologies in presidential campaigns (Watts 2003). Yet, despite the internet-friendly chief executive, South Korea shaped and limited information on the internet.

and Skype were blocked for one month in the Jammu and Kashmir state, a politically unstable and violence-prone region (Najar 2017).

Besides, political content is also periodically censored in India: for example, criticism of the government and leading party (BJP) on social media. Similarly, internet users are arrested for sharing anti-governmental materials and criticising or insulting politicians (Freedom House India 2017, 2018). Furthermore, the Indian public sphere is heavily manipulated by state-aligned mobs of online trolls, who assault all critics of the government and BJP, undermining anti-government narratives (Chaturvedi 2019). The Indian electronic army is well organised, having "fulltime staff members who are employed year-round to control the information space" (Bradshaw and Howard 2019: 18). As a result of the continuous employment of internet control tactics, Reporters without Borders (2020a) has put India, along with Russia, China, and Iran, in a list of digital predators – countries that resort to propaganda, surveillance, and censorship on the internet.

Pakistan is also a country with competitive elections and considerable limits on the executive authority, albeit with factional political competition, according to Polity IV. In 2010, new amendments to the constitution significantly circumscribed political power of the president and military, making Pakistan a "parliamentary democracy" (Bremmer 2020). Yet the country follows India being the second in the world to practice internet shutdowns; some of them lasting for months (Wagner 2018). The major pretext for communications disruptions is national security considerations. In addition, in 2017, social media was temporarily blocked in the whole country amid violent protests (Freedom House Pakistan 2018). Also, like in India, political content is thoroughly filtered while internet users are penalised for their anti-governmental stance. However, in some cases the severity of punishment is extraordinary: in 2017, two individuals were found guilty of blasphemy on the internet and given death penalties (Farmer and Gillani 2018). At the same time, it cannot be said that Pakistan is a politically stable country as it has a continuing territorial dispute with India over the Kashmir region along with other economic and social problems[89].

South Korea, India, and Pakistan are just three examples of countries with more inclusive institutions that employed information controls during politically volatile periods of protests, violence, and regional tensions. As I demonstrate in chapter 7, the Ukrainian leaders also exercised significant control over information on the internet amidst the ongoing conflict with Russia and the separatist war in Eastern Ukraine. From 2014

[89] The World Bank's (2018) Governance Indicator also demonstrates that Pakistan is a (highly) unstable country. The "Political stability" indicator of Pakistan ranged from -2.40 to -2.81 between 2008 and 2017.

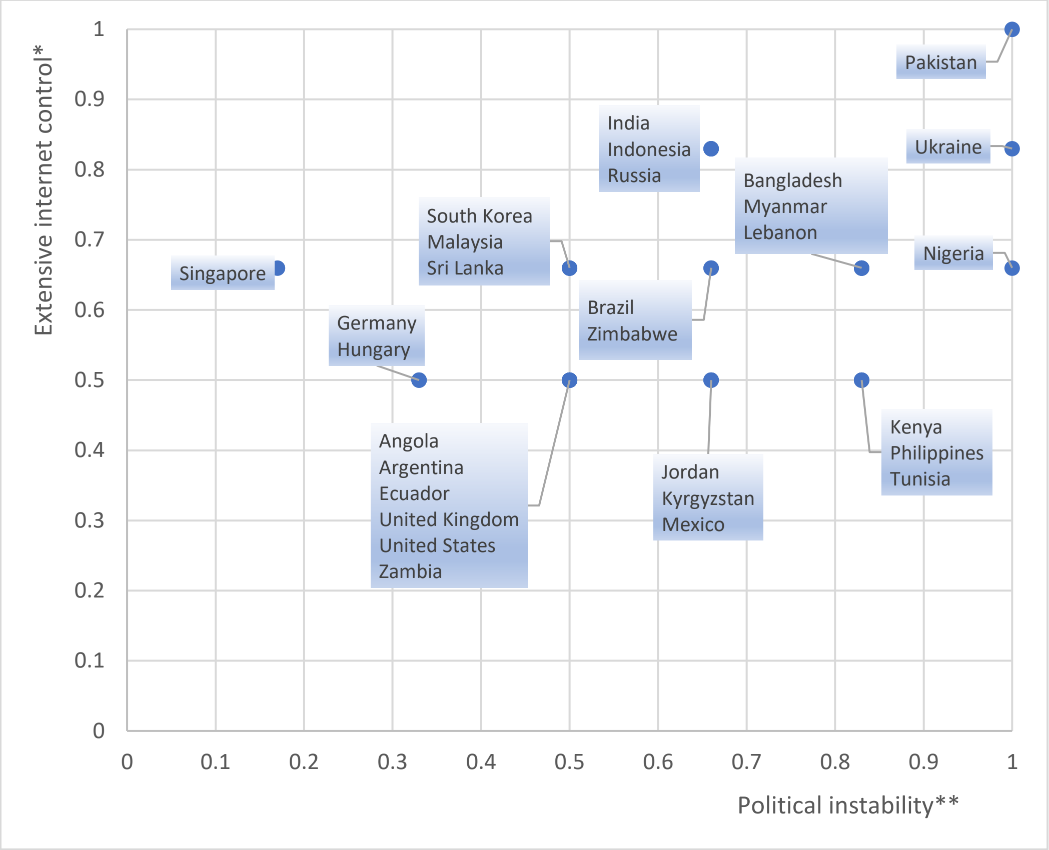
onwards – after Russia annexed the Crimean Peninsula – the number of employed internet control tactics increased. Many pro-Russian websites and social media platforms were blocked and numerous internet users were penalised for their political views expressed online (Freedom House Ukraine 2018).

Similarly, in Nigeria, numerous websites promoting the secession of one of the regions were blocked in 2017 (Freedom House Nigeria 2018) supposedly to secure political stability, given that Nigeria had previously fought a war with that region. In Myanmar, due to the high resonance of the Rohingya crisis, the leadership was involved in organising social media manipulation, spreading the pro-governmental narrative on the internet. Furthermore, the government has also prohibited to use the word Rohingya in news (The Washington Post 2018). Meanwhile, those who were reporting on the Rohingya crisis were targeted. For example, in 2017, two Reuters journalists were arrested and imprisoned for seven years; in 2019, they were amnestied (Ellis-Petersen 2019). Thus, the Myanmar authorities attempted to shape and limit the distribution of crisis-related information.

What is common in all these examples above is that the local authorities responded to political crises by seeking to control the online flow of information. This is because political instability could undermine the political support of those in power. A crisis and its (mis)handling by the government could eventually result in large-coalition leaders' loss of voters' trust and probably next elections, given that people "turn to the internet as a source of news and information in times of political crisis" (Howard 2010: 10). Consequently, stricter control over information on the internet tended to follow as to allow political leaders to hold onto power (that is, to be re-elected).

In the case of internet shutdowns and websites blockings, the authorities tried to restrict the dissemination of negative information on the internet. As Roberts (2018: 21-22) argues, such information could be hazardous for the government's survival. It is also of note that, in 2017, the United Nations Human Rights Council (2017) raised concerns about the states' regular use of internet shutdowns to control information, condemning and calling to stop the implementation of communications disruptions. In the case of fining or detaining individuals for their online activities in the aftermath of politically tense moments such as unrests, protests, conflicts, wars, or disasters, state agencies attempted to instil a sense of fear and self-censorship with the aim, again, to shape the dissemination of potentially negative information. Meanwhile, state-orchestrated manipulation of public opinion on the internet (via paid commentators and bots) served as “censorship through noise” (Pomerantsev 2019b: 37). However, such tactics did not always help political leaders stay in office[90].

Figure 14. Political instability and internet control (29 countries)
* the higher the QCA score in the Y axis, the more extensive internet control[91]
** the higher the QCA score in the X axis, the more politically unstable country[92]



Thus, the inclusive nature of institutions alone cannot guarantee the limited extent of internet control. When an event undermining political stability in a country happened, more tactics of internet control were employed. As can be seen in figure 14, only three countries out of twenty-nine (Germany, Singapore, and Hungary) were politically stable during the coverage period, whereas at least seventeen countries suffered from political instability[93]. Consequently, with the consistency rate of 86.6% (and the coverage rate of

[90] For example, as noted above, South Korean President Park Geun-hye did not manage to hold onto power. Similarly, as I discuss in chapter 7, Petro Poroshenko, the President of Ukraine from 2014 to 2019, despite the repeated employment of information controls, did not win in the following elections.
[91] According to the calibration of the outcome (chapter 4), membership scores of limited internet control are 0, 0.17, and 0.33; significant – 0.5 and 0.66; and extensive – 0.83, and 1.
[92] According to the calibration of the additional condition (chapter 4), membership scores of politically stable countries are 0, 0.17, and 0.33; neither stable nor unstable – 0.5; and politically unstable – 0.66, 0.83, and 1.
[93] The remaining nine countries, according to the calibration of the condition (chapter 4), do not clearly belong to either group, that is, they were neither evidently stable nor fully unstable.

89.8%) among twenty-nine countries with large-coalition leaders but significant and extensive control of digital information, I argue that *political instability*[94] *is a sufficient condition of substantial state control over the online flow of information*[95].

Furthermore, some recent events after the coverage period, in which governments decided to manage a crisis via the implementation of internet control tactics, confirm the refined proposition. For instance, the Bangladeshi government during the July-August 2018 students-led protests terminated communication networks in the country while individuals supporting the protests on social media were arrested (Lacy and Mookherjee 2020). In addition, in an attempt to control the online flow of information, stricter digital legislation was introduced in Bangladesh (Lacy 2018). Similarly, in April 2019 in the United Kingdom, London underground's internet service was made unavailable to the public on the police orders in response to the Extinction Rebellion group's protests (Embury-Dennis 2019). In another example, in April 2019, after the numerous bombings of churches and hotels by terrorists in Sri Lanka, the local government blocked social media applications to prevent the possible dissemination of rumours[96] (Bastians et al 2019). Previously, the Sri Lankan authorities also resorted to internet control at the time of disturbance. In February and March 2018, when violence between Buddhists and Muslims was sparked, leading to numerous riots on ethnic grounds, an emergency was declared with the following social media blockage and communications disruption (Freedom House Sri Lanka 2018).

In India, in December 2019, hundreds of thousands of people took to the streets protesting a newly passed citizenship law, fearing that it would lead to the discrimination of minority Muslim population (Gettleman and Abi-Habib 2019). The response of Indian authorities, along with curfews and troops deployment, included the (predictable) shutdown of the internet. The tendency to resort to information controls in the aftermath

[94] To calculate the causal relations between political instability and internet control in case countries, I resorted to the World Bank's (2018) Global Governance Indicator that "measures perceptions of the likelihood of political instability and/or politically-motivated violence, including terrorism" across the world. In chapter 4, I provide more details.

[95] The causal relations between political instability and internet control in all sixty-five countries: consistency is 83.5%; coverage is 83%. The causal relations between political instability and internet control in fifty-two countries (extractive plus inclusive institutions) that have significant and extensive internet control: consistency is 88%; coverage is 81%. All these mean that political instability leads to stricter control of digital information within both extractive and inclusive institutions. Besides, the reverse condition of political stability supports the refined proposition. The consistency between political stability and internet control in forty-two countries with inclusive institutions is 76% (coverage is 89.7%), which is sufficient to propose the causal relationship between the condition and the outcome. In this regard, the consistency of the condition of political stability with limited control of information on the internet does not undermine, but rather supplements, the proposition that political instability is consistent with substantial internet control. That is, when a political climate in a country is comparatively stable, there seem to be fewer incentives to control the dissemination of information online.

[96] Terrorist attacks in Sri Lanka led to more than 250 deaths.

of a political crisis continued in 2020. In June 2020, India, under national security considerations, banned fifty-nine Chinese applications including popular TikTok and WeChat (Phartiyal et al 2020). The action was evidently directed against China, being a result of heating regional tensions after the June 2020 border dispute, in which twenty Indian soldiers lost their lives (Gettleman et al 2020).

In addition, in 2020, following the refined proposition that political instability often leads to the implementation of internet control tactics, the global epidemiological crisis has not become an exception as well.

5.2. Covid-19 and internet control

The Covid-19 global pandemic has also affected the extent of internet control in countries with inclusive political institutions[97]. For example, in March 2020, the South African government adopted legislation that criminalised disinformation about Covid-19, extending state powers in censoring online content (Committee to Protect Journalists 2020). These regulations, which became part of the state policy to manage disasters, were already applied in April 2020. That month, a man was arrested for distributing a video on social media that ostensibly contained fake information about the coronavirus testing (Grobler 2020). South Africa, was not, however, the only country with inclusive political institutions that enacted legislation, expanding state powers to censor information flows during the epidemic.

In March 2020, amidst the coronavirus outbreak, Hungary passed an emergency bill, extending Prime Minister’s already sweeping executive powers (Walker and Rankin 2020). In addition, the law envisaged up to five years in prison for disseminating false information about Covid-19 (Picheta and Halasz 2020). The bill, consequently, brought criticism from human rights watchdogs and international organisations. Amnesty International (2020), for example, rebuked the new measure to imprison for disinformation as “inconsistent with international human rights law and standards”. The Organisation for Security and Co-operation in Europe (2020), too, criticised the new law, arguing that it can lead to the suppression of reporting about the coronavirus.

In the Philippines, in March 2020, the government also passed a Hungarian-like Republic Act (2020) that expanded President Duterte’s powers and designated a fine or prison sentence up to two months for spreading coronavirus-related disinformation on the internet. The same month, two online journalists and a city mayor were charged for violating the newly enacted bill, among other laws, by distributing ostensibly fake

[97] I do not discuss internet control in countries with extractive institutions during the coronavirus pandemic as small-coalition leaders resort to information controls regardless of political instability.

information via social media (Rappler 2020). Restrictive legislation in the wake of the epidemiological pandemic, in other words, by extending state powers to handle the crisis negatively affected the extent of internet control. In this context, it is also of note that democratically elected President Duterte is not fond of personal criticism, instead preferring to silence those who expose and criticise him and his government's policies. The case of Maria Ressa convicted of cyber-libel is illustrative of the current approach to online journalists in the Philippines. Besides, state-aligned pro-government brigades of trolls and bots are always ready to manipulate public perception of politically salient events, including the coronavirus.

Notably, legislation related to the dissemination of false information – be it about Covid-19 or otherwise – is relatively common in countries with inclusive institutional setups. In Brazil, for instance, a restrictive law known as "fake news bill" is currently under consideration. If passed, the bill would significantly extend the government's capability to censor online content, access internet users' data, and silence critics, thereby affecting the free flow of information and endangering the privacy of local citizens (Alimonti 2020). Likewise, in Ukraine, the authorities have been discussing the adoption of disinformation law. As I argue in chapter 7, the proposed law is a harsh encroachment on the media and freedom of expression as the document offers hefty fines for spreading disinformation and prison sentences for operating bots and fake accounts. In addition, the law envisages the creation of a position of a special government commissioner solely tasked with identifying and judging whether the information under question is fake. In both cases, governments seek to acquire sweeping powers to control the dissemination of information on the internet.

Besides legislation, South Africa and the Philippines are not the only countries with inclusive institutions that have resorted to arrests of journalists and/or internet users. In Bangladesh, eleven people were arrested and accused of distributing false information on social media about the government's handling of the coronavirus outbreak (Aljazeera 2020). Yet, there is an indication that these arrests could be politically motivated as one of the arrested was drawing and posting caricatures of political leaders on Facebook, whereas another person was criticising the government for the lack of the protection equipment. Similarly, in May 2020 in Malaysia, a local journalist came under investigation the next day after publishing an investigative report about the government's crackdown and raids on migrant workers during the coronavirus outbreak (Walden 2020). The journalist can now face up to two years in prison for the online article[98].

[98] The author under investigation is Tashny Sukumaran (2020).

India has also attempted to substantially control coronavirus-related information on the internet. In particular, in March 2020, Prime Minister Modi in a meeting with owners and journalists of mainstream media outlets urged them to provide positive coverage of the government's management of coronavirus crisis (Modi 2020). News media, in other words, was asked not to criticise the Indian authorities and serve as a supporter of the government. The interaction between the Prime Minister and journalists has been fruitful as the following news stories and articles about the response to the Covid-19 outbreak were not critical, despite many failures of the government (Sagar 2020). In addition, the same month, media outlets were requested via the supreme court's decision to cite and publish the government's official information about the coronavirus (Goel and Gettleman 2020).

In response, those who decided to express the disapproval of how the Indian government fights the pandemic have been targeted. For instance, a journalist was threatened and harassed by government-linked trolls, according to Reporters without Borders (2020b), after she published an online article about the belated and insufficient management of public health crisis and the cruel lockdown imposition by Indian state agencies[99]. There have also been numerous arrests of online journalists related to criticism of the government and the dissemination of ostensibly false information about Covid-19 (Awasthi 2020). In short, the intention of the Indian political leadership to command the news coverage after imposing the nationwide lockdown has been relentless, significantly shaping the free flow of information.

In other words, the authorities of the aforementioned countries with inclusive institutions resorted to information controls due to being worried that the government could be (and actually was) criticised for the insufficient response to the coronavirus outbreak. By enacting restrictive legislation and arresting critics of the government's handling of the epidemiological crisis, many countries limited the dissemination of information online. Overall, almost half of all members of the United Nations, including democratic ones, "have failed to respect the right to inform" in the wake of the coronavirus outbreak, according to Reporters without Borders (2020c). However, political instability, caused by various crises including the public health emergency, is not the only additional condition of state control over digital information. As I discuss in the following sub-section, a forthcoming leadership contest also leads to the employment of internet control tactics.

[99] The author is Vidya Krishnan (2020).

5.3. Leadership contest and internet control

The second identified pattern of internet control is the implementation of information controls during forthcoming elections – a leadership competition that, given the inclusive nature of political institutions, would eventually shape the distribution of political power, that is, whether a chief executive and his large winning coalition would stay in office for the next term. Due to a more competitive political landscape compared to countries with extractive institutions, the winner is often not known in advance and thus many executives, notwithstanding institutional constraints, tend to resort to internet control tactics in the ultimate pursuit of political power.

Overall, I found that out of twenty-nine countries with more inclusive political institutions but significant and extensive control over digital information fourteen held leadership contests in the form of general and local elections during the coverage period (between June 2016 and May 2018). These countries are Russia, India, South Korea, Lebanon, Malaysia, Angola, Ecuador, Germany, Hungary, Kenya, Kyrgyzstan, the United Kingdom, the United States, and Zambia. Notably, in all fourteen countries, elections were accompanied by internet control tactics with governments and political parties[100] being the main initiators. Moreover, in three additional countries (Pakistan, Mexico, and Zimbabwe) leadership contests were held in July 2018 (after the coverage period) but information controls were implemented in the lead-up to elections, thus covering May 2018 (the coverage period).

The most deployed tactic was manipulation of public opinion and the spread of disinformation on social media, mainly with the help of pro-government commentators and bots. Political actors (including the core executive) in almost all these countries engaged in social media manipulation in the wake of coming leadership contests. Besides, other tools such as blocking of websites and censorship of opposition materials, intimidation and arrests of journalists and users (those who criticised politicians and parties on the internet), adoption of restrictive laws, and communications shutdowns were also used by many governments. For instance, in Malaysia, legislation that extended government's powers in censoring online content was adopted while internet users were arrested shortly before the May 2018 election (Freedom House Malaysia 2018). These actions affected the dissemination of digital information in the country but did not help the incumbent large-coalition leader to stay in power. Nevertheless, it can be seen that at the time of the leadership contest, institutional constraints on executives and their coalitions do not always serve as a hindrance to the employment of information controls.

[100] Many of political parties later formed the government.

In some cases, both conditions (political instability and elections) can be presented. For instance, in some of the previously discussed countries suffering from an unstable political environment, the upcoming leadership contest also led to the implementation of internet control tactics. In Pakistan, in addition to numerous internet shutdowns during politically tense situations, the authorities resorted to disinformation campaigns on social media in the wake of elections. Thus, ahead of the July 2018 parliamentary elections, political parties were active in cyberspace, exploiting fake accounts and bots to advance their narratives on the internet (Shahid 2018). In Zambia, both conditions contributed to internet control: the unstable political climate was amplified by the upcoming elections in August 2016, resulting in the implementation of information controls. In particular, as a result of the leadership contest, communication services were disrupted, (opposition) websites were blocked, and internet users critical of the government were arrested (Freedom House Zambia 2017).

Similarly, in South Korea, government agencies also resorted to social media manipulation prior to elections. In 2017, a head of the security service was convicted of being involved in the organisation of digital disinformation campaigns to influence public opinion to the advantage of then-candidate Park Geun-hye in the lead-up to the 2012 presidential election (Chase-Lubitz 2017). Similarly, in 2019, a close associate of current President Moon Jae-in was found guilty of meddling in the 2017 election by orchestrating online opinion manipulation. Overall, “1.4 million comments, aimed at promoting Mr. Moon and his policies” were posted ahead of the leadership contest that altogether “generated 99.7 million “likes” and “dislikes”” (Choe 2019). In both cases, those involved were given jail terms for violating election legislation.

After the coverage period, the tendency to control information on the internet in the run-up to the upcoming leadership contest continued. In Bangladesh, the authorities disrupted communication services and blocked opposition websites in the wake of the December 2018 parliamentary elections (Freedom House Bangladesh 2019). Moreover, one month before the elections Skype was blocked to disrupt contacts between opposition leaders in exile and their supporters. This tactic to thwart the operation of social media platforms to prevent the interaction between dissidents and their followers is also common in countries with extractive institutions. For example, in Kazakhstan, every time an exiled oppositionist declared his forthcoming online streams, social media websites and messengers such as Facebook, Instagram, Messenger, and Telegram were denied access in the country (Webb 2016, Putz 2019).

In addition, the implementation of information controls after the coverage period was also reported in Indonesia, Ukraine, Brazil, India, Nigeria, and the US. As I discuss in chapter 7, shortly before the 2019 presidential elections in Ukraine, then-incumbent

Petro Poroshenko exploited a huge army of paid-for commentators and bots to improve his image. These digital supporters, known as “porokhobots”, praised Poroshenko and heavily criticised his political rivals, manipulating election-related narratives. In the US, a similar tactic of influencing public opinions was used by the leading political parties and actors in the lead-up to the November 2020 election. For instance, Trump’s team, in a pursuit to persuade the electorate to vote for the incumbent president, extensively invested in digital propaganda and misinformation campaigns (Coppins 2020). Meanwhile, all these manipulation actions (censorship through noise) shaped the online flow of information in both Ukraine and the US.

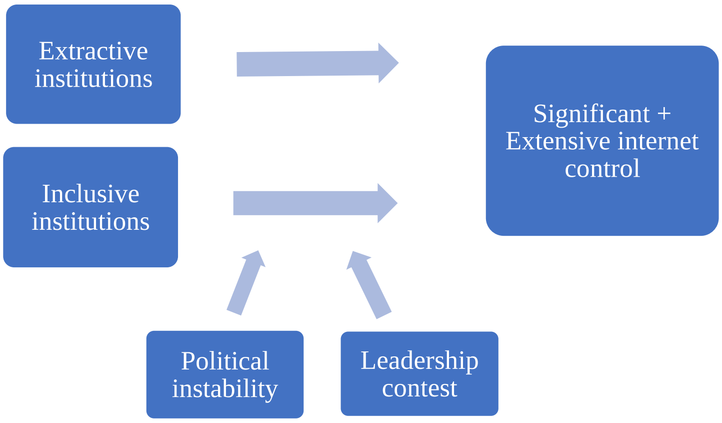
In countries with a limited extent of internet control, information controls were also applied in the wake of the leadership contest. For instance, in South Africa, in the lead-up to the May 2019 general elections, all main political actors and their associates were involved in manipulation of online opinion through social media (Freedom House South Africa 2019). Similarly, in Georgia, as a result of the coming presidential elections in October 2018, the ruling political party tried to influence the electorate by resorting to disinformation campaigns on the internet (Freedom House Georgia 2019).

In this regard, Bradshaw and Howard, similar to my findings, argued that in most cases government-organised social media manipulation of public opinion occurs “during elections, military crises, and complex humanitarian disasters” (2018: 3), that is, at the time of upcoming leadership contests and political instability. However, as I found, internet control tactics are implemented not only during military and humanitarian crises but also during civil demonstrations, ethnic conflicts, and street protests. Furthermore, besides disinformation campaigns on social media to sway public opinion, I also identified that many governments employ other tactics such as censorship of online content, blockage of social media websites and applications, shutdown of communication services, adoption of restrictive legislation, and punishment of internet users – all with the aim to control digital information in the wake of the leadership contest. In other words, governments are not confined only to social media propaganda.

Similarly, Deibert (2015: 69) argued that a tactic of communications disruptions is applied at the time of “elections, anniversaries, and public demonstrations”, albeit attributing it solely to authoritarian regimes. However, the authoritarians are not the only actors resorting to internet shutdowns as many large-coalition leaders, as demonstrated above, encouraged the implementation of this internet control tactic. Also, the latter tactic is not the only one being employed during elections and demonstrations. In brief, the findings of the comparative analysis presented in this chapter help to supplement the literature on internet control.

All in all, the first confirmed condition leading to substantial state control of digital information is the extractive nature of political institutions. In addition, I found intervening conditions (sometimes overlapping) leading to the increasing implementation of internet control tactics in countries with inclusive institutions. These are political instability (in the form of conflict, unrest, violence, or public health emergency, among other things) and an upcoming leadership contest (in the form of elections) (Figure 15). Under these additional conditions, many large-coalition leaders' governments tended to resort to information controls. Consequently, the proposition that the inclusive nature of political institutions leads to limited control of information on the internet was not confirmed.

Figure 15. Refined propositions (causal model)



6. CONCLUSION

In this chapter, I conducted a comparative study of political institutions and internet control in sixty-five countries. The aim was to explore and understand the effects of political institutions on the extent of state control over digital information. Following the comparative analysis, the first proposition that a more extractive nature of political institutions (small-coalition leaders) leads to a strict approach to the internet (that is, to a high number of employed tactics) was confirmed. I did not, however, fully confirm the second proposition as a more inclusive nature of political institutions (large-coalition leaders) was inconsistent with a low number of applied information controls. This is because many executives operating within inclusive institutions, in the wake of politically unstable situations (such as protests, violence, regional tensions, tragic incidents, or public health emergencies) and/or an upcoming leadership contest (such as elections), resort to various tools of internet control.

On the other hand, although one of the propositions drawn from institutional research was not confirmed, I was able to refine it by identifying additional intervening conditions of internet control. Hence, it can be argued that, despite the settings of more inclusive political institutions, numerous tactics to shape and restrict the online flow of information are nevertheless employed when there is an (existential) threat to the political survival of large-coalition leaders. Political instability and upcoming elections seem to intensify the incentive to hold on power as under such conditions many large-coalition leaders (such as in South Korea, India, Pakistan, Indonesia, Ukraine, Malaysia, Hungary, and many other countries) resorted to internet control, despite being institutionally restricted in their actions.

In this regard, some scholars (e.g. Diamond 2020, Goel and Gettleman 2020, Ben-Ghiat 2020) provide an agency-centred explanation, arguing that the advent of authoritarianism-prone leaders into power has led, among other things, to the systematic employment of information controls. Nevertheless, the tendency to restrict the dissemination of digital information was present in many countries with inclusive institutions even before would-be autocrats took office via democratic elections. For example, in India, the targeting of conflict-related online content that could lead to collective action, given the continuing unstable political situation in Kashmir and ensuing religious and caste tensions, was revealed in 2006-2007 and later in 2009-2010 (Deibert et al 2008: 286, Deibert et al 2012b: 300) – that is, before “authoritarian” Modi became the Prime Minister in 2014. The same tendency, as argued above, was reported in South Korea: censorship of online materials and arrests of internet users have been constant, regardless of who occupied the presidential office[101].

It is, thus, not only about political actors (though they play an important role as well) but also about the structural features in the form of domestic volatility and regular general elections. In the first case, there is a high consistency between political instability and information controls: when there is a political crisis, including the global outbreak of Covid-19 in 2020, that undermines domestic stability and political support of incumbents, survival strategies are in action. The same logic plays out in the wake of coming leadership contests. Most countries with more inclusive institutions that held elections during and after the coverage period, as a result, resorted to different internet control tactics[102]. All these also mean that a more inclusive nature of political institutions is insufficient for the limited extent of control over information on the internet.

Hence, my refined argument is that there are now two explanations for internet control. The first, as it was proposed, is the extractive nature of political institutions (such

[101] In chapter 8, I further extend on an agency-structure explanation of internet control.
[102] In the case of extractive political institutions, there is no necessity for a political crisis to emerge as hold on power of executives is continually at risk due to the lack of electoral legitimacy (Frantz 2018).

as in China, Iran, or Kazakhstan). The second, refined, is the presence of political instability or an upcoming leadership contest (or both) within inclusive institutions (such as in South Korea, Ukraine, or India). In other words, it is not only authoritarian countries with extractive institutions that substantially control information on the internet. Many democracies with inclusive institutional settings also systematically employ information controls. Consequently, in the following chapters, I proceed to two case studies that represent both – confirmed and refined – propositions. I study the causal relations between the extractive nature of political institutions and internet control in more detail, drawing evidence from Kazakhstan (chapter 6). After that, I analyse the interplay between inclusive institutions and control of digital information in the wake of political instability and an upcoming leadership contest in Ukraine (chapter 7).

The comparative analysis of sixty-five countries allowed the identification of general patterns and regularities in the relationship between political institutions and internet control and, thus, served as the first important step to explore and understand conditions of state control over information on the internet. The next and final step is to further examine (and illustrate) how and whether political institutions affect the extent of internet control. Therefore, the case studies, following the findings of the comparative analysis, shed more light on details of internet control. If the comparative analysis of a large sample of countries provided for the breadth, two case studies are expected to deepen the study of tactics and conditions of state control over digital information.

CHAPTER 6. EXTRACTIVE POLITICAL INSTITUTIONS AND INTERNET CONTROL: A CASE OF KAZAKHSTAN

1. INTRODUCTION

In the previous chapter, two main conditions of substantial state control over digital information[103] were identified. These are the extractive nature of institutions and political instability and/or a forthcoming leadership contest within inclusive institutional settings. In this chapter, I conduct a case study of Kazakhstan to examine the interplay between extractive institutions and internet control. In this regard, Kazakhstan represents a typical approach of governments to digital information under the extractive institutional setup.

In the case of Kazakhstan, one needs to trace the development of political institutions to understand how information on the internet became eventually heavily controlled by the state. In the early 2000s, when the first internet users were emerging in Kazakhstan, the country had already become irrevocably undemocratic: the president was the only source of political power, the election process was manipulated, and the regime's opposition was co-opted or destroyed. As a result of the established extractive nature of political institutions, the Kazakh government adopted a strict regulative policy towards first the printed press and then the internet. The main cause for media and internet control lies in their ability to transform political institutions by opening them to a wider segment of society. As political institutions were already amended to provide the first President with the extensive authority, the latter had no intention to initiate the redistribution of political power, that is, to change institutions[104].

Consequently, given that the internet was widely perceived as a democratiser (as discussed in chapter 2), legislation was introduced to give the Kazakh authorities more powers and leverage over cyberspace. Now, the General Prosecutor's Office and the National Security Committee can disconnect communications and restrict internet access nationwide without a court decision. Internet-related laws and programs also attempted to justify the heavy regulation of media and technology spheres, mainly under security provisions. However, in practice, the government resorts to censorship largely to stop the circulation of critical and oppositional content. Kazakh agencies also cut off communication signals and internet access in the whole regions in the event of street protests, ethnic clashes, and during dissidents' online broadcasts. The main rationale, again, is not to allow the distribution of negative information. Technically, it is not difficult

[103] As defined in Chapter 4, substantial internet control means the employment from three to six out of six information controls (significant and extensive extent of internet control).

[104] Actually, as I demonstrate below, after fighting with parliament members between 1991 and 1995, the President acquired a wide range of executive authorities not to easily give them up with the advent of the internet.

for the government to implement information controls as the key internet infrastructure and actors belong to or obey the state. Yet, if all these measures are insufficient to keep the President's rule intact, then the punishment of internet users and online journalists in the form of harassment, arrest, and/or prosecution follow suit. The Kazakh state, in essence, resorted to all main internet control tactics to secure the political survival of the chief executive.

Therefore, to understand the relationship between institutional structures and internet control, I first discuss the development of political institutions in Kazakhstan (section 2). It is important to trace the evolution and change of institutions as they affect the severity of state control over digital information. After that, the legislative framework that provides state agencies with the necessary tools and justifications to exercise control over communication networks and the distribution of information in the country is analysed. I also study how the authorities employ tactics such as online censorship, internet shutdown, communication surveillance, social media propaganda, and a crackdown on users and journalists (section 3). My conclusion is that since political institutions became acutely extractive, the internet had few options but to be heavily controlled (section 4).

2. EXTRACTIVE POLITICAL INSTITUTIONS

The evolution and change of political institutions in independent Kazakhstan are closely associated with Nursultan Nazarbayev, the President from 1991 to 2019. Nazarbayev became the only major player on the Kazakh political arena, gradually changing the "rules of the game" to his advantage[105]. Political institutions were eventually amended to prolong the President's political life. Thus, in this section, I trace the development of political institutions in Kazakhstan, discussing first a short power contest between Nazarbayev and the Parliament (sub-section 2.1.). For a while, there was a possibility of more democratic development of the country. However, the consequent consolidation of political power by the first President led to irrevocably extractive institutions (sub-section 2.2.). This transformation of political institutions would eventually affect the extent of state interference with the internet (section 3).

2.1. The first President and Parliament

The initial development of political institutions in Kazakhstan was affected by the power struggle between the President and Parliament. The former tried to accrue the political

[105] Nazarbayev resigned only on March 19, 2019 after being the president of independent Kazakhstan for 28 years. However, he still exercises enormous influence on domestic politics.

authority to ultimately and solely rule the country whereas the latter fought back, attempting to balance the executive's power and gain more authority for the legislature. The President eventually won over the legislature's claims to dominate the political landscape and, having diminished Parliament's powers, proceeded to change political institutions in line with his whims. Thus, the 1990s were important for the formation of political institutions in Kazakhstan. After the "Rubicon" was crossed after the second dissolution of the defiant Parliament in 1995, political institutions have eventually ceased to be independent, having no influence on the real balance of domestic political power. Political oppositionists were either co-opted or silenced and the rules of the game were amended so that the President could dominate Kazakh politics.

Even before the collapse of the Soviet Union, Nazarbayev had been the influential political figure in the Soviet political hierarchy, holding key positions in communist Kazakhstan: the Council of Ministers' head (the second-highest rank in the republic) from 1984 and the Kazakhstan Communist Party's first secretary (the highest rank) from 1989. In April 1990, following the creation of the Soviet Union President's post for Gorbachev, Nazarbayev also became the President of the Soviet Republic of Kazakhstan[106]. Finally, on 1 December 1991, Nazarbayev became the first President of independent Kazakhstan[107]. Nevertheless, he did not have much political power at the time, having to manoeuvre and compromise with another looming political force, the Parliament.

Although Nazarbayev was a popular political figure in Kazakhstan (and within the Commonwealth of Independent States), his authority at the dawn of independence was balanced by the Parliament that held capabilities to control the executive branch. The first half of the 1990s was thus characterised by the conflict between the head of the legislature (S. Abdildin) and the President (N. Nazarbayev) (Borisov 2018: 50). The main disagreement between the Parliament and the President had been over the political system: whether the country should be parliamentary or presidential. The former insisted that Kazakhstan was better to be a parliamentary state whereas the latter claimed that (strong) presidentialism was the best option in the transition period (Cummings 2005:

[106] Nazarbayev was not elected by Kazakh citizens via regular elections but was chosen by the Supreme Soviet's (legislature) members, in line with the then functioning 1978 constitution of Soviet Kazakhstan (The Constitution of the Kazakh Soviet Social Republic 1978). Notably, already in May 1990, laws protecting the President's reputation were passed, establishing fines for insults and slander against Nazarbayev (Borisov 2018: 46).

[107] According to Hiro (2009: 247), Nazarbayev's sole opponent Kozhakhmedov, the head of the Zheltoksan opposition party, failed to provide a necessary number of signatures to participate in the leadership contest (one hundred thousand was required) due to the assault. However, Kozhakhmedov could not have challenged Nazarbayev given the popularity of the latter (Chebotarev 2015: 55). Eventually, 88% of voters attended the elections and, left with the only option, 98.8% of them chose Nazarbayev as a president of Kazakhstan (Sputnik Kazakhstan n/d).

24). The favour of one political system over another would eventually mean the dominance of either the President or the Parliament. Evidently, none of them wished to voluntarily give up in the ensued power contest. Besides, Abdildin was demonstrating presidential claims while the Parliament as an institution was increasingly gaining political ambitions (Olcott 2010: 107-108). The Parliament thus became the direct competitor of Nazarbayev, challenging his design of the political system of Kazakhstan.

Beset by growing claims of the legislature, Nazarbayev eventually found a way to outmanoeuvre the competing institution. In December 1993, the 12th Parliament (the Supreme Soviet at the time) was voluntarily dissolved by the initiative of the President's administration. A call and justification for the dissolution by Nazarbayev, eventually supported by most of the deputies, was based on the argument that the Parliament, being a last Soviet-era-elect body, had not been elected in a democratic manner (Cummings 2005: 25). In this context, it is important to note that the President had no authority to dissolve the legislature, and consequently had no direct influence over the defiant legislative branch. Only later, in 2007, by amending the constitution, the President would acquire the right to directly dissolve the legislature. At the time, though, in the absence of other options, the President asked the Parliament to self-dissolve[108].

After the voluntary dissolution, there was no legislative body from December 1993 to March 1994, until the next elections were held. The President exercised the legislative authority in the absence of the Parliament (Borisov 2018: 319). Nevertheless, the self-dissolution of the first legislature and election of the second did not significantly change the distribution of political power in Kazakhstan. The following Parliament did not become fully obedient in the way the President had envisioned. For instance, the 13th Parliament's speaker (A. Kekilbayev) was claiming more rights for the legislature and was trying to make the government more accountable (Olcott 2010: 109). In addition, in May 1994, the Parliament expressed a vote of no confidence in the government (ibid, 103). A growing appetite of parliament members for political power, claiming more authority and supervision rights, eventually led to the Constitutional Court's decision of March 1995 to nullify the 1994 parliamentary elections (ibid, 108-109). Nazarbayev, still having no constitutional right to directly dissolve the Parliament, resorted to the less disobedient Constitutional Court. The 13th Parliament was thus formally dissolved.

By "destroying" the legislative organ, the President was trying to topple his political opponents. After two consecutive attempts to terminate the Parliament within less than one- and half years, Nazarbayev managed to subdue the legislative branch to

[108] There is no clear answer to why the Parliament agreed to self-dissolve. Kurtov (2000) and Borisov (2018) argue that some of the deputies were co-opted by the President.

his will. In retrospect, the second dissolution of the last competitive legislature by hands of the Constitutional Court was a turning point in the political history of the young country. For the Parliament at the time "was beginning to develop some of the fundamental characteristics of an institution capable of providing the checks and balances essential to the functioning of a pluralistic society" (Olcott 2010: 109). As the following events demonstrated, the 1994 Parliament was the last and closest to be called a democratic institution. Since then, the President began accruing more political power, indicating no intention to share or give it up. This is not to mention measures that, as I discuss below, institutionalised the dominant position and role of the first President in the ensuing period.

2.2. Consolidation of (unlimited) political power

The two dissolutions of the Parliament were critical junctures in the political history of independent Kazakhstan. After submitting the legislature to his will, Nazarbayev amended the integral parts of political institutions so that he could stay in office as long as he wanted. Thus, the executive selection was changed, exclusively permitting Nazarbayev to participate in the presidential elections the unlimited number of times. Constraints on the executive authority were also modified, removing any restrictions on the first President's power while shrinking capabilities of the legislature and government in the decision-making process. Finally, political participation was also severely restricted whereas the opposition became too fragmented to defy the incumbent.

Consequently, after the second termination of the legislature, the first President was already in a position to extend his presidency without holding elections. Nazarbayev, following Islam Karimov of Uzbekistan and Saparmurat Niyazov of Turkmenistan, decided not to participate in the elections originally scheduled for 1996. Instead, in April 1995, the term of the first President was prolonged until 2000 via the national Referendum: 91% of voters turned out, with 95% of them voting for the extension of Nazarbayev's mandate (Moldabekov 2015).

The Assembly of Peoples of Kazakhstan (created a month earlier) initiated the Referendum to extend the incumbent's tenure ostensibly "in order to maintain the unity of society and to avoid the deep polarization of political and social situation in the country" (Razina 2016). Nazarbayev himself justified the necessity of extending his tenure, arguing that "the leadership struggle of any kind is not in the country's best interests" (Inter Press Service, 1 May 1995, quoted in Hiro 2009: 259). As can be seen, narratives were employed to rationalise the necessity of not holding presidential elections[109]. These

[109] However, the growing recognition and prominence of opposition leaders also contributed to Nazarbayev's decision to avoid the presidential elections. At that time, Olzhas Suleimenov, a

(unfair) practices of engaging the state apparatus (in this case, the creation of the Assembly of Peoples to advance the Referendum to extend the presidential term allegedly on behalf of peoples of Kazakhstan) and conveying narratives to legitimise such actions would soon become institutionalised. Furthermore, calls for early elections would also be one of the main features of the Kazakh political game. The following presidential and parliamentary elections, with a few rare exceptions, were summoned prior to the planned schedule to disadvantage opposition leaders, depriving them of necessary time for preparation and campaigning.

In addition, in August 1995, a new Constitution of the Republic of Kazakhstan (1995) was accepted. According to the document, the Parliament was no longer able to control the execution of the state budget, losing its main leverage over the government. Meanwhile, the President became more independent in pursuing policies with no need to consult with the government, legislature, and judiciary and receiving the right to assign members of the Constitutional Council, heads of regional courts, and governors (akims) of districts. It also became almost impossible to legally oust the President. In line with article 47, the President can only be deposed due to two reasons: illness and treason. Yet, the final decision should be accepted by the vast majority (¾) of deputies from both houses. Given that parliament members were much less defiant from 1995 onwards, it became much more difficult to imagine a scenario of constitutional impeachment of the President. Hence, by 1995, the President had consolidated a significant amount of political power. As a result, though, the country was ultimately turning authoritarian.

In October 1998, early presidential elections to be held in January 1999 were announced. Previously, the incumbent's rule was extended by the Referendum. This time, instead of planned elections in 2000, the President used the practice of early elections that gave the opposition only one month to nominate a candidate (Borisov 2018: 385). The political opposition was caught off-guard and had no time to organise large-scale campaigns. Eventually, four contenders ran for the office, though the main contender, Abdildin, the ex-head of the Parliament and leader of the Communist Party, received only 11.7% of votes. Another leader of the opposition, Kazhegeldin, was disqualified from the participation in the elections (Hiro 2009: 267). Nazarbayev won with 79.8% of votes, though the OSCE[110] observation mission concluded that the election

renowned Kazakh writer and an initiator of the environmentalist anti-nuclear movement "Nevada-Semipalatinsk", and then Prime Minister Akezhan Kazhegeldin could have challenged the first President (Cummings 2005: 26, Olcott 2010: 115), making the elections much more competitive in comparison to 1991. Against the President and his government was also a worsening economic situation, leading to the rise of prices and discontent among the population (Olcott 2010: 101, 107). As a result, the chief Kazakh executive, worried that the political opposition could capitalise on deteriorating economic and social conditions, preferred an alternative to the elections.

[110] Kazakhstan is a member of the OSCE.

process (as well as other that followed) was not held in line with the OSCE norms of fair elections (The Organisation for Security and Co-operation in Europe 1999).

Crucially, in June 2000, the Constitutional Council declared Nazarbayev's victory in the 1999 presidential election as his first presidency, contending that the previous election in 1991 was held under the old constitution (The Constitutional Council 2000). Thus, Nazarbayev's presidency from 1991 to 1999 was merely nullified (Radchenko and Rakhmetov 2020). This decision also meant that the first President could legally run for the second term. In other words, the rules of the political game were baldly changed with a single purpose: to prolong the political life of Nazarbayev. The institution that nullified the first term of the President was the same body that approved the dissolution of the 13th Parliament – the Constitutional Council, a successor of the Constitutional Court.

To further consolidate political power, in May 2007, new amendments to the constitution gave the President the right to directly dissolve the Parliament after consulting with the heads of upper and lower houses and the prime minister[111] (Law on Amendments to the Constitution 2007). Given that the government and Parliament became "hand-picked" and "rubber-stamp" institutions respectively, new amendments simply indicated that Nazarbayev could suspend the legislature at any time. Besides, the most important amendment with far-reaching consequences was that the first President was formally excluded from the constitutional limit of two presidential terms. Nazarbayev could be legally re-elected as many times as he wished.

In June 2010, sweeping powers of Nazarbayev were further extended as the 2000 law on the first President was amended (Constitutional Law of Kazakhstan 2010). Nazarbayev's role in state-building was reconsidered from "one of the founders" (as up to the previous version) to "the founder" of independent Kazakhstan. His immunity from the prosecution was also modified. According to the previous variant, the first President could be legally held responsible for the acts of state treason. In line with new amendments, Nazarbayev cannot be charged for any actions (including treason) during and after his presidency, making his retirement comfortable and completely free from the (possible) prosecution[112]. Another important innovation, following the "Turkmenbashi" title of Niyazov, was to introduce a special title of the "Leader of the Nation" (from capital letters) to Nazarbayev. Nazarbayev thus became the first President, the founder of independent Kazakhstan and the Leader of the Kazakh Nation able to be re-elected the

[111] Previously, Nazarbayev could terminate the Parliament only after the latter expressed a vote of no confidence in the government, twice rejected a candidate for the premiership, or in time of insurmountable disagreements between the legislative and executive branches (Borisov 2018: 207).

[112] It is of note that the prosecution of ex-presidents is common in authoritarian states.

unlimited number of times and impossible to be impeached[113]. As it is the law on the first President of Kazakhstan, all clauses of the document apply only to Nazarbayev.

After twenty years of presidency, Nazarbayev again called for early elections to be held in April 2011 (RBC 2011). Previously, February 2011 amendments to the constitution rendered the President with the right to declare extraordinary presidential elections (Law on Amendments to the Constitution 2011). Thus, an informal practice regularly employed in the past was institutionalised in the constitution. Consequently, institutional constraints in the form of holding early presidential elections (instead of planned for 2012) gave the incumbent a clear advantage, (again) depriving other contenders of time to prepare and organise political campaigns. Unsurprisingly, Nazarbayev won with overwhelming 95.5% of votes. The last elections of the first President in 2015 were also held earlier than planned – Nazarbayev won with 97.75% of votes[114].

The record percentage of Nazarbayev's total votes in the elections reflects the fragmentation of political opposition. The latter, since the mid-1990s, was tamed by the first President by manipulating the rules (adjusting legislation to the President's advantage), employing various practices (of early presidential and parliamentary elections, dissolutions of the legislature, holding Referendum to extend the tenure), and conveying narratives (publicly justifying the necessity of implemented actions). Nazarbayev, in addition to the unlimited presidential mandate and powers, also became able to dissolve the Parliament at any time. As a result, the political opposition not represented in the legislative branch (as well as in the hand-picked government and judiciary) drastically withered. Although not destroyed completely, those oppositionists who courageously decided to challenge the rule of the first President found themselves

[113] The President's minions did not stop paying tributes to Nazarbayev. To commemorate his induction into the presidency, in December 2011, a day of December 1 (date of the first presidential elections in Kazakhstan) was named a day of the first President of Kazakhstan due to his high achievements and officially became a state holiday. July 7, a day of moving the capital from Almaty to Astana, is also a state holiday, coinciding with the President's birthday. Though, the scale of honours devoted to the first President was only growing. Now, in addition to Nazarbayev avenues and parks, the airport, university, library, museum, and numerous schools bear his name. The apogee was a decision in March 2019 to rename the capital city from Astana to Nur-Sultan, the first name of the President.

[114] In February 2015, the Kazakhstan Assembly of People asked the President to have the extraordinary presidential elections, justifying it by the complicated situation in the world. Nazarbayev expectedly agreed with the proposal (BBC 2015). In April 2015, the first President easily won, receiving the record percentage of votes.

either co-opted[115], exiled[116], or dead[117] (assassination or suicide). Even being a part of Nazarbayev's family did not guarantee immunity from a purge as Rakhat Aliyev, the President's son-in-law, could have attested[118]. The destiny of oppositional political figures, regardless of their affiliation with Nazarbayev, was predetermined once they turned their back to the President. Eventually, the opposition became fragmented to the extent that it represented no challenge to Nazarbayev.

Thus, Nazarbayev managed to change political institutions and expand the executive authority to a great extent. Three integral institutional aspects such as the election process, executive constraints, and political competition were transformed so that the first President could unilaterally rule the country for almost three decades. Although 79-year-old Nazarbayev decided to voluntarily step down as the President of Kazakhstan in March 2019, he continues to hold an exceptional range of political authorities as the first President, the Leader of the Nation (Elbasy), and the head of the Security Council. Moreover, in October 2019, Kassym-Zhomart Tokayev, Nazarbayev's successor and the second President of Kazakhstan, singed the order that obligates him to consult with the head of the Security Council (that is, with Nazarbayev) the appointment of all ministries apart from the ministries of foreign affairs, defence, and internal affairs (Decree of the President of Kazakhstan 2019). Even in his retirement, the first President continues to exercise enormous influence on domestic politics.

However, as a result of the transformation of political institutions, Nazarbayev's authoritarian regime influenced all key spheres of life in the country, including the media and technology area. The internet, as I demonstrate in the following section, was not an exception as it represented a potential (liberating) threat to the regime, being in a position to undermine the extractive institutional setup. Consequently, the internet, like the printed media, came under extensive state control.

3. INTERNET CONTROL

Currently, 18-million Kazakhstan has one of the highest internet penetration rates among the post-Soviet countries. Internet access in the country rocketed from 0.67% in 2000 to 81.8% in 2019 (figure 16). Although the number of internet users in Kazakhstan in the

[115] Olzhas Suleimenov, a very popular public figure, was appointed the ambassador to Italy in 1995.

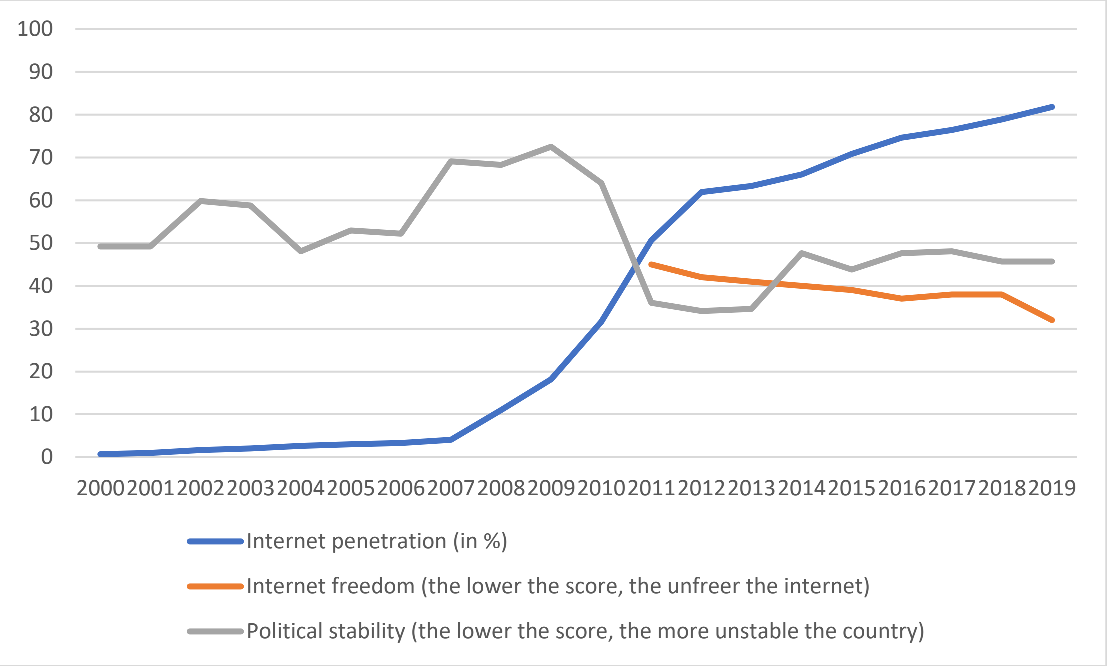
[116] Akezhan Kazhegeldin, a former Prime Minister and oppositionist, left the country in 1998. Mukhtar Ablyazov, an outspoken critic of the President and regime's opponent, left the country in 2009.

[117] In 2005, Nurkadilov, an oppositionist, committed a suicide. In 2006, Sarsenbayev, a vocal critic of Nazarbayev's regime, was killed (the main organiser of the assassination appeared to be Aliyev, his political opponent (Lillis 2019: 30)).

[118] Rakhat Aliyev, who turned against the President, committed a suicide in Vienna's prison in 2015.

early 2000s, not to mention the 1990s, was small, the Kazakh authorities, as I demonstrate below, have begun controlling information on the internet from the very beginning. This was possible given that the proliferation of the internet (and mobile phones) from 2000 onwards began at the time when political power in Kazakhstan had already been centralized by Nazarbayev. As a result, the internet sphere had no other way as to follow the path of printed media, that is, to be heavily regulated.

Figure 16. Internet penetration[119], internet freedom[120], and political stability[121] in Kazakhstan



Initially, the printed media in the 1990s and the internet in the 2000s were in a position to transform political institutions in Kazakhstan. Both the press and digital technologies could have shaped the distribution of domestic political power by giving a voice to the opposition and critical opinions and by subjecting institutions and politicians to accountability and transparency. The internet was able to facilitate the exchange of alternative information, empowering grass-roots movements and consolidating opposition forces. Hence, keeping this liberating potential of the internet in mind and also fearing the repetition of "colour" and Arab Spring revolutions in Kazakhstan, the President and his entourage, already authoritarian by 2000, resorted to internet control

[119] According to the International Telecommunication Union's statistics. Available from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[120] According to Freedom House. The scores for all but the 2019 year were reversed. The score for 2019 was already reversed by Freedom House.

[121] According to the 2018 World Bank Worldwide Governance Indicators. The indicator of political stability was included for comparison with Ukraine.

tactics in order to secure political survival. As the rules of the game had already been amended so that Nazarbayev could indefinitely stay in office, it was not hard for government agencies to start exercising control over the expanding digital sphere.

In addition, the Parliament, too, was in the pocket of the first President, ceasing to be independent. It was crucial for the President to be able to control the legislature as the latter consequently stamped all necessary internet-related laws. In this context, the legislative framework is essential for the political survival of the regime for two main reasons. First, it attempts to provide a rationale for government interference in the digital domain under various grounds (for example, the security pretext). Second, legislation gives government agencies legal tools to manage and command communications and the distribution of information. Consequently, as political institutions were under the command of the President, a year by year, control over information on the internet in Kazakhstan has only been strengthened.

3.1. Internet-related legislation

Legislation regulating the internet was introduced when the first President had already consolidated extensive political powers in his hands. Overall, several laws such as on Mass Media (1999), Communication (2004), Personal Data and its Protection (2013), National Security (2012), and Informatization (2015) were adopted. In addition, Concepts of Information Security (2006, 2011) and Cybersecurity (2017) that define the main threats to cyberspace of Kazakhstan affect the regulation of the internet. Finally, “Informational Kazakhstan – 2020” (2013) and “Digital Kazakhstan” (2017) programs also deal with the internet, outlining the main steps for the transition to information society and digitalisation of Kazakh economy and life.

As I discuss below, internet-related laws and policies provide a solid foundation and justification for state involvement in internet regulation while national security provisions under the pretext of fighting terrorism and extremism have become one of the main formal reasons for state intervention. Furthermore, state strategies such as the 2017 Cybersecurity Concept and the 2017 Digital Kazakhstan Program attempt to justify the increasing role of the state in the internet sphere by providing vague and general statements, whereas the role of society and its interests are hardly outlined, if reflected at all.

3.1.1. Restrictive legal framework

The first main document related to the internet in Kazakhstan was a Law on Mass Media (1999) passed in July 1999. Crucially, by that time, main Kazakh media outlets already belonged to the first President’s family (Djankov et al 2003: 353). The print press in

Kazakhstan enjoyed the relative freedom only in the first half of the 1990s, at the time of (12th and 13th) Parliaments' resistance to the President (Olcott 2010: 104). In the second half of the 1990s, when the resistance was broken and the legislature was eventually tamed, the freedom was gradually restricted. As a result, the most influential Kazakh press enterprises and TV channels came under control of the President's entourage. For instance, in 1998, a mainstream Kazakh newspaper (Karavan) that was criticising Kazakh politicians and state policies changed owner. Consequently, the direction of the newspaper's political narrative was also changed, becoming more loyal to Nazarbayev's regime (Mamashuly 2011). Likewise, the TV network “Khabar”, owned by President's daughter Dariga Nazarbayeva, began dominating the national TV sphere from the end of the 1990s onwards (Cummings 2005: 27). At the same time, journalists brave enough to report on politicians' misbehaviours “were subject to official and unofficial harassment” (Olcott 2005: 36).

This was the context for the Mass Media Law introduction in 1999. Initially, there was no reference to the internet in the document[122]. Only two years later, in May 2001, new amendments were passed, adding and defining websites as a means of mass media. Notably, the turning point occurred in July 2009, when according to Amendments to Acts on Information and Communication Networks, all internet resources including websites, chats, and blogs were equated to the mass media with the appropriate liability of traditional media (Zakon 2009). (At the time, internet proliferation in Kazakhstan reached only 18.2%.) New amendments gave the Kazakh authorities the right to treat ordinary internet users blogging and posting on social media in the same manner as professional journalists. Similarly, website hosts became liable for the content on their resources to the same extent as media outlets. Several years later, in July 2016, the Ministry of Information and Communication clarified that not all internet resources but those that voluntarily registered as online media are considered the mass media (Letter of the Ministry of Information and Communication 2016). By that time, however, the regulation of the internet was already tightened. Thus, this clarification did not suffice to loosen existed extensive control of digital information.

In addition, the Mass Media Law stipulates that media outlets must assist counterterrorism state agencies. The law also specifies that divulgation of state secrets, propaganda and justification of extremism and terrorism, the disclosure of information about techniques and tactics of ongoing anti-terrorist operations, and propaganda of drugs, cruelty, violence and pornography are prohibited. This article is crucial as the

[122] At the time, the mass media, according to the law, referred to the periodically printed edition, radio- and TV-program, documentary filmmaking, audio-visual record, and another form of periodic or continuous public distribution of the mass media.

pretext for fighting terrorism and extremism has been widely used to filter and censor online content as well as to arrest internet users (discussed below).

Furthermore, according to the law, all mass media outlets must be registered with the Ministry; the registration of internet resources (websites) as online media was declared voluntary, though, as mentioned above, somewhat late. The requirement for the registration is crucial as it gives the government (the Ministry of Information and Communication) necessary control over Kazakhstan's media outlets and their websites. By threatening to cancel their registration and thus affecting their survival, the Ministry has acquired a necessary tool to put pressure on media outlets and the stories they distribute in Kazakhstan. Given the extractive nature of political institutions, control over the media was vital for the first President as a lack thereof could shake the foundations of the balance of power. On the other hand, the manipulated media (under pressure) can advance pro-government narratives necessary to justify (authoritarian) domestic policies, refraining from subjecting the government to accountability.

Even moving a website abroad would not help a defiant media outlet as, according to the law, if the Ministry has revealed that the information and communication infrastructure of online media is located outside of Kazakhstan, then a registration certificate is recognised as void. Consequently, Kazakh media without the registration cannot freely work in Kazakhstan. If this is insufficient to suppress a disobedient target, the Ministry of Information can also affect media outlets by stopping the circulation of their products (e.g. magazines) and/or blocking their websites, given a vague definition and application of termination causes. The mass media (in line with the law) can be, and actually have arbitrarily been, terminated ostensibly for propaganda and agitation of war, violent change of the constitutional order, violation of the integrity of Kazakhstan, and undermining of state security; for propaganda of extremism and terrorism; for the publication and distribution of information inciting interethnic and interfaith hostility.

Another important document, laying down the foundation for governmental control, is a Law on Communication (2004) passed in July 2004. The law gives state agencies extra powers to further tighten up the regulation of the internet and functions to control and monitor communications of people. Communication operators (providers) and/or owners of communication networks (ISPs) operating in Kazakhstan, according to the law, must collect and store service information (the storage of information on subscribers is carried out only on the territory of Kazakhstan; the law prohibits the transfer of information outside of Kazakhstan). They also must provide the authorities conducting investigative and counter-intelligence operations (the police and the National Security Committee) with organisational and technical capabilities and with access to information on all communication networks[123]. State agencies have thus acquired access to citizens' data. The fact that "ISPs connect end-users to the Internet" and "able to provide the most direct and straightforward enforcement of legal rules on the Internet" (Kurbalija 2016: 40) explains why the Kazakh government has imposed strict requirements on internet providers.

Moreover, in line with the Communication Law, owners of cellular devices are obliged to register with a mobile operator; the latter is prohibited to provide communication services to an unregistered cellular device. Importantly, personal information must now be stored in databases located in the territory of Kazakhstan, as a Law on Personal Data (2013) requires, easing access for the Kazakh authorities. As a result, government agencies (e.g. security services), by having access to communication operators, have become able to identify the owner of a particular mobile phone and telephone number.

However, a turning point, which significantly eased state control over the dissemination of information, took place in April 2014. The President signed a Law on Amendments to Legislative Acts on the Activities of Internal Affairs Agencies (2014) that has endowed the General Prosecutor of Kazakhstan with the right to terminate the operation of communication networks without a court decision. Now, the General Prosecutor and his deputies can order the authorised body to temporarily suspend the operation of communication networks and internet access in case communications are used for criminal purposes. The spectre of reasons for the termination is broad, including purposes: (1) detrimental to the interests of the individual, society and state; and (2) to disseminate information that violates Kazakhstan's legislation on elections, contains calls for the extremist and terrorist activity, riots, and participation in mass (public) events (which are held in violation to the established procedure), and promotes sexual exploitation of minors and child pornography. In this context, the Communication Law requires telecommunication operators and/or the State Technical Service within three hours to suspend communication services and internet resources.

In urgent cases that may lead to the commitment of serious crimes, the Communication Law maintains that the head of the Security Committee (plus his deputies and heads of regional branches) also can shut down communication networks and internet access. All the Security Committee needs to do is to notify the Ministry of Information and the General Prosecutor's Office within twenty-four hours *after* the

[123] Besides, operators and providers must secure the functionality of telecommunication equipment for the technical conduction of investigative and counter-intelligence operations at their own expense (e.g. the SORM system). In addition, communication providers (operators) of all categories are required to maintain at their own expense the system of centralised management of its networks, which should be located on the territory of Kazakhstan.

shutdown. The Ministry and communication providers are legally responsible for the failure to comply with termination requests. In addition, the Law on National Security (2012), passed in January 2012, also provides the Security Committee with a right to terminate communication channels. During anti-terrorist operations and containment of riots, the committee can give orders to networks owners and communication operators to suspend or restrict the use of networks and communications.

In October 2018, the right of state agencies (the General Prosecutor's Office, the Security Committee, the Interior Ministry, and the Ministry of Defence) to interfere with networks was expanded (Decree of the Government of Kazakhstan 2018). Now, internet and mobile services can also be terminated at the time of social emergency (the term was not defined). Basically, by referring to all potential (small and large) protests as a social emergency, the government has accrued a right to cut off communications and restrict internet access (without a court order), depriving protesters of the possibility to coordinate forces, communicate, and exchange information. Consequently, as I discuss in the following sub-sections, communication networks were disrupted numerous times in Kazakhstan under the security pretext. However, the main objective of internet shutdowns was to stop the circulation (via messengers and social media) of negative information on the internet.

Another document regulating the internet is a Law on Informatization (2015) accepted in November 2015[124]. Despite the ambitious aims and a prevalent technical language[125], the law serves to strengthen control over digital information. For instance, according to 2017 amendments, the anonymous online commentary was banned (Zakon 2017). Now, internet users, in order to place any information on a website, should conclude an agreement with the website owner by providing their personal data. The user still can use a nickname to comment online but the website owner will store his/her real personal data. In other words, a person in case of criticising the government can be easily identified, further amplifying self-censorship in the country.

[124] The first law on informatization was passed in May 2003, losing legal force in January 2007. The second law on informatization was passed in January 2007, losing legal force in November 2015. On November 24, 2015, a new law was accepted. According to the law, informatization means the organisational, social-economic and scientific-technical process directed to the automatization of activity of informatization subjects.

[125] The law regulates public relations in the informatization sphere between state agencies, individuals, and legal entities. The aim of state regulation of informatization processes is to form and ensure the development of information and communication infrastructure. The formation and development of information society; improvement of digital literacy; development of "e-government"; monitoring of the provision of information security for state agencies, legal entities, and individuals; and prevention and reaction to incidents of information security are the aims of state management of informatization processes.

Thus, internet-related legislation serves the main goal: to give the Kazakh authorities levers to control communication networks and the distribution of information and to prosecute users if needed. Laws were designed to benefit and empower solely the government and its agencies, further cementing the President's political power, whereas a possibility to spread anti-governmental messages was diminished. The free flow of digital information was substantially constrained. Yet in addition, the government also tried to justify state's sweeping powers to control the internet.

3.1.2. Justifying concepts and programs

Internet-related legislation also attempts to justify state involvement in the digital domain. One of the justifying documents is the Concept of Information Security, which was accepted in 2006 and updated twice afterwards. Another is the Program of "Informational Kazakhstan" adopted in 2013 and transformed into "Digital Kazakhstan" in 2017. Such legislation endeavours to lay the grounds for the government's participation in (already strict) internet regulation, though presented in a somewhat vague and flawed manner. Below, I discuss how the Kazakh state through various concepts and programs justifies its growing role in the information space.

The first document, attempting to justify the increasing role to be played by the state, was the Concept of Information Security of Kazakhstan (2006) passed in October 2006. The concept maintained that the growing role of the internet leads to a necessity to protect people from violent and fake information. However, it did not provide any information about the internet's role and how the state aimed to protect its people from harmful information as well as how such information would be defined. The concept also argued that the state should play a bigger role in providing information security. Yet, there was no argumentation as to why the state's role should be expanded. Likewise, the concept simply listed the threats to information security without demonstrating how these threats were affecting the information space of Kazakhstan in practice. The concept lacked the supporting arguments and provided no links of mentioned threats with Kazakhstan. The document, thus, appeared to manipulate the common security threats in the world to justify state interference in the information space.

The 2006 Concept of Information Security provided foundations for state policy in information security until April 2011. In November 2011, the second Concept of Information Security up to 2016 (2011) was signed. Importantly, the second concept claimed that the global media and communication technologies have an extended impact on the social, political, and economic situation in different countries, implying but not naming the 2011 Arab Spring. Accordingly, the concept maintained that social media and blogs, which were popular in Kazakhstan, might be explicitly used to affect domestic politics at the expense of national interests of the state. Given that before the 2011 revolutions in the Middle East, the protests leading to regime change took place in the neighbouring post-Soviet countries, this reference to a potential threat of social media explains why the state strictly controls information on the internet. The Kazakh government was scared that social media can be used as a platform to organise and empower massive anti-governmental protests in Kazakhstan.

Interestingly, the concept also highlighted the problem of low quality and low-level competitiveness of domestic media content, which cannot compete with foreign counterparts. Ironically, the reason for such low quality of local content can be found in the state's heavy control and monitoring of media and the widespread culture of self-censorship (due to the extractive nature of political institutions). Thus, the government itself was responsible for the low competitiveness of domestic media that was now referred to as a threat to state information security.

Additionally, the concept in the concluding part listed ways to strengthen the level of information security of Kazakhstan. For instance, the document, among other policy recommendations, promised to introduce an optimal model of development and regulation of the Kazakh segment of the global internet and to develop mechanisms of encouragement to produce positive content. All these need to be done to expand the presence of Kazakh media in the Central Asian and international information space to promote a positive image of the country. The concept, however, failed to provide any further details of the model to regulate the Kazakh internet.

Meanwhile, equally important is the absence of results on the achievement of goals outlined in both aforementioned documents, vividly demonstrating the real attitude of government bureaucrats and officials to the formation of state doctrines and concepts. For example, the 2011 concept (as well as the previous one) emphasised the significant lack of both IT specialists in the country and information technologies developed in Kazakhstan. Thus, the concept promised to achieve the production of Kazakhstan-made computer equipment and software by 2016. However, none was achieved (the same problems and goals were again repeated in the following concept). Information security doctrines were written not to achieve its goals but to justify state interference in the digital domain.

In June 2017, the Concept of Cybersecurity called the "Cybershield of Kazakhstan" (2017), replacing the 2011 concept, was adopted. This time "information" in the title was substituted by "cyber", and a newly established Ministry of Defense and Aerospace Industry has become responsible for the concept's implementation. Despite the rebranding of the concept and change of the organisation in charge, problems of information security remained the same. (Though, political institutions under the command of the first President also remained the same.) Problems like the insufficient number of qualified specialists in the IT-sphere, the absence of local technologies and software, and low digital literacy and culture were highlighted in the 2006 concept, and later again in 2011 and 2017. Despite being aware of them and setting ambitious goals in the first two concepts (2006 and 2011), these problems were not addressed and tackled. The current concept repeats the same problems, hoping to handle them within the next five years. At the same time, the 2017 concept, like the previous documents, continues to set ambitious goals. One of them is, for example, to extend the share of local software in informatization and communication spheres used in the state and quasi-state sectors by 50% in 2022.

Besides, the concept, claiming that the chaotic character of the existing system of global internet governance has led to both the militarisation of the ICT sphere by some countries (no reference to particular states) and the attribution problem, signals the authors' lack of understanding of how the internet works. Contrary to their assumption, the current system of global internet governance is relatively structured and organised, representing several international organisations. Each of them is assigned with particular functions (for example, the management of the domain system), being responsible for managing the internet on a global scale. Thus, the governance system, though still lacking a supranational body, is not chaotic. Another contradiction is that the concept, referring to the fast development of informatization processes of society and the state, claims that Kazakhstan has preconditions to build information society, though also referring to the low level of information culture in the country.

In addition to security concepts, in January 2013, the President approved the Program of 2020 Informational Kazakhstan (2013). The program aimed to create conditions for the transition to the information society. The objectives were to provide accessibility to the information and communication infrastructure; to create an information environment for the social, economic, and cultural development of society; and to develop a national information space. The first stage of the program (2013-2017) sought to create a new architecture of government agencies, to begin the gradual introduction of both ICTs into all spheres of economy and training/retraining of IT specialists, and to improve media legislation and modernise the national media. As can be seen, the program's objectives were ambitious but too broad. For example, the aim to train a new cohort of professionals in the IT-sphere was not novel and repeated the tone of information security concepts. Also, it is unclear what the development of national information space and modernisation of national media meant, given that by 2013 both the internet space and media were under the close supervision of the state. In short, the document, despite its impressive goals, did not contribute to relaxing internet control in the country.

After four years, in 2017, the ambitious program was transformed into another one. Basically, a new document called the Program of Digital Kazakhstan (2017) was simply rephrased, while the deadlines to successfully complete the program were conveniently extended under the new title. The aims of the program have become to boost the development of the Kazakh economy and improve the wellbeing of citizens by using digital technologies. According to the program, all population, businesses, and government agencies of Kazakhstan would become beneficiaries as the program covers all spheres of life and seeks to increase the life quality of every citizen of the country. All these aims appeared to be mere words as the program of digitalisation (and the cybersecurity concept) serves another, more important and more subtle, reason. It justifies the interference of the state in internet regulation.

The Digital Kazakhstan program asserts that the expansion of internet access may become more attractive for network operators as the big data technology develops. The program states that data collection and analysis of internet users will secure a better understanding of users' preferences and capabilities, market dynamics, subscriber's life cycle, and influence of external conditions. However, the authors do not clarify why this information about users should be known. Nevertheless, the program claims that the coordination, combination, and unified direction of efforts in the development of big data technology are vitally important for the state. Therefore, the state, according to the logic of authors, holding the largest data on both individuals and the corporate sector should play a key role in the big data development. Yet, the authors do not provide any evidence supporting the statement and explaining why the role of the state is important and mention nothing about the users' privacy and its protection.

All in all, internet-related legislation, by providing legal means and justifying expanding state powers in the regulation of the digital domain, has significantly empowered state agencies.

3.2. Empowered state agencies

Given the extractive nature of domestic institutions, it was not difficult to design and adopt legislation that empowered government agencies to a great extent. The latter, as a result, play a crucial role in the regulation and control of (online) media, the internet, and digital infrastructure. Meanwhile, private companies (such as internet providers and communication operators) are insignificant actors as they are bound by harsh legislation and merely follow the government's commands. The largest internet service provider

(Kazakhtelecom) is state-owned (52% of shares)[126]. The only Internet Exchange Point (IXP)[127], opened in Kazakhstan in 2007, is also controlled by the state. Governments need to have IXPs on their territory as its absence means that a large portion of internet traffic between customers would be directed through another state, which gives rise to the service cost (Kurbalija 2016: 178). This also can diminish the state's capacity to control information distributed over the internet.

Overall, two government agencies[128], the Ministry of Information and Communication and the National Security Committee, are largely involved in regulating and managing the internet and associated spheres such as ICTs, communication networks, and online media in Kazakhstan. The Information Ministry runs the day-to-day governance of spheres related to information, communication, and mass media[129]. The Ministry carries out the state regulation and control of communications, develops and passes laws and regulations, licenses activities in the sphere of communication, and maintains the register of national resources and communication providers. The Ministry is also responsible for the coordination of laws and regulations related to the provision of national security and works with the Security Committee to coordinate the activity of communication providers on the issues of national security (Law on Informatization 2015). In addition, the agency forms and implements the state policy in the sphere of mass media, registers mass media outlets (including the foreign ones), oversees compliance with the Law on Mass Media, and monitors the mass media. In other words, the Ministry has a wide range of authorities, significantly affecting the extent of internet control in the country[130].

Moreover, the Information Ministry uses special software to effectively monitor online content (Decree of the Minister of Information 2019). Although it was made public that the Ministry planned to use the automated system to monitor the mass media (the minister commented that the system was needed not to control but only to monitor the

[126] The company controls 85% of the broadband internet market; the remaining 15% is controlled by Beeline (VimpelCom) and other minor providers (Freedom House Kazakhstan 2016).

[127] IXP is a physical object "through which different ISPs exchange Internet traffic through peering (without paying)" (Kurbalija 2016: 178).

[128] Another state actor is the Ministry of Defense and Aerospace Industry, which is responsible for the formation and realisation of information- and cyber-security.

[129] Various institutions within the Ministry of Information are also involved in information and communication regulation. According to the Law on Informatization (2015), the Committee on Telecommunications is in charge of the implementation of state policy in the sphere of informatization. The National Development Institute in the Sphere of ICTs (the National IC holding "Zerde") was formed by the Kazakh government to increase the competitiveness of the sphere of ICTs, stimulate industrial and innovation activities in ICTs. The Institute provides analytics and consultations in the ICT sphere and analyses the development of ICTs.

[130] Most importantly, the Ministry was headed from 2016 to 2020 by Dauren Abayev, a loyal follower of the first President. Abayev was the President's press secretary for five years, before heading the Ministry in 2016. Currently, he is a deputy head of the President's Administration.

media (Today 2018)), any details about the system remain unknown[131]. However, given the acutely extractive nature of political institutions and numerous cases of online censorship (discussed below), it is no exaggeration to suggest that the system helps the government strengthen control over information circulated in cyberspace. Thus, the agency, in addition to harsh legislation, is also empowered by the technical equipment – all with the aim to timely and effectively shape and limit the dissemination of digital information within national borders.

The second important state actor that controls the internet is the National Security Committee[132] (KNB) and its agencies, subordinated and accountable to the President of Kazakhstan, according to the Law on National Security (2012). (The Committee also provides government communications[133].) Specifically, the Committee's State Technical Service is in charge of technical maintenance of the centralised management system of Kazakhstan telecommunication networks. The Technical Service is also responsible for the organisation and maintenance of internet traffic points of intercity and international communication providers and the connection of providers' network to the internet traffic exchange point (Law on Communication 2004). These activities, justified by state monopoly over information security, give the Technical Service direct access to internet entry points[134]. In essence, the Security Committee controls the main communication channels in the country.

Besides, in October 2016, the Parliament discussed amendments to counter-terrorism and extremism laws that would endow investigative agencies with extensive powers to block networks and means of communication, including the internet, mobile connection, social networks, and messengers, by notifying the General Prosecutor's Office within one day (Nurmakov 2016). Amendments were adopted two months later (Law on Amendments to Legislative Acts on Issues of Countering Extremism and Terrorism 2016). Now, the National Security Committee can terminate the operation of communication networks and restrict internet access in extreme cases that can lead to

[131] In 2014, Freedom House (2014) argued that three more Kazakh agencies (the Administration of the President, the General Prosecutor's Office, and the Security Committee) were going to employ various systems to monitor information online. Until 2019, the launch of the system was postponed a few times (Mamyshev 2019); before, the monitoring of mass media was done manually (Dubovaya 2018).

[132] The head of the Security Committee since 2016 has been Karim Masimov, a political "heavyweight" loyal to the first President, who previously was the prime minister of Kazakhstan between 2007 and 2012 and from 2014 to 2016.

[133] The State Security Service provides presidential communications.

[134] The Technical Service also conducts the examination of information system, information and communication platform "e-government", and internet-resources of government agencies on their compliance with information security requirements, in accordance with the Law on Informatization (2015). It carries out activities to ensure security of telecommunications connected to the internet through the single gateway for internet access.

serious crimes without a court order. In this context, it is unsurprising that Kazakhstan has been referring to issues of national security and political stability as a pretext to intervene in internet regulation and to "justify expansion of surveillance and censorship practices" (Privacy International 2014: 23).

Likewise, in May 2018, the rules for the registration of mobile phones of subscribers were issued, requiring all mobile phones working in cellular networks of Kazakhstan to be registered by January 1, 2019 (Decree of the Acting Minister of Information 2018). To register, an owner of the mobile phone must provide a mobile operator with the individual identification number (IIN), the ID code of mobile phone, and telephone number used in the mobile phone. Unregistered mobile phones were disconnected starting from 2019 (Burdin 2018). Hence, given that state agencies already had leverage over communication operators, new amendments have further empowered the Security Committee, easing surveillance of communications. Meanwhile, the privacy and rights of internet users have been significantly limited.

As I demonstrate below, having been empowered by Orwellian-like legislation, Kazakh state agencies unleashed all their powers on online media, internet resources, communication networks and digital users.

3.3. Systematic censorship of online content and internet shutdowns

Nazarbayev's regime, used to commanding both the legislative and executive branches and having no political opposition, was cautious about digital technologies and new media from the very beginning. Given the state's suspicious and intolerant stance, the internet as a potential democratising source has come under strict supervision. Consequently, anti-government and critical digital content that could undermine the legitimacy of those in power has been targeted and censored. Numerous independent and opposition websites and online media, critical of high-office politicians and state policies, have been blocked.

Notably, censorship of politically sensitive digital information began as early as internet use began slowly growing in Kazakhstan. For instance, in 2000, when less than 1% of citizens had internet access, the opposition website (www.eurasia.org.ru) that published about a corruption scandal, involving the President, was blocked (Human Rights Watch 2004: 11). In another incident in 2003, when only 2% of Kazakh citizens had access to the internet, the online news outlet (Navigator) was heavily fined for the critical publication about the Nazarbayev's family (McGlinchey and Johnson 2007: 284).

Nevertheless, despite a low number of internet users in the country, incidents of restricting access to undesirable content persisted. In 2005, the Kazakh authorities, infuriated by a British comedian's portrayal of Kazakhstan, blocked his website (borat.kz)

(Radio Free Europe 2005). Also, in 2005, the coverage of Kyrgyzstan's Tulip Revolution and Uzbekistan's Andijan unrest on the internet (as well as on TV) was limited in Kazakhstan (Mcglinchey and Johnson 2007: 284). Given that both the revolution and unrest in the neighbouring countries were evidently anti-government, shaking the grounds under the Central Asian autocrats, the Kazakh government restricted information about both events that could instigate collective action in Kazakhstan.

In the following years, censorship only intensified. In 2007, four popular opposition websites were blocked for publishing allegedly incriminating evidence related to the feud between the first President and his son-in-law Rakhat Aliyev (Bolshakov and Solovyov 2007). To implement the blockage, the Information Agency invoked the requirement for Kazakh media outlets to host websites in Kazakhstan. Otherwise, as discussed in sub-section 3.1.1., the registration certificate would become invalid and the media, as well as its website, would not be able to operate in Kazakhstan. State agencies, shielded by harsh legislation, began "legitimately" restricting access to internet resources deemed critical of the government. Similarly, at the time, Deibert et al (2010: 188) revealed that the Kazakh government via internet providers was blocking "opposition groups' Web sites, regional media sites that carry political content, and selected social networking sites".

In addition to domestic media resources, the authorities also targeted foreign ones. For instance, in 2008, a popular Russian blogging platform, Livejournal, was blocked in Kazakhstan (Bushuyev 2009). Although the Kazakh government gave no explanation, the blockage was related to Aliyev's critical materials posted on the website. Livejournal eventually deleted Aliyev's account and was unblocked in 2010, yet the following year, under the extremism pretext, was blocked again (Nurmakov 2015). Importantly, because of anti-government posts from one account, access to the whole website was restricted. Likewise, in 2011, due to the two ostensibly extremist posts, the wholesale blocking of another popular blogging platform (Wordpress) was implemented (Glushkova 2011).

In other words, information censorship in the 2000s in Kazakhstan was evident. Despite the low internet penetration rate, the Kazakh government seriously considered politically sensitive digital content and widely restricted access to opposition materials. In the 2010s, censorship of online content different from the state discourse continued. For instance, in 2010, access to websites of the independent media outlet (Republic) was restricted (Yakubov 2010). To have legal means and justifications, in 2012, an Almaty court declared Republic extremist and outlawed its activity in Kazakhstan. Overall, eight newspapers and twenty-three websites under the Republic umbrella were banned (Toguzbayev 2012). The accusation of opposition media and political parties (movements) of extremism and their consequent ban would soon become a normal practice in Kazakhstan.

In 2014, another independent media (ratel.kz) that regularly published critical materials and investigations of corruption scandals was blocked without any explanations (and court decision) (Forbes Kazakhstan 2015). The same year, a Russian website (meduza.io) was also blocked in Kazakhstan due to publishing material about local separatists (Kichanova 2014). Similarly, in 2014, online petitions platform (avaaz.org) was blocked after a petition about the Kazakh President’s and government’s resignation was launched (Radio Azattyq 2014). In 2016, access to another website (change.org) in which a resignation petition of the Kazakh Prime Minister was initiated was also restricted (Mamashuly 2016a). It became evident that the Kazakhstan government was highly sensitive to critical information on the internet, immediately resorting to its blockage.

Many websites have been blocked for publishing anti-government content. As a result, owners of internet resources encountered numerous problems, including the shutdown of the website. Sometimes the authorities provided no explanation for the internet blockage, referring to technical issues instead: for instance, when the website of Foreign Policy was blocked in 2017 (Kulshmanov 2017). In other instances, the main pretext for restricting access to materials on the internet was the accusation of extremism as examples above demonstrate. Anxiously, the number of blocked internet resources ostensibly containing extremist materials has exponentially grown.

If only 125 reportedly extremist websites were blocked in 2011 (Kosenov 2011a), the number of blocked websites increased to 596 in 2013 (Kazinform 2014). In 2015, according to the General Prosecutor of Kazakhstan, 700 out of 100 000 checked websites were found illegal largely because of terrorist and extremist content and were consequently blocked (Kosenov 2015). However, the number reached thousands soon. In 2017, the Minister of Information reported that 9 000 websites, propagandising terrorism, extremism, violence, and suicide, were blocked and 230 000 similar materials were removed (Selezneva 2018). Of note, the politically motivated blockage of Livejournal in 2011, Republic (twenty-three websites) in 2012, and Meduza in 2014 – these are just a few prominent examples – fell under the extremism category. In that way, numerous websites that disseminated critical and anti-government materials have been effectively blocked in Kazakhstan.

Despite the systematic filtering of information on the internet and restrictive legislation, mainstream websites such as Facebook, Google, YouTube, Twitter, Wikipedia, and other popular sources are currently available in Kazakhstan. Nevertheless, the government attempts to remove online content on these websites as well, albeit unsuccessfully. According to the Google Transparency Report (n/d), Kazakhstan sent 277 requests to remove more than 280 000 named items from Google products and services over the period between December 2011 and December 2019. The number of requests significantly increased in the last few years: 264 requests were made since July 2015. The vast majority of these requests was related to national security reasons (202 requests) and only 21% of all requests by the Kazakh government led to eventual removal from Google. In accordance with Twitter Transparency (2020), between July 2014 and December 2019, Kazakhstan made twelve removal requests, including thirty-four reported accounts to be withheld. However, none of the content was removed by Twitter. Likewise, Kazakh state agencies requested information about Facebook users ten times between January 2013 and December 2019 (Facebook Transparency 2020). Facebook complied with none of the requests.

The Kazakh government, unable to directly influence foreign social media platforms to remove undesirable content, has been systematically resorting to internet disruptions. The shutdown of internet and mobile access, including messengers and social media, happens either selectively in one of the regions or the whole country, depending on the government's objectives. When the Kazakh leadership wants to isolate only one region or city from the rest of the country, in particular during some politically explosive events such as protests or unrest, then all communication networks in the region in question are cut off. When the Kazakh authorities want to prevent all citizens from accessing anti-government content, for instance, during online streams of dissidents, then the internet in the whole country is thwarted or simply stops to function.

Access to the internet was disrupted or considerably slowed down before, during, and/or after politically explosive events such as the unrest in Zhanaozen in December 2011, currency devaluation in February 2014, ethnic clashes in South Kazakhstan in February 2015, protests against the land code reforms in May 2016, the terrorist attack in Aktobe in June 2016, and post-election protests in May 2019. The Kazakh government, aware of the internet's ability to quickly share information and spread rumours and keeping in mind several regime changes in neighbouring states, actively attempts to prevent the dissemination of information in cyberspace by participants and witnesses of events. Hence, it systematically employs information controls within the country.

In addition, internet access is disrupted at the time of online streams of Mukhtar Ablyazov, an oppositionist in exile and vocal critic of the first President, on social media platforms. One of the numerous shutdowns took place on 16 December 2016 – the 25th anniversary of national independence – when several social media and Kazakh websites were blocked (Webb 2016). Although Ablyazov was interviewed online in Paris on that day, the Minister of Information and Communication denied any implications and connections with the interview and referred to (coincidental) technical errors on websites (Forbes Kazakhstan 2016). Nevertheless, at least two motives point out to state interference with the internet. The first is the obvious desire to restrict access to Ablyazov's interview, who deliberately and vocally criticises Nazarbayev's regime and whom the Kazakh government tries to extradite from France to Kazakhstan for the conviction of large-scale financial crimes. Second, given that at the time five years passed since the tragic events in Zhanaozen[135], the government apparently wanted to avoid the event's replay. Hence, social media as a tool of communication and navigation of potential protests and as a channel to distribute oppositional information was blocked.

Notably, the Kazakh government has not stopped fighting back all attempts of Ablyazov to undermine the legitimacy of current political leaders. In March 2018, a court ruled the Democratic Choice of Kazakhstan (DVK), an opposition political party led by Ablyazov, to be extremist and, thus, to be banned (Radio Free Europe 2018a). In November 2018, Ablyazov, already sentenced to twenty years, was also given life imprisonment by a Kazakh court (Radio Free Europe 2018b). Due to his current residence in France, Ablyazov was given a sentence in absentia. As can be seen, the accusation of extremism was again applied so that to silence opposition voices.

From the government's point of view, all those politically tense incidents, including dissidents' online appeals, are hazardous for its political survival as can instigate anti-government sentiments and demonstrations and possibly lead to regime change. The remaining post-Soviet autocrats are aware of numerous revolutions that took place in the neighbour-states and the Middle East, and of the (perceived) role that digital technologies played in facilitating and empowering street protests. Thus, in order to prevent explosive events to spill over from one region to another within the country, the government resorts to the technical isolation of "hot" spots by disrupting communications[136]. However, if it does not suffice, the Kazakh state has other tactics of internet control in its arsenal.

[135] In December 2011 in Zhanaozen, street demonstrations of oil workers turned into the unrest. As a result of police intervention, sixteen people died and hundreds more were injured.

[136] However, if needed, harsh intervention also can follow. For instance, dozens of people died and hundreds were injured (Kosenov 2011b) after the police arrived to pacify protesters (communication services were switched off as well) during the 2011 Zhanaozen riots. Meanwhile, media outlets covering the incidents run the risk to be shut down. After the tragic events in Zhanaozen in December 2011, for instance, numerous independent media sources including online media were closed (Amnesty International 2017a).

3.4. Communications surveillance and manipulation of public opinion

In addition to systematic censorship of online content and frequent internet shutdowns, the Kazakh authorities are also capable of intercepting communication networks via Russian-like Systems for Operative Investigative Activities (SORM). Russia introduced SORM in the middle of the 1990s, enabling the Federal Security Service (FSB) to access telecommunication networks; at the end of the 1990s, SORM-2 to police internet traffic was further adopted (Deibert et al 2010: 218). In 2014, the Russian government introduced SORM-3 to intercept, access, and store communications within the country (Privacy International 2014). Under SORM, all internet providers in Russia have to install the equipment, giving the security services access to activities and emails of internet users within national borders. In addition, ISPs are obliged to pass all information that they used to the FSB for the registration and storage (Valeriano and Maness 2015: 90). Thus, SORM was gradually upgraded, allowing extended surveillance of communication channels.

Kazakhstan implements surveillance methods similar to Russian practices. Internet providers in Kazakhstan are also required to record and store digital activities of users. Besides, the Security Service has straight and unrestrained "access to the population's phone and internet activity through the establishment of monitoring centres" in Astana and Almaty, the two biggest Kazakh cities (Privacy International 2014: 71). In addition, communication operators and internet providers, according to the Law on Communication (2004) and Law on Personal Data (2013), have to collect and store information about users, give investigative agencies (including the Security Committee) access to information, and buy and install the equipment (SORM, for instance) at their own expense. They also must store personal data in databases located in Kazakhstan.

Moreover, according to the Citizen Lab, Kazakhstan along with another twenty countries are suspected of having sophisticated spyware, the Remote Control System (RCS). This software enables surveillance over "hundreds of thousands of targets", remaining "untraceable" to an initiator, according to the manufacturer, Milan-based Hacking Team (Marczak et al 2014). Freedom House Kazakhstan (2017), referring to the WikiLeaks publication in July 2015, argued that "the government might have obtained software [from Hacking team] to monitor and interfere with online traffic, including encrypted communications, as well as to perform targeted attacks against certain users and devices". Consequently, the Kazakh government in at least one case is believed to employ spy software targeted against Kazakh dissidents and representatives of exiled oppositionists (Galperin et al 2016).

Furthermore, in 2016, the Kazakh authorities introduced the controversial national security certificate, requiring all internet users to install it allegedly for the safe surfing of foreign websites and fighting the international terrorism and child pornography (Digital Report 2016). The Kazakh mass media and mobile operators began publishing information that the certificate is solely for the security reasons to protect Kazakh internet users from cybercrimes and from accessing illegal websites (e.g. Informburo 2016a, Kcell n/d). The introduction of the national certificate was, however, criticised as experts worried that the National Security Committee would simply extend already increasing surveillance capabilities under the security pretext (Baituova and Atoyanz-Larina 2016). The certificate was called "the certificate of hazard" (Nurmukhanbetov 2016) and compared to the Chinese Firewall (Vorotilov 2016).

Criticism that the certificate threatens the privacy of Kazakh citizens was not groundless as, in August 2019, Google Chrome blocked Kazakhstan's security certificate in order to protect its users (Whalley 2019). Similarly, Mozilla also blocked the certificate, characterising it as "not trusted …, and once installed, allow[ing] the government to decrypt and read anything a user types or posts, including intercepting their account information and passwords" (Mozilla 2019). In other words, the foreign tech-giants cared about the privacy of Kazakh users more than the government of Kazakhstan. In addition, Raman et al (2019) found that Kazakh agencies, with the help of the certificate, occasionally intercepted internet traffic within the country.

Eventually, although in July 2019 the Kazakh communication operators began sending messages to subscribers about the necessity to install the national security certificate on all mobile devices connected to the internet (Kursiv 2019), the consequent implementation of the certificate was postponed. In August 2019, the Security Committee reported that the testing of the certificate was successfully completed and that citizens can now delete it from personal devices (National Security Committee 2019). The reasons for the certificate's suspension were not provided, though there has been an implication that Kazakh agencies could not technically ensure the functioning of the certificate (Chernyavskiy 2019), given that users needed to install it manually since, as mentioned above, internet browsers did not trust and blocked the certificate.

Besides sweeping surveillance powers and attempts to access personal data, state agencies also resorted to social media manipulation to further advance government's political discourses. For instance, in the wake of the 2011 Zhanaozen events, bloggers were co-opted to convey the state's narrative. In particular, in December 2011, preceding strikes of Zhanaozen oilmen who demanded the salary's increase turned to the unrest with dozens of killed, injured, and arrested. As a result, the state of emergency was declared while external communication with the city was restricted (Lewis 2016: 6). Eventually, due to the isolation of the city and control over journalists' movements, rumours and speculations about the causes and consequences of the unrest moved to cyberspace while activists' alternative narratives were critical of the government (ibid, 6-7). As a countermeasure, the Kazakh government, in addition to censoring reports about the events, invited six popular bloggers to visit the city, who eventually helped to "undermine reports from opposition media, not only by providing alternative information, but also by helping maintain aspects of the state's discourse" (Lewis 2016: 13). Likewise, Freedom House (2013: 447) contends that the bloggers' interpretation was similar to the Kazakh authorities' position.

After that, the notion of the "state blogger" emerged in Kazakhstan, meaning that a blogger works for the state. In addition, State Secretary Marat Tazhin suggested creating a formal list of popular bloggers, which was quickly dubbed the "Tazhin's list" (Mukankyzy 2013), ostensibly to control alternative narratives distributed by bloggers on social media. Besides, in 2014, Almaty's mayor selectively invited to a restaurant a group of loyal bloggers, whereas three other bloggers were detained as a result of trying to access the meeting (Lillis 2014). This incident once again indicates that Kazakh bloggers are split between pro-governmental, who receive various perks from those in power, and independent, who are largely being arrested.

That the government attempts to influence public opinion via co-opted bloggers became more evident in 2015 when the Kazakhstan Alliance of Bloggers, created in 2014, offered to hold a referendum (like in 1995), instead of elections, to extend the first President's term until 2022 (Khabarov 2015). Moreover, the following year, the Alliance's head (Galym Baituk) publicly expressed the willingness to engage in state propaganda for money (Bekbasova 2016). Given that bloggers openly ask rewards from the state for their pro-government opinions, it is challenging to argue about the impartiality of the blogosphere in Kazakhstan.

In addition to paid-for bloggers, there have also emerged salaried commentators, like the Chinese "50-cent" internet army or Russian factory of trolls, collectively called Nurbots as they methodically leave positive posts under news on Nur-Otan (the dominant political party) and Nursultan Nazarbayev. The Kazakh internet army of Nurbots, reportedly located in a small village in the south of the country, produces resolutely pro-government messages from numerous fake accounts to divert attention from various politically tense events or to praise domestic policies and high-level officials (Kozhanova 2019, Bannikov and Li 2019). In other words, the information space in Kazakhstan is heavily populated by paid-for pro-government bloggers and commentators who relentlessly manipulate public narratives on the internet. The government, thus, exercises censorship through noise, shaping the digital flow of information.

3.5. Crackdown on internet users and online journalists

If harsh legislation, capabilities of communication surveillance, co-optation of bloggers, systematic censorship of online content, and regular internet shutdowns are in some way insufficient to stay in power, Nazarbayev's regime also can resort to physical pressure and persecute and prosecute those who express alternative views on the internet. In this regard, a crackdown on (anti-government) digital users and journalists serves "to ensure that those publishing online know that they are being watched and that the state is capable of shutting them down – or putting them in jail" (Palfrey 2010: 990). This tactic, creating a sense of fear and contributing to self-censorship, significantly shaped and limited the free flow of digital information in the country.

Numerous incidents of intimidation, fines, arrests, and/or imprisonments of internet users and online journalists methodically take place in Kazakhstan. The crackdown on the authors of reportedly anti-government and critical materials has begun almost as early as the blocking of websites. Already in July 2002, when on average less than two out of one hundred citizens were connected to the internet, a journalist (Sergey Duvanov) was prosecuted for online publications that were critical of the government and exposed corrupted politicians (Human Rights Watch 2004: 36-37). (As discussed above, in 2000, the website of opposition media was blocked for the same reason – publishing about the corruption scandal.) Moreover, in August 2002, Duvanov was beaten and stabbed next to his house, and in October 2002 was charged with the alleged rape of an underage girl (Human Rights Watch 2004: 37). In 2003, he was given a 3.5-year jail sentence (Reporters without Borders 2003a).

In other words, the Kazakh authorities sent an unambiguous signal that cyberspace is being watched and thus any critical publications will not be tolerated. Henceforth, intimidation of disobedient journalists, including those working for online news outlets, went on to be constant. That the Kazakh regime was (and is) intolerant toward independent journalists, systematically persecuting and prosecuting them, is also confirmed by the World Press Freedom Index (conducted by Reporters without Borders). The index evaluates "the degree of freedom available to journalists in 180 countries" (Reporters without Borders n/d). Kazakhstan has always been at the bottom of the ranking, among the countries with the worst press freedom, and the situation has not radically changed: the 119th position in 2005, the 162nd in 2010, the 160th in 2015, and the 157th in 2020 (Reporters without Borders 2005, 2010, 2015, 2020d). Put simply, journalism in Kazakhstan is heavily suppressed.

However, apart from (online) journalists, bloggers – if not co-opted – have also been punished for their online activities. One of the earliest crackdown incidents took place in the wake of the 2011 Zhanaozen riots. In particular, a popular blogger (Murat

Tungishbayev), who was posting videos about the Zhanaozen unrest on YouTube, was beaten by the police in front of journalists (Radio Azattyq 2011). Thereafter, the intimidation and punishment of bloggers became regular in Kazakhstan. In 2013, for instance, a blogger and journalist (Aleksandr Kharlamov) was detained for provoking religious hatred in his online publications (Toguzbayev 2013). (The article 174 of the Criminal Code of Kazakhstan (2014) entails from two to seven years in prison for inciting inter-ethnic and religious hatred; and up to twenty years if the crime is committed by a group, leading to grave consequences.) However, Reporters without Borders (2013b) attributed the arrest to Kharlamov's criticism of authorities, urging to drop charges against him.

In addition, regular internet users have also been arrested and imprisoned. For instance, in 2015, a woman, charged for inciting religious hatred (separatism) on Facebook, was sentenced to four years conditionally (Radio Azattyq 2015). This was only one of the numerous arrests and imprisonments of users in 2015 reportedly for inciting interethnic hatred and promoting extremism on social media (Trotsenko 2015). The suppression of internet freedom continued in the following year. In one out of the numerous incidents, two civil activists, Serikzhan Mambetalin and Yermek Narymbayev, were accordingly sentenced to one- and three-years freedom restriction for an ostensibly extremist post on social media (Mamashuly 2016b). Both men published a book's excerpt on Facebook that later an Almaty court considered insulting the dignity of the Kazakh nation.

Consequently, in the 2016 report on Kazakhstan, Freedom House concluded that the Kazakh authorities on the grounds of fighting extremism "continued to arrest and detain individuals for posting content on social media which is deemed to be threatening or critical of the ruling regime" (Freedom House Kazakhstan 2016). Of note, many independent and opposition websites were also blocked under the same (extremism) charges. Detainments and court convictions for internet activities under the extremism pretext would be common in years to come. Thus, in May 2016, at least thirty-four activists were arrested reportedly for posting on social media platforms calls to protest against the reform of land legislation (Amnesty International 2017a: 13). Some of them received lengthy jail terms, attracting considerable international attention and condemnation. Two bloggers, Max Bokayev and Talgat Ayan, were accused of inciting ethnic hatred and organising the unsanctioned demonstration via social media and sentenced to five years in prison (Informburo 2016b). Human Rights Watch (2016) regarded convictions of both activists as "a miscarriage of justice", asking for their unconditional release. Similarly, Amnesty International (2017b) named both men "prisoners of conscience", calling to immediately free them.

As can be seen, under the charges of promoting extremism and inciting religious hatred, numerous active internet users, disagreeing with state policies (such as amendments to the land code), were detained and sentenced to lengthy jail terms. In general, the accusation of extremism is widely used in Kazakhstan to silence the activists as examples above demonstrate. In addition, numerous media outlets, websites, and organisations were shut down reportedly for promoting extremism: for instance, the Republic media in 2012 and the DVK party in 2018, both in opposition to the government, were eventually outlawed. Overall, between 2015 and 2017, 205 individuals were convicted for spreading content that provokes hatred and propagandises terrorism (Moldabekov 2017). In the period between 2014 and 2018, 301 criminal cases were opened under the article 174 of the criminal code – "Inciting of social, national, tribal, racial, class, or religious hatred" (Adil Soz 2019).

Nothing changed in the following years. One of the latest incidents was the arrest of the Kazakh citizen in April 2020 for posting a video in which he criticised the first President (Veber 2020). According to the Criminal Code (2014), it is a criminal offence to insult the dignity of the first President that can lead up to three years in prison. In other words, the Kazakh authorities continued to "routinely arrest and prosecute individuals for posting critical commentary online" (Freedom House Kazakhstan 2019), sending a message to those criticising that they are being watched. Similarly, in the 2019 analysis of freedom of speech in Kazakhstan, Adil Soz (2020), the International Foundation for Protection of Freedom of Speech, concluded that the Kazakh state under the guise of fighting crimes spends great budget resources in order to establish total control over the information space; any critical opinions and information are suppressed, journalists and media outlets are prosecuted.

Thus, the state-implemented methodical crackdown on internet users – combined with restrictive legislation, empowered state agencies, sweeping surveillance capabilities, manipulation of public narratives, systematic censorship and blocking of online content, and regular internet shutdowns – has severely affected the dissemination of digital information in Kazakhstan.

4. CONCLUSION

In the previous chapter, I confirmed the proposition that the extractive nature of political institutions is conducive to considerable state control over the digital flow of information. In this chapter, I examined how and to what extent extractive institutional settings affect the dissemination of digital information, drawing evidence from Kazakhstan. The main argument was that when the internet began penetrating Kazakhstan in the 2000s, the nature of domestic political institutions had already been acutely extractive. Nursultan

Nazarbayev, the first President from 1991 to 2019, amending the rules of the political game, accumulated a considerable range of authority, extended the presidential mandate via unfair elections and staged referendums, and restricted political competition in the country. As a result, a large part of society was excluded from political life. Given the liberating potential of digital technologies, of which the first President was aware, the internet had no other options as to be controlled by the Kazakh state. The president's logic of political survival, in other words, played its role.

Yet, although Nazarbayev eventually structured political institutions according to his whims, at the beginning of the presidency (between 1991 and 1995) he had faced obstacles and resistance in the form of the defiant Parliament. Members of the legislature, intending to form the parliamentary political system, had their own political ambitions. Despite the defiance, the first President, unwilling to share political power with other actors, managed to diminish the role of Kazakhstan's Parliament in the decision-making process. This allowed Nazarbayev to substantially expand his executive authority during the long-lasting presidency and guarantee the prominent role in politics even in retirement. Consequently, after the main challenges to his authority were eliminated, Nazarbayev went on to become the undisputed and ultimate source of political power in Kazakhstan.

This turning point (of crushing the legislative body) was crucial for internet control as in the 2000s when the internet was slowly entering the country, the introduction of restrictive legislation of media, information, and communications faced no resistance from the Parliament. By the end of the 1990s, the legislature was already in the President's pocket and legislative initiatives were easily advanced and approved. Given this, internet-related laws and rules served the only purpose: to expand state capabilities and rights to control information and to justify such substantial involvement in the digital domain. As a result, the legislative framework severely reduced the possibility of mounting alternative opinions and empowered state agencies to substantially influence political narratives in the country. The Ministry of Information, for instance, was rendered with the authority to strictly regulate domestic media outlets and their websites, whereas the National Security Committee obtained sweeping powers in the communication sphere. Now, the agency can shut down the internet and mobile access without a court decision. The Kazakh authorities, fully loyal to the first President and shielded by legislation, has affected the digital flow of information within national borders to a great extent.

In particular, online content critical of the government and high-level officials (especially of the President) has been methodically targeted. Anti-state (that is, anti-Nazarbayev) materials – with the help of adopted harsh legislation – were (and still are) censored ostensibly under the security pretext. Meanwhile, access to independent and opposition websites has been continuously restricted within the country. In addition, at the time of politically sensitive and explosive incidents such as protests, demonstrations, or merely online streams of popular dissidents, internet and mobile services are disrupted in either one of the regions or the whole country – depending on the event's scale.

Nazarbayev's regime, in other words, did everything possible to fence off the population from criticism of the government and its policies. For that reason, numerous bloggers have been co-opted to subtly influence public perception of events happening in Kazakhstan and the world. The government has also organised an internet army of Nurbots, paid-for commentators and trolls, who – along with state bloggers – bombard the Kazakh information space with pro-government messages. Another instrument in the government's hands is covert surveillance of communication networks. Due to installing the surveillance equipment in internet provider's facilities, the Security Committee, fully obedient to the first President, has acquired access to internet users' data. Sometimes, though, bald attempts of the government to spy on its citizens turned to be unsuccessful. For example, the implementation of state-controlled security certificate on all devices connected to the internet in 2016 faced widespread criticism and was later blocked by some techno-giants. The government had eventually to abandon the idea (at least temporarily).

Yet, if all these tactics of internet control are somehow insufficient, physical pressure on active internet users will follow suit. A large number of digital journalists, activists, and ordinary users – who happened to publish critical materials on the internet – was intimidated, attacked, and detained. Many of them were imprisoned, largely under the security grounds: convictions of inciting national or social hatred of regime's critics became a usual business. By penalising those who publish on the internet, the government sends a clear message that everything is watched and criticism of Nazarbayev's regime will not go unnoticed. The systematic crackdown on internet users and online journalists also contributes to self-censorship as many authors would carefully think before publishing anything anti-state.

On the other hand, given the acutely extractive nature of political institutions, such an approach of Kazakh authorities to the dissemination of digital information should not be surprising. Nursultan Nazarbayev was dispassionately and methodically getting rid of any threats to his reign. His position and political powers shall be ultimate and unconditional. Therefore, the defiant 12th and 13th Parliaments were the first victims of President's ambitions; numerous oppositionists, who happened to cross the President's path, fell prey to the undemocratic regime shortly afterwards. The internet, with its open networks and instant communications and exchange of information, was next on the line.

It is thus no coincidence that all these information controls have been employed from the very beginning of the internet's expansion in Kazakhstan. As the internet was slowly entering the country starting from the early 2000s, consequent blockings of websites and arrests of online publications' authors instantly followed. The authoritarian political system created by the first President could not expose itself to alternative and, more importantly, critical views. Only the government, that is Nazarbayev's regime, should control public narratives in the country, including on the internet. In this regard, after understanding the nature of the existed (and still existing) institutional setup, it becomes clear that internet control was the only way for Nazarbayev's regime to hold onto power. Otherwise, having a free internet and free dissemination of digital information, such an extractive nature would not last too long.

Undoubtedly, the internet in Kazakhstan was (and still is) considered a liability to the authoritarian regime. This is because digital technologies such as the internet and internet-connected mobile devices can empower a large segment of civil society, facilitating collective action such as protests and demonstrations. Due to the lack of electoral legitimacy (Frantz 2018), Nazarbayev-like small-coalition leaders operating within extractive institutions are especially sensitive to collective action, fearing people's masses in any form[137]. Moreover, Nazarbayev was perfectly aware of regime changes initiated by those masses in the neighbouring post-Soviet countries: Georgia in 2003, Ukraine in 2004 and 2014, Kyrgyzstan in 2005 and 2010, and Armenia in 2018. The 2011 Arab Spring was another indication not to trust open networks such as the internet. All in all, information distributed via digital technology, perceived as a threat to the political survival of Nazarbayev's regime, was destined to be controlled in a country with extractive political institutions.

[137] Autocrats have all reasons to fear the masses as almost 1/5 of all collapses of authoritarian regimes between 1946 and 2014 happened due to popular uprisings (Frantz 2018: 123).

CHAPTER 7. INCLUSIVE POLITICAL INSTITUTIONS AND INTERNET CONTROL: A CASE OF UKRAINE

1. INTRODUCTION

This chapter examines the interplay between political institutions and internet control in Ukraine. The nature of political institutions in Ukraine, largely due to the fragmentation of population and political elite along regional lines (west and south-east), has been inclusive since obtaining independence in 1991. Consequently, given the dispersed balance of domestic political power, the extent of state control over information on the internet was limited. No systematic censorship or blockage of online content was evident, arrests and intimidation of internet users and online journalists were rare, the legislative framework was liberal, and social media manipulation was not acute (Deibert et al 2010, Freedom House 2013, 2014). Such an order of things persisted while a political situation in the country was comparatively stable, that is, under control of those in power. However, once a serious political crisis that was hard to manage fell upon Ukraine, the number of employed tactics to control information online soared in an unprecedented manner. Despite the comparatively fair rules of the political game, the extent of internet control in Ukraine turned to be substantial.

Here lies the main difference with Kazakhstan (chapter 6) where the main condition of extensive internet control was the extractive nature of political institutions. As I argued in the previous chapter, the first President Nursultan Nazarbayev managed to accrue a wide range of political powers and, as a result, submitted the Parliament and government to his will. By the time the internet began penetrating Kazakhstan in the 2000s, the rules of the game were already amended and thus the online flow of information was eventually heavily censored and controlled. Nazarbayev's regime, having destroyed the opposition and indicating no signs to liberate politics in the country, perceived the internet as a potential democratiser that could challenge its rule. Therefore, information distributed over the internet had no other options but to be controlled.

In Ukraine, in contrast, the main condition of the extensive use of information controls was not political institutions, as institutional settings from 1991 to 2019 were inclusive, but the overt regional confrontation with Russia that began in 2014. In particular, in February 2014, Russia annexed Ukraine's Crimea and shortly after that Donetsk and Lugansk oblasts declared independence from Ukraine, resulting in a war in the east of the country between separatists and the Ukrainian army. As a result of political instability stemming from the 2014 conflict and the ensuing information war between Ukraine and Russia, the freedom of information in the country has noticeably deteriorated and internet control has been considerably strengthened. Both the

President and Parliament and their subordinate state agencies (such as the Security Service and the Ministry of Information Policy), under the pretext of containing Russia's aggression, have played a great role in the extension and implementation of information controls in Ukraine. In other words, the political crisis, in line with the findings (chapter 5), has become a critical juncture in internet control in a country with inclusive institutions.

In section 2, I first discuss the development of political institutions in Ukraine to demonstrate that their nature has been (and still is) inclusive throughout the whole period of independence obtained after the Soviet Union's collapse. Politics in Ukraine was characterised by constant power contests between the main political actors such as the President, Parliament, and government. Although some Presidents (for instance, Viktor Yanukovych) managed to amass more rights and authority at the expense of other political actors (the Parliament), their "success" was short-lived and the balance of political power was eventually redesigned to the existed status-quo. The Parliament in due course has become independent vis-à-vis the President, forming the cabinet of ministers, whereas the President's executive authority has been circumscribed. Civil society, too, has become vibrant and strong enough to affect political processes in the country. The orange revolution in 2004 (and Euromaidan in 2014) and following regime change showcases the potential strength of civil society. Under such conditions, the internet in Ukraine, which like in Kazakhstan began to slowly proliferate in the 2000s, was not controlled.

However, as I discuss in section 3, the liberal approach to digital information existed until 2014. After that, the number of tactics applied to control the dissemination of information on the internet increased. In particular, pro-Russian and thus anti-Ukrainian content has been censored. Accordingly, internet resources that ostensibly contain the anti-Ukrainian rhetoric were widely blocked, and internet users and online journalists were increasingly intimidated, arrested, and imprisoned for expressing political views online. In addition, reportedly pro-Russian media outlets were numerously raided by law enforcement agencies. Doctrines justifying the targeting of both materials and authors deemed to be sympathetic to Russia and separatists were passed, and laws to further extend state powers in the digital domain have been proposed. Besides, state agencies, receiving relative freedom under the guise of fighting the information war with Russia, negatively affected the extent of internet control. Finally, although manipulation of public opinion on social media was evident in Ukraine due to the 2019 presidential election, the focus on Russia was also significant.

In other words, as a result of the 2014 political crisis, internet control in Ukraine has become extensive. Consequently, I conclude that the ongoing conflict with Russia, serving as a justification, contributed to the increasing implementation of information controls in Ukraine. This conclusion validates the findings of the comparative analysis (chapter 5), illustrating how countries with inclusive institutions resort to control of digital information in the wake of political instability.

2. INCLUSIVE POLITICAL INSTITUTIONS

In this section, before proceeding to the discussion of Ukraine's political institutions in the post-Soviet period, I provide the background information on both domestic regional divisions, which contributed to political competition within the country, and the 2014 political crisis (sub-section 2.1.). I do not delve deep into specifics of the ongoing confrontation between Ukraine and Russia as the aim is not to evaluate the legitimacy of both states' actions but to demonstrate the implication and severe impact of the ensued crisis on the extent of internet control in Ukraine.

After providing the context, constant battles for power between the President, Parliament, and government that characterised the consequent development of political institutions in Ukraine are analysed (sub-section 2.2.). If in Kazakhstan the winner was apparent by the end of the 1990s, in Ukraine the political game is still on with regular conflicts and compromises between the main actors. As a result of such competitive political landscape, the nature of institutional settings in the country has become inclusive. However, despite the inclusive nature of political institutions, the extent of internet control changed in 2014 (section 3).

2.1. Background: Russia and Ukraine's regionalism

Russia has been playing a profound and determinative role in Ukraine. The latter has always been more important to Russia than any other neighbour-states as Ukraine's territory is strategically vital to Russia's security (Mearsheimer 2018: 176). In addition, both Slav countries share a common past that goes back to the 10th century Kievan Rus, making inter-state relations more intimate (Wilson 2015, Plokhy 2017). As a result, Ukraine despite having been subordinated to Moscow for many centuries[138] enjoyed a special, albeit symbolic, role: in 1922 Ukraine became one of the formal creators of the Soviet Union and in 1945 obtained a seat in the United Nations (Kazakhstan did not have such a privilege). It is also no coincidence that some high positions in the Soviet political hierarchy, including the general secretary, were occupied by Ukrainians or those with

[138] After a Ukrainian hetman Khmelnitsky pledged loyalty to a Muscovy tsar Aleksey in 1654, the Moscow Tsardom became the suzerain of the Ukrainian Hetmanate. In the 18th century, Ukraine became a part of the Russian empire and in 1922 a member state of the Soviet Union. However, Ukraine, unlike Kazakhstan, experienced a short period of statehood in the form of the Ukrainian People's Republic between 1917 and 1919.

close ties to Ukraine[139]. Most importantly, the historical development, which was entwined with Russia, and the in-between geographical location[140] contributed to regional divisions in Ukraine. This subsequently shaped the development of political institutions.

The diversity of Ukrainian regions takes roots in Ukraine's fate of being sandwiched between European and Russian powers. The longstanding geopolitical contestation between the two regional powers has become "a constituent element of Ukraine's historical DNA" (Sakwa 2016: 9). This is because the security and survival of Russia depend on who controls the borderlands, specifically who has the access to the Black Sea (Marshall 2016: 15). Hence, Russia has been frantically opposing the NATO eastward expansion as a potential military deployment of NATO in Ukraine and the Black Sea is of the immediate threat to Russia[141]. It was essential for the Russian political leaders to keep independent Ukraine aligned with Russia or at least make it neutral (a buffer zone). That is why Boris Yeltsin, within the Commonwealth of Independent States, and later Vladimir Putin, within the Eurasian Economic Union (EEU), were keen to integrate Ukraine with Russia economically and politically.

Europe, on the other hand, wanted to establish a "comfort zone" along its borders by making the neighbouring countries more west-orientated, simultaneously reducing the Russian influence in the region (Sakwa 2016: 39). That is why the European Union (EU) launched the European Neighbourhood Policy in 2004 and, following the eastward enlargement on the continent[142], the Eastern Partnership in 2008. Both projects have aimed to promote deeper cooperation between the EU and its neighbour-states, including Ukraine and other post-Soviet countries[143]. Additionally, at the NATO summit in April 2008, the formal acceptance of Ukraine (and Georgia) into the organisation was promised. France and Germany, however, realising that such a pledge would antagonise Russia, opposed the membership plan (Sakwa 2016: 9). Nevertheless, the West did not stop its efforts to extend the integration with the former Soviet republics. In 2012, the EU,

[139] For instance, the Politburo was dominated by Slavs (largely Russians but also Ukrainians). In addition, Leonid Brezhnev was born in Ukraine, Konstantin Chernenko was from a Ukrainian family, and Mikhail Gorbachev and his wife were half Ukrainians (Sakwa 2016: 22-23).

[140] Geographically, Ukraine is in Eastern Europe, a territory called the borderlands (Sakwa 2016) or bloodlands (Snyder 2011).

[141] The NATO expansion to the Eastern Europe significantly contributed to the Russia's resistance of EU policies toward Ukraine (and Georgia). "Colour revolutions" in the post-Soviet region, too, alienated Russia as "the Orange Revolution [in 2004] was seen by many as a potential model to oust Putin himself" (D'Anieri 2019: 16).

[142] In 2004 and 2007, a range of Central and Eastern European countries, including the former Soviet republics (Estonia, Latvia, and Lithuania) joined the EU.

[143] These countries are Armenia, Azerbaijan, Belarus, Georgia, and Moldova.

following the 2008 Russia-Georgian war, initiated the Association Agreement with Ukraine to be signed in November 2013[144].

Ukraine thus happened to be a hostage of its geographical location, being a borderland between Europe and Russia and forced to choose between the two poles: deeper integration with either the west (the EU) or the east (Russia and the EEU) (D'Anieri 2019: 24). Consequently, faced with a zero-sum option, the Ukrainian leaders sought to play off both powers against each other, taking advantage of the geopolitical contest (Sakwa 2016: 79). Even Viktor Yanukovych, who is often portrayed as a pro-Russian president, was merely a pragmatic politician toying with the integration with both the EU and Russia at the same time (Wilson 2015: 348, Marshall 2016: 15). However, such manoeuvring between the two major regional powers persisted until 2014, in the end resulting in regime change and Ukraine's full pivot to the west (at least politically and ideologically). The current Ukraine crisis – that would soon become the turning point in internet control – is, in other words, the manifestation of the "Europe vs Russia" contest over Ukraine, both pulling the country in its direction (Trenin 2014).

Crucially, as a consequence of the continuous geopolitical rivalry between Russia and Europe over the sphere of influence in the borderlands, entrenched and deep-rooted regional divisions emerged within Ukraine. The political culture in Ukraine has become heterogeneous given that the western territories of Ukraine had previously been ruled by the various European Kingdoms whereas the southern and eastern regions were continuously under control of the Russian Empire and then the Soviet Union[145] (Plokhy 2017). The religious composition in Ukraine is also different now: largely Catholic (Uniate) population in the west and Orthodox in the east (Borisov 2018: 111).

It is thus unsurprising that the current cleavages are particularly vivid between Ukraine's more Europe-orientated west and more Russia-orientated south-east, significantly contributing to, if not creating, political turbulence in the country[146]. Ukraine's

[144] Nevertheless, according to Sakwa (2016: 43), the EU integration project with Ukraine, although promising deeper economic, political, and security integration between Ukraine and the EU, appeared to have a few flaws. The economic help envisaged by the program was negligible, acceptance of Ukraine to the EU was uncertain (indeed, very dubious), and integration was crafted within already existing forms of cooperation (e.g. free trade zone between Russia and Ukraine) (ibid). The Agreement, in particular Yanukovych's announcement not to sign it after publicly endorsing the deal, would later trigger the street protests in Kiev.

[145] Western regions of Ukraine were joined to the Soviet Union at the end of the WWII in 1944-1945 and given to the jurisdiction of the Ukrainian SSR. Previously, for example, a region of Galicia belonged to Austro-Hungary till 1918 and to Poland after WWI until the German and Soviet invasion in 1939. Transcarpathia belonged to Hungary since the 10th century; in 1919 it was transferred to Czechoslovakia. (Crimea was given to Ukraine in 1954.)

[146] During the Soviet time, the political culture in the Ukrainian Republic was also disparate as the western part was more pro-European and dissident while the easterners were more conformist towards the Soviet rule (Borisov 2018: 111).

“population remained divided by ethnic, linguistic and religious differences and by the variety of historical experiences of regions in which they lived” (Wilson 2015: 160-161). Such diversity still persists, with the political elite, as a result, being considerably fragmented within the regional lines as people tended to vote by prioritising regional issues first. Thus, votes for presidential candidates in 1994, 1999, 2004, and 2010 were divided along regions: west and south-east appeared to support different front-runners. (In 1991, 2014, and 2019 winners managed to prevail by a landslide in most regions, though the regionalism was still present.)

Notably, the regional tensions in Ukraine subsequently contributed to the emergence of inclusive institutional settings. “[R]egional diversity was a challenge for leaders, but made it much more difficult for anyone to consolidate autocratic power” (D’Anieri 2019: 17). The balance of political power, due to the fragmentation of the political elite and population within regional lines, has been comparatively evenly dispersed. As I discuss in the following sub-section, although the main political actors continually competed with one another to change the rules of the game, their attempts were either unsuccessful or had the interim effect. Due to the inclusivity of political institutions, control of digital information was also limited – until 2014.

2.2. Development of political institutions: conflicts and compromises

As a result of entrenched regional divisions, the development of political institutions in post-Soviet Ukraine was characterised by the struggle for power between the President, Parliament, and government. If in Kazakhstan the contest for ultimate power ended by the mid-1990s when President Nazarbayev dissolved the legislature for the second time, in Ukraine the game between all main political actors to accrue more authority continues even now.

The contest for political power began shortly before the Soviet Union’s collapse when in July 1990 Ukraine’s Supreme Soviet (the legislature) adopted the Declaration of State Sovereignty of Ukraine (1990), paving a path for consequent independence[147]. A few months later, in October 1990, Ukraine’s Supreme Soviet accepted a Law on Amendments to the [1978] Constitution of the Ukrainian SSR (1990), excluding article 6 that stipulated the Communist Party of the Soviet Union as the key governing body and the core of the political system. Amendments significantly reduced formal powers and legitimacy of the Ukrainian Communist Party, increasing those of the Supreme Soviet.

[147] The Declaration entailed the supremacy of the Ukrainian legislation over the Soviet one, declared the lands and resources of the country to become the property of the Ukrainian people, and laid down the right of Ukraine to have armed forces.

Thus, at the time, in addition to the Communist Party[148], another powerhouse emerged: the Supreme Soviet headed by Leonid Kravchuk, a future first President of independent Ukraine.

In May 1991, Ukraine's Supreme Soviet, following the common trend in the Soviet Union, also decided to initiate a presidency in the country, though there was no full understanding nor agreement on what presidency model (strong or representative) to form (Borisov 2018: 114-117). In July 1991, a Law on the President and Amendments to the Constitution (1991) was passed. Nevertheless, the political system did not become fully presidential (like in Kazakhstan) as the position of the prime minister has remained and both the President and cabinet were subject to accountability before the legislature. In addition, the President had no presidential veto, no right to discharge the Parliament, and had to consult with the latter the choice of the prime minister and ministers, according to new amendments. Thus, the system was de-facto presidential-parliamentary.

After obtaining independence[149], conflicts and trade-offs between the President, Parliament and government characterised a consequent development of political institutions in Ukraine. Practices of brokering a deal to avoid or resolve a political stalemate would soon become institutionalised in Ukraine. One of the earliest examples of conflict between the President and Parliament[150] was the adoption of the constitution – designed to draw the lines between the sphere of influence of key political actors (what they can and cannot do) – that was hindered until the mid-1990s due to disagreements over its structure. In 1995, as a result of a compromise between Leonid Kuchma, the second President elected a year earlier, and Olexander Moroz, the head of the Parliament, the Constitutional Agreement (1995) was eventually signed.

The agreement expanded the President's political authority, making him the head of the state, executive branch, and government. The latter, although maintaining a prime-

[148] The Communist Party won the majority of seats in the 1990 and 1994 parliamentary elections: 331 and 86, accordingly.

[149] In August 1991, in the aftermath of unsuccessful coup in Moscow, the Act of State Independence of Ukraine was accepted while the Ukrainian Communist Party was banned (though restored in 1993). On 1 December 1991, both a referendum on the Independence Act and the direct presidential elections were held: 90.3% of voters supported the Act whereas Kravchuk, with 61.5% of votes, became the first President of independent Ukraine. Importantly, the first presidential elections in Ukraine (as many other that followed) were competitive (Borisov 2018: 176-177) – a significant difference from Kazakhstan.

[150] Another example is the 1993 Massandra summit, in which Russian and Ukrainian leaders gathered to discuss a number of (contentious) bilateral issues that surfaced in the aftermath of the Soviet Union breakup. As a result of the meeting, Leonid Kravchuk, under economic pressure from Russia, agreed to concessions giving up the nuclear weapons and the Black Sea fleet to Russia (D'Anieri 2019: 41-42). The Parliament, however, did not gain the needed majority to ratify the agreement, demonstrating the discord with President's decision and forcing him to abandon the deal (ibid). In other words, the legislature acted as an actor independent from the President's will. If in Kazakhstan the Parliament lost independence by the mid-1990s becoming the rubber-stamp body, in Ukraine the Parliament is a crucial and independent player up to date.

minister's position, became accountable to the President. The Parliament, in turn, accrued the right to dissolve the government through a vote of no confidence. In addition, the legislative body retained immunity from the President as the latter still had no constitutional right to dissolve the former. Thus, the constitutional agreement between the President and Parliament extended powers of both actors, setting a 1-year deadline for the acceptance of the constitution.

Following the agreement, in June 1996, the first and current Constitution of Ukraine (1996) was adopted, further reshaping the balance of domestic political power. This time the President obtained the right to dissolve the Parliament if plenary meetings did not start within 30 days of a plenary session, and to appoint and dismiss the heads of regional and local governments, facilitating Kiev's political control of regions. However, the Parliament retained much of political power as well: it now appoints the prime minister on the President's proposition. Furthermore, although the government becomes responsible before both the President and Parliament, it is accountable to and controlled solely by the Parliament. In other words, the accepted document was "a compromise text" as both the Parliament and President "got most of what ... [they] wanted" (Wilson 2015: 196).

In 2000, an attempt to reshape the balance of political power was made. Leonid Kuchma managed to initiate changes to the 1996 constitution to further expand the presidential authority and diminish parliamentary powers (Kommersant 2007). His proposed measures would have eased the President's power contest with the defiant Verkhovna Rada[151] (Parliament). Although constitutional amendments were endorsed by the national referendum, they, in line with the constitution, should have been approved by the legislature. The MPs, unsurprisingly, decided not to implement the referendum's results that would significantly reduce the Parliament's authority. In other words, new amendments to the constitution did not come into force.

Nevertheless, Leonid Kuchma, at the end of his second and final term, again attempted to redistribute political power, though this time from a different side. In 2003, willing to weaken a future occupier of the presidential palace, he issued a Presidential Order to Discuss Constitutional Amendments (2003) that would make the legislative body more powerful vis-à-vis a chief executive. The Parliament, though, again did not authorise these reforms of the political system. However, a law to change the electoral system from mixed to proportional that was considered in the Verkhovna Rada together

[151] Proposed amendments envisaged: the right of the president to dissolve the Parliament if it did not form a parliamentary majority within a month or did not approve the proposed budget within three months; the decrease in deputies' number from 450 to 300; the annulment of MPs' immunity from the prosecution; and the creation of the bicameral Parliament.

with constitutional amendments was approved (Law on Elections 2004), serving the Kuchma's goal. The measure weakened a future President as pro-presidential forces could no longer exploit single-mandate districts by the majoritarian electoral system, allowing opposition parties to be better represented in the Parliament[152].

In December 2004, amidst the mass protests sparked by the authorities' fraudulent attempts to steal the presidential elections (Kuchma's successor Viktor Yanukovych was staged to win), another compromise between the political opposition (Viktor Yushchenko) and those in power was achieved (Wilson 2015: 320). As a result of a trade-off between Yushchenko, Yanukovych, Kuchma, and Lytvyn (the head of the Parliament), in return to agreeing to rerun the second round of the presidential elections, earlier proposed amendments to the constitution were adopted (Law on Amendments to the Constitution 2004, D'Anieri 2019: 132). Thus, the Parliament accrued more powers whereas the President's authority was significantly circumscribed. In particular, the legislature was to fully control the government by acquiring the right to appoint and dismiss the members of the government, whereas the President was to propose (and nothing more) candidates to positions of the prime minister, minister of defence, and minister of foreign affairs[153]. Due to constitutional amendments and change of the electoral system, the President became exceptionally weak whereas Parliament was strong[154].

Consequently, given the established parliamentary-presidential political system in Ukraine since 2004, whereby the legislature played a crucial role in the political life of the country, it has become highly important for the President of the day to tame the Parliament. Thus, in 2011, taking advantage of having the majority (the Party of Regions and the Communist Party) in the Verkhovna Rada, then-President Yanukovych changed the electoral system back to mixed (Law on Elections 2011). This would allow him to limit

[152] If previously political parties supporting the incumbent gained additional seats via the majoritarian system, now they did not have such an option. Consequently, in the 2006 and 2007 (the 2006 legislature was dissolved) parliamentary elections the winner was the opposition Party of Regions that won 186 and 175 out of 450 seats, accordingly.

[153] Also, the President's right to dissolve the Parliament was extended by two additional conditions: if a coalition of parliamentary factions is not formed within a month and if a cabinet of ministers is not formed within 60 days after the dismissal of the government.

[154] Such an order of things – that is, a constant power struggle between the Parliament and President – continued to inevitably lead to numerous domestic political conflicts. In May 2007, following four orders of then President Yushchenko to dissolve the Parliament, the key political actors found themselves in a political stalemate. To resolve it, the legislature, President, and government had to reach yet another compromise. In the end, President Yushchenko, Prime Minister Yanukovych, and the head of the Parliament Moroz signed a Common Declaration (2007), all agreeing to hold the extraordinary parliamentary elections in September 2007. As a result, although the opposition Party of Regions again won the majority of seats (186) in the Verkhovna Rada, Tymoshenko's bloc that came second, taking 129 seats, eventually formed the coalition and thus the government.

the representation of political opposition in the legislature, especially given that the popularity of the pro-presidential Party of Regions was declining (Borisov 2018: 260). Furthermore, following Yanukovych's ascendance to the presidential office in 2010, the Constitutional Court annulled the 2004 law on constitutional amendments that had significantly restricted the authority of the chief executive (Wilson 2015: 344). Instead, Yanukovych restored the 1996 version of the constitution that guaranteed more powers to the President, changing the system from parliamentary-presidential to presidential-parliamentary. The rules of the game were again rewritten, now favouring the President. As can be seen, the battle for political power between the main political actors has been a constant feature of Ukrainian politics, each trying to amass more authority and influence at the expense of others.

Although Yanukovych managed to turn the scale in his favour, the effect was interim. In the wake of the mass street protests that began in November 2013 due to the refusal to sign the Association Agreement with the EU, Yanukovych, rapidly losing political support, had to agree to a number of concessions. In particular, on 21 February 2014, he signed with opposition forces the Agreement on the Settlement of the Crisis in Ukraine[155] (2014) (ministers of foreign affairs of France, Germany, and Poland, and a special representative of the Russian President brokered the deal). Nevertheless, Yanukovych left Kiev (and then Ukraine) shortly after endorsing the deal. The Verkhovna Rada immediately seized the opportunity: the next day it declared the extraordinary presidential elections to be held in May 2014, justifying the measure on the basis of the President's self-removal (Decree of the Verkhovna Rada 2014). The 2004 version of the constitution that granted more powers to the legislature was (as according to the agreement) restored (Law on the Restoration of Some Provisions of the Constitution 2014). Ukraine became, yet again, the parliamentary-presidential polity.

In August 2014, in the aftermath of the Euromaidan revolution, a newly elected President Petro Poroshenko discharged the Verkhovna Rada. However, lacking a majority in the legislature, his initiative to change the electoral legislation and restore the proportional system was not supported by the MPs (Borisov 2018: 262). The parliamentary elections in October 2014 were held according to the existed mixed system. Yet, it helped Poroshenko's bloc win the majority (132 out of 450 seats): 63 seats by the proportional system (the second result) and 69 by the majoritarian one (the first result). Besides, in November 2017, Poroshenko managed to return the right to appoint

[155] The agreement, among other things, envisaged: to restore the 2004 version of the constitution within 48 hours; to initiate a constitutional reform to balance the authority of the President, Parliament, and government; and to hold presidential elections no later than by December 2014.

and dismiss the heads of local state administrations and their deputies, who previously had to pass through a contest, regaining political control of regions (Shumilin 2017).

Nonetheless, Poroshenko, lacking political support and popularity due to the deteriorating economic conditions, did not manage to amass significant political powers, losing in the 2019 presidential election to political outsider Volodymyr Zelensky. Yet Poroshenko's regime under the guise of containing Russia's aggression in the information sphere managed to implement a range of measures that significantly affected the extent of internet control. As I discuss in section 3, the Ukraine-Russia conflict in 2014 appeared to be a good justification for state control over the dissemination of digital information in the country.

All in all, the balance of political power has been relatively fairly distributed in Ukraine, with none of the political actors having the centralised authority over others. The nature of political institutions in Ukraine has been inclusive. The parliamentary and presidential elections are competitive, the authority of the chief executive is significantly restricted, and a large segment of society is able to participate in, and if needed to shape, politics[156]. In this regard, civil society in Ukraine, after the 2004 Orange revolution and 2014 Euromaidan has become strong and vibrant (Wilson 2015: 322, 348). Furthermore, some Presidents could do nothing but to have their political rivals in the government, albeit for a short period of time. For instance, during the Yushchenko presidency, Yanukovych was a prime minister (in 2006-2007), and during the Yanukovych presidency, Poroshenko was a minister of trade and economic development (in 2012). In contrast to other non-Baltic post-Soviet countries, such a situation seems to be rather an exception. In Kazakhstan, it is merely impossible to imagine having political rivals in the government.

Consequently, given the inclusive nature of institutions in Ukraine, control of information on the internet was selective throughout the years and cyberspace was thus diverse and vibrant (Freedom House 2012, 2013). Occasionally, control of digital information took place during some politically volatile events: for example, during the 2014 mass street protests when (online) journalists were attacked by the police. Nevertheless, the extent of internet control was overall limited (Deibert et al 2010, Freedom House 2014). This order of things lasted until 2014 – a year when Russia annexed the Crimean Peninsula, followed by the all-out information war between Ukraine and Russia. Thereafter, the extent of internet control has been significantly extended under the guise of containing Russia's aggression toward Ukraine. In the following

[156] Also, it is of note that two interconnected structural factors such as pervasive corruption and business interests of oligarchs affect politics in Ukraine. Although both negatively affect the democratic development of the country, they do not determine the nature of political institutions.

section, I provide further details of how the regional conflict with Russia led to the unprecedented implementation of numerous information controls by the Ukrainian authorities.

3. INTERNET CONTROL

In Kazakhstan, by the turn of the 21st century, the nature of political institutions became irrevocably extractive and consequently the internet slowly but gradually, if not inevitably, appeared under the wing of the state. In contrast, in Ukraine with inclusive institutional settings, the extent of internet control was limited for a long period of time. Although some information controls, specifically during protests, were sporadically applied, the overall implementation of tactics from the early 2000s until 2014 was selective (Deibert et al 2010, Freedom House 2012, 2013, 2014)[157]. However, after Russia annexed Ukraine's Crimea in February 2014 and the following month held a referendum on the peninsula to legitimise the occupation, the overt confrontation between the two neighbour-states both in offline and online spaces ushered in a new stage in internet control. From 2014 onwards, the number of applied tactics significantly increased (at the time almost half the Ukrainian population had internet access). The political crisis of 2014 has thus become a critical juncture in internet control in Ukraine.

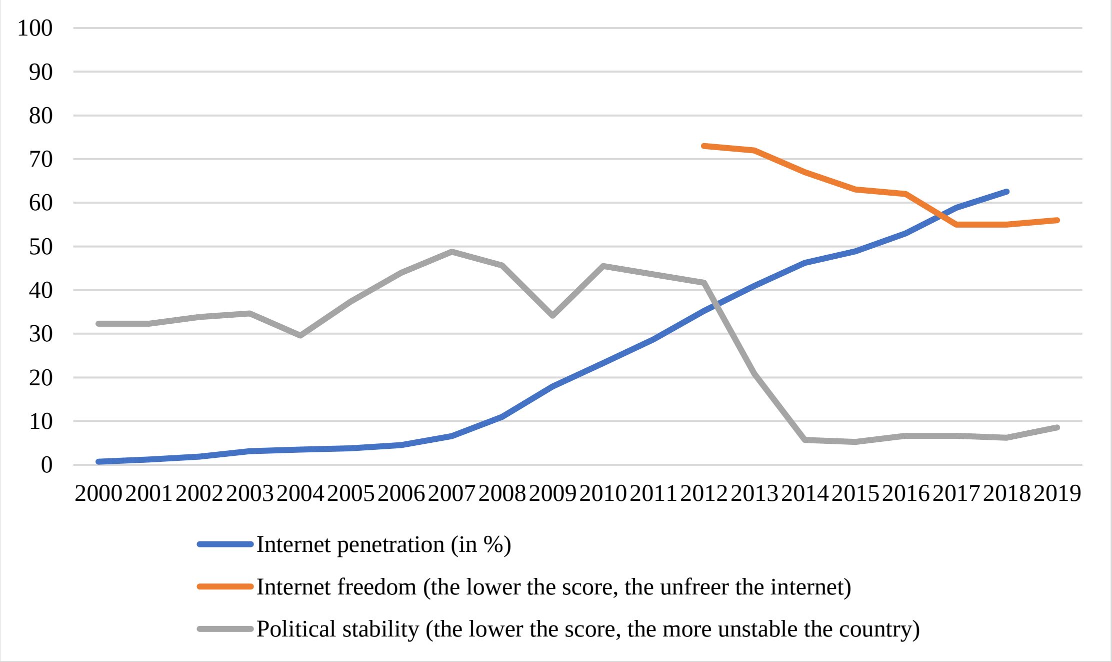
As discussed in chapter 5, amidst a political crisis, more inclusive political institutions did not always prevent the authorities from resorting to information controls. In Ukraine, Petro Poroshenko, the President from 2014 to 2019, implemented a range of measures that significantly affected the extent of internet control, justifying them by the necessity to counter Russia's aggression. The Parliament, an independent body that previously frequently opposed the Presidents, in the post-Euromaidan years was largely compliant with Poroshenko's decisions. The collision with Russia appeared to unite both the President and Parliament to work in unison against the Russian front. In addition, the Security Service of Ukraine (SBU), subordinated to the President, and the government (in the form of a newly created Ministry of Information Policy), formed by the Parliament, played a great role in state interference with digital information. Despite the fair rules of the game, political instability emanating from the 2014 Ukraine crisis contributed to the extension of internet control (figure 17).

Consequently, shortly after the onset of the Russia-Ukraine conflict, Russia's TV channels were shut down in Ukraine. Censorship of online content, which was mainly absent before, followed suit. If in 2014 "[t]he Euromaidan protests did not cause the

[157] According to 2012, 2013, and 2014 Freedom House reports on freedom of the internet in Ukraine. In the previous decade (in 2007-2008), information control was absent (Deibert et al 2010: 249).

[Yanukovych's] government to block or filter websites" (Freedom House 2014: 832), then by 2019 "[t]he government, which rarely blocked content in the past, now restricts access to several Russian-owned web platforms as well as websites deemed to contain Russian propaganda" (Freedom House Ukraine 2019). The direction and pretext for other tactics (such as restrictive legislation, a crackdown on internet users, and social media manipulation) were also evident: all pro-Russian and anti-Ukrainian (both perceived as equal) have been targeted. In the following sub-sections, I discuss specifics of internet control in Ukraine in more details.

Figure 17. Internet penetration[158], internet freedom[159], and political stability[160] in Ukraine



3.1. Systematic censorship of online content

First, during the spring and summer of 2014, in the wake of the Ukraine crisis, Ukraine's authorities banned dozens of Russia's TV channels, including the First Channel – the Kremlin's main propaganda megaphone – to broadcast in the country (NTV 2014). The ban was implemented allegedly to contain Russia's aggression in the information sphere.

After having dealt with TV, the authorities turned to the digital domain. In September 2014, the Ukrainian Security Service seized servers of the reportedly pro-

[158] According to the International Telecommunication Union's statistics. Available from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx

[159] According to Freedom House. The scores for all but the 2019 year were reversed. The score for 2019 was already reversed by Freedom House (2019).

[160] According to the 2018 World Bank Worldwide Governance Indicators.

Russian Vesti newspaper[161], temporarily deactivating its website (Gavrilov 2014). In the following year, a Kiev court sanctioned the Security Service to seize servers of the largest domain registrar (NIC.UA) because it ostensibly hosted a bunch of separatist pro-Russian websites (Karpenko 2015). However, this time the seizure of servers to block five websites temporarily disabled thirty thousand websites, which were unrelated to Russia's information aggression (Poludenko-Young 2015). State agencies in Ukraine acted without considering consequences of their actions as long as websites supposedly favouring Russia were kept off, even if it also led to the deactivation of thousands of websites. Consequently, the Internet Association of Ukraine accused the government of creating political censorship including in cyberspace (Glukhov 2017).

Yet the intolerant approach to digital content allegedly deemed to be anti-Ukrainian (that is, separatist and Russia-orientated) persisted throughout the post-Euromaidan years. For instance, in July 2017, the Security Service informed that it blocked ten more websites that were allegedly disseminating Russian propaganda. The agency reported on its website that "another episode of the RF [Russian Federation] hybrid aggression against Ukraine" was thus prevented (Security Service of Ukraine 2017). Previously, in May 2017, President Poroshenko, as part of sanctions on Russia, had already banned for three years a wide range of Russian websites, including highly popular social networks, email service, search engines, online news, anti-virus software, and various aggregators (Decree of the President of Ukraine 2017). Some of the blocked internet services (such as vk.com, mail.ru, and yandex.ru/ua) were among the top-5 most popular websites in Ukraine (Kalyukov et al 2017), whereas social media platforms Vkontakte (vk.com) and Odnoklassniki (ok.ru) had 27 and 11 million Ukrainian users accordingly – much more than Facebook's 3.2 million (Webb 2017).

Poroshenko justified the ban of popular websites on the basis of fighting Russia's aggressive behaviour in the information sphere: "massive cyberattacks of Russia across the world, in particular recent meddling in the election campaign in France, indicate that it is time to act differently and more decisively" (Vkontakte 2017). The denial of access to mainstream Russian internet services was not, however, supported by international watchdog organisations. Human Rights Watch (2017) regarded the Poroshenko's decree as an infringement on freedom of expression and information, urging the Ukrainian authorities to repeal the ban. Reporters without Borders (2017) also opposed the decision to block Russia's internet services, seeing it as "a disproportionate measure

[161] In May 2015, the Verkhovna Rada's National Security Committee declared that the Vesti is favourable to Russia's aggression and a threat to Ukraine's national security, urging to close the newspaper (Lenta 2015).

that seriously undermines the Ukrainian people's right to information and freedom of expression".

Nevertheless, in 2018, the encroachment on information on the internet continued: in May, President Poroshenko issued another decree, extending measures against Russia's companies and individuals (Decree of the President of Ukraine 2018). This time, almost two hundred websites, including those of Russia's leading TV channels, were ordered to be blocked in Ukraine (Detector Media 2018). In response, some Ukrainian media organisations condemned the blockage of websites as "not correspond[ing] to democratic practices or international norms", asking the President and government for the decree's review (Internet Freedom 2018). Overall, in 2018, about 300 websites presumably exploited by Russia for anti-Ukrainian propaganda and aggression were blocked by the Security Service (Security Service of Ukraine 2018a).

In addition, the government of Ukraine attempted to target content on international platforms such as Facebook, Google, and Twitter. Notably, the number of requests skyrocketed from the second half of 2014 onwards. Overall, the government made 279 requests to remove 2 109 items on Google between January 2012 and December 2019; 95% of them (266) were made since July 2014 (Google Transparency Report n/d/). The main reason to take down items from Google services was related to defamation. Only 22% of all requests led to eventual removal. Also, the government made 241 enquiries about data on 308 Facebook users between July 2014 and December 2019; there were no requests before that (Facebook Transparency 2020). In most cases (64%), some information about Facebook accounts was revealed. Finally, there were only three removal requests and two information requests to Twitter made between July 2016 and June 2019 (Twitter Transparency 2020). Twitter complied with none of them.

At last, in May 2019, the President further extended sanctions against Russia (Decree of the President of Ukraine 2019). The Yandex services (sixty-six websites altogether) again appeared on the list, with the ban now extended until the spring of 2022. By 2019, at least 461 websites reportedly containing pro-Russian and thus anti-Ukrainian content were blocked in Ukraine (Rzheutskaya 2019). As a result, if before the 2014 crisis "the citizens of Ukraine enjoy[ed] largely unhindered access to the internet" and there was "no practice of institutionalized blocking or filtering, or a regulatory framework for censorship of content online" (Freedom House 2013: 744, 747), then later "internet freedom in Ukraine steadily deteriorated in the ensuing period of conflict" (Freedom House Ukraine 2017).

Consequently, far-reaching content censorship of everything perceived as supportive of Russia and separatist regions in the Donbas has become the normal practice of internet control in Ukraine. Interestingly, the blockage on the internet is not selective as access is denied not to a targeted material but the whole website. Unlike in Kazakhstan, there is no legal mechanism for blocking media resources in Ukraine, making the whole process vague as criteria for restricting access to websites apart from the ambiguous "pro-Russian" pretext is unclear. Another issue is the effectiveness of the blockage of so-called pro-Russian websites as sometimes the Ukrainian population, not the Russian government or business, suffered instead. For instance, after restricting the operation of the WebMoney service in Ukraine, as part of May 2018 sanctions, funds of four million Ukrainians were frozen (Nekrasov 2018). Nevertheless, the hysteria about Russia and its aggression has followed most, if not all, tactics of internet control since 2014. In addition, online media outlets and digital users were also intimidated and/or arrested if considered to be loyal to Russia.

3.2. Crackdown on internet users and online journalists

Ukraine's authorities sporadically (but not systematically) resorted to information controls before the onset of the 2014 conflict with Russia, mainly during politically tense periods. For instance, when the mass street protests against Yanukovych's refusal to sign the Association Agreement with the EU erupted in Kiev in November 2013, state agencies, to secure the political survival of the regime, began intimidating and threatening protesters including digital journalists, bloggers, and those streaming online. Overall, 281 journalists, including those working for online media outlets, were attacked during the protests from November 2013 to February 2014 (Rets 2019). Some of them (like journalist Tetiana Chornovil in December 2013) were reportedly punished for criticising the government on the internet (Reporters without Borders 2013a). Also, in an attempt to threaten protesters, an SMS stating "Dear subscriber, you are registered as a participant of mass riots" was distributed to all those located in the Maidan square – a core of the Euromaidan protests (Soldatov and Borogan 2017: 138). By intimidating protesters, including numerous online journalists, Ukraine's authorities attempted to restrict the circulation of anti-government information.

Previously, many independent journalists in Ukraine were also not favoured by those in power. One of the most appealing incidents of past regimes (before 2014) was the "Gongadze scandal" – the murder (decapitation) of opposition journalist Hryhorii Gongadze, reportedly by the instruction of then-President Kuchma (Wilson 2015: 311-312). In other words, Ukraine was not a tolerant place for journalists: 139th out of 167 countries in 2004, 90th out of 175 in 2009, and 126th out of 179 countries in 2013, according to the World Press Freedom (Reporters without Borders 2004, 2009, 2013b). Despite a slight improvement in recent years – the 101st in 2018 and the 102nd in 2019

(Reporters without Borders 2018, 2019) – Ukraine still remains a country with a considerable problem for journalists' freedom.

Nevertheless, despite the unpleasant working atmosphere for journalists in Ukraine, a crackdown (in the form of arrests and imprisonments) on online journalists/bloggers and internet users before the 2014 Ukraine crisis was rare. In 2013, Freedom House (2013: 751) reported that "[t]raditional journalists continue to face regular intimidation and threats of physical violence, although this trend has not been seen as frequently in regard to online journalists". However, after the 2014 conflict with Russia, the number of punishment cases soared in Ukraine. The pretext was straightforward: those (journalists and ordinary users) expressing views on the internet thought to be favourable of Russia and the Donbas were targeted and punished.

Intimidation of Ukrainians for online expressions ostensibly sympathetic to Russia started shortly after the Euromaidan revolution. One of the first investigations began in March 2014 when houses of three Ukrainian internet users were searched and a criminal case for posting separatist and pro-Russian messages was opened (Karpenko 2014). In another incident, in July 2014, a citizen of Dnepropetrovsk was sentenced to three years for separatist calls on social media (Korrespondent 2014a). In February 2015, a journalist (Ruslan Kotsaba) was arrested and charged with treason for spreading anti-Ukrainian views on YouTube (Rafal 2017). Kotsaba urged people not to join the Ukrainian army. Amnesty International (2015) condemned the journalist's arrest, naming him the prisoner of conscience; in July 2016 Kotsaba was acquitted. In May 2015, three more users were detained by the Security Service for sharing whereabouts of the Ukrainian army (and thus the anti-Ukrainian information) and charged for promoting the terrorist organisation (Novoe Vremya 2015).

The repeated prosecution of Ukrainians for internet activities in 2014-2015 "signalled the Ukrainian government's growing intolerance for critical content online" (Freedom House 2015: 827). However, the situation did not change in the following years. In September 2016, the Security Service detained a woman for promoting anti-Ukrainian propaganda on social media (Korrespondent 2016a). This was just one of the numerous detainments and arrests in Ukraine for spreading pro-Russian and anti-Ukrainian separatist materials on the internet in 2016. Imprisonments were not rare either. In March 2016, for instance, a Ukrainian was sentenced to five years for separatist views voiced on social media (Korrespondent 2016b). Thus, throughout 2016, state agencies continued to punish for "so-called "separatist" and "extremist" expression online, with many users detained, fined, and even imprisoned" (Freedom House Ukraine 2016).

Similarly, in 2017, the punishment for internet activities in Ukraine persisted, even for comments or reposts. In March 2017, a Uzhhorod's citizen was given three-year probation for comments on Facebook, in which he urged to overthrow a local administration (Romanov 2018). Also in March 2017, a worker from Mariupol was arrested for reposting on a social networking website a message that promoted separatism and later given a three-year sentence in prison (Tikhiy 2018). Thus, in addition to posts, comments and reposts on social media were also targeted. Overall, between spring 2014 and summer 2017, at least thirty-six court's convictions were given for promoting the anti-Ukrainian position (interpreted as calls to overthrow the regime) (Yastremskaya 2017); this is not to count a large number of detainments, intimidations, and house searches of internet users since 2014 that did not result in a court hearing. However, in 2017 alone, the number of convictions surpassed those of previous years: thirty-seven administrators and owners of reportedly anti-Ukrainian communities on social media, in which they agitated to overthrow the constitutional order and regime, were sentenced (Arguments and Facts 2017). (Articles 109 and 110 of the Criminal Code of Ukraine (2001) entail up to five-year imprisonment for such charges).

The Ukrainian spy agency did not stop a crackdown on Ukrainians for their internet activities. In February 2018, the Security Service arrested a user who ostensibly administered anti-Ukrainian communities on social media (Security Service of Ukraine 2018b). In the following month, another Ukrainian was detained for distributing separatist materials and propaganda (Security Service of Ukraine (2018c). In both cases, criminal proceedings followed. Overall, the Security Service reported that in 2018, for disseminating calls on the internet to overthrow the regime, fifteen convictions were given and twenty-three individuals were notified, with eighty-three more criminal cases being under investigation (Security Service of Ukraine (2018a). The agency also stated that "preventive measures have been taken against 220 administrators of Internet communities distributing destructive [anti-Ukrainian] content to more than 10 million Internet users" (ibid), though without clarifying any details of preventive actions.

In addition to the systematic persecution and prosecution of users, law enforcement also targets digital journalists. In one of such episodes, in May 2018, Kirill Vyshinsky, then the head editor of the RIA Novosti news outlet, was arrested by the Security Service for his pro-Russian stance and charged with treason and support of separatist regions in the east of the country (RIA Novosti 2019). Curiously, the day of arrest (15 May 2018) coincided with Putin's opening of the Crimea bridge over the Kerch strait that joined the Crimean Peninsula with the rest of Russia (Kremlin 2018). Eventually, in September 2019, after numerous trials, Vyshinsky landed in Moscow as part of a mutual exchange of individuals between Ukraine and Russia (Anoshin 2019).

In 2019, the situation with regard to pro-Russian and separatist content and authors did not improve. The name of the enemy was clear – the Russian Federation – and thus control of information on the internet via numerous detainments and notifications remained in place. For instance, in April 2019, a court in Odessa sentenced a man to five years in prison with three-year probation for separatist calls on his webpage (Segodnya 2019). In a similar incident the same month, another Ukrainian citizen was not arrested but was warned of an illegal action (Security Service of Ukraine 2019a). In May 2019, the Security Service searched the house and detained a "pro-Russian propagandist who, tasked by Russian supervisors, prepared and distributed anti-Ukrainian materials in the Internet" (Security Service of Ukraine 2019b).

In other words, the situation has not changed since 2014: state agencies continued to encroach on individuals perceived as supportive, via social media, of Russia and separatist regions of the Donbas. Consequently, hundreds of criminal cases were opened in retaliation to expressing anti-Ukrainian views on the internet. Likewise, Freedom House in the 2019 report on internet freedom in Ukraine concludes that "[a]rrests of users are commonplace, primarily as an extension of ongoing hostilities between the government in Kyiv and Russian-backed separatists, as are attacks against online journalists" (Freedom House Ukraine 2019).

However, apart from punishing users for their political views expressed online (even in a comments' section), Ukraine's authorities also intimidate online media outlets and their journalists deemed to take Russia's side. For instance, in May 2018, in addition to the arrest of Vyshinsky (discussed above), the office of RIA Novosti and apartments of some of its journalists were raided (RIA Novosti 2018a). Previously, in June 2017, the office of another, reportedly anti-Ukrainian, media (Strana) was searched while its head editor was arrested on suspicion of receiving bribes (Ukraine 112 2017). In August 2017, a repeated search of Strana's office and houses of its journalists was conducted (Channel 24 2017). Similarly, in July 2017, the National Police and the Military Prosecutor's Office raided the office of Vesti online news, holding its employees for fifteen hours (Gubin 2017). It was not the first raid of Vesti: in May and September 2014 and in June 2015, the authorities had already searched its offices (Vesti 2017). Yet the July 2017 incident was not the last one as in February 2018 the office of Vesti was again searched by law enforcement agencies (RIA Novosti 2018b). Both Strana and Vesti outlets, which were portrayed as pro-Russian, attributed the raids to their professional activity.

Overall, a harsh and punitive approach toward internet users and online journalists "sends a strong signal of government presence and policing of online activity, aimed at deterring similar activity in the future" (Rød and Weidmann 2015: 341). Thus, the systematic persecution and prosecution for views expressed online contribute to increasing self-censorship among clients of cyberspace, shaping and limiting the digital flow of information. Besides, if such a tactic of internet control is insufficient, restrictive legislation that empowers state agencies can follow suit.

3.3. Internet-related legislation

During politically turbulent periods, governments tend to resort to information controls despite the inclusive nature of political institutions (chapter 5). A political crisis, in general, can change the government's attitude toward the dissemination of information on the internet. This happened in Russia in the aftermath of the 2011-2012 mass protests provoked by Putin's decision to run for the third presidential term. The Russian authorities exercised a relaxed approach to the internet prior to 2011 but unexpected demonstrations in Moscow became a wake-up call to Putin and his acolytes (Oates 2013). As a result, from 2011 onwards, Kremlin changed its attitude to the circulation of digital information and now Russia has arguably become one of the most sophisticated countries in shaping narratives in cyberspace.

The Yanukovych government faced a similar problem when a large number of people took to the streets in the late autumn of 2013. It is estimated that in some critical moments up to half a million Ukrainians participated in the protests (Sakwa 2016: 82). In January 2014, in the wake of demonstrations and in a desperate attempt to retain political power, Yanukovych's regime passed twelve legislative acts (N3879) aimed to curtail the protest movement. Laws, quickly dubbed "dictatorship laws", in contrast, backfired further intensifying the anger of activists (Wilson 2015: 349). In the end, Yanukovych, unlike Putin, did not manage to stay in office.

Meanwhile, in the digital domain, Yanukovych's new legislation significantly extended the state authority in the regulation and control of communications and information (Law on Amendments to Some Laws of Ukraine 2014). In particular, January 2014 amendments vested the State Commission in charge of communication and informatization spheres with the authority to restrict access to websites that ostensibly contain illegal materials. At the same time, all internet resources that create (but not reproduce) news content were equalled to information agencies, which must be registered with the government within three months, according to amendments. If a website fails to register, then the State Commission might block access to the website (webpage). New legislation also increased the size of fine in case internet providers fail to deny access to websites by the Commission's instruction.

In essence, by having control over the registration process, the government, like in Kazakhstan, received a sway on all information resources on the internet.

Consequently, all critical media, including online journalists and bloggers, could be targeted and silenced under new amendments. Furthermore, articles that the distribution of extremist materials on the internet will be fined for the first time and prosecuted (up to three years in prison) for the second time were included to the 2001 Criminal Code. In addition, the 2001 decriminalisation of offence for slander was reversed as, according to new laws, slander on the internet and media could be fined or lead to up to one year of correctional works. In this regard, ordinary internet users could be prosecuted for their anti-government stance.

The adoption of January 2014 legislation, in line with my findings (chapter 5), demonstrates that the authorities employ internet control tactics in the wake of political instability. Nevertheless, given the extension of state control over the digital domain, new laws were heavily criticised by NGOs and civil society activists (Bohdanova and Lokot 2014). Under increasing pressure, most of the anti-protest laws (nine out of twelve legislative acts) were eventually withdrawn by the end of January 2014 (Law on Recognising Some Laws of Ukraine as Invalid 2014), being in action less than two weeks. Yanukovych's attempt to expand state's powers at the expense of the free flow of digital information proved to be unsuccessful.

At present, there is no explicit reference in Ukrainian legislation to the internet as a means for the dissemination of extremist and separatist calls (like in January 2014 Yanukovych's amendments). In the current edition, the Criminal Code of Ukraine (2001) (articles 109 and 110) entails up to three years in prison for public calls to overthrow the constitutional order and from three to five years in prison for public calls to change the state borders, without clarifying the means (and platforms) for making calls and distributing separatist and extremist materials. Yet, as discussed in sub-section 3.2., numerous arrests and imprisonments of internet users and journalists for their political views expressed online imply that activities in cyberspace, too, can be covered by the Criminal Code. Basically, under the current edition (last amendments to articles 109 and 110 were made in October 2014), anti-Ukrainian propaganda on the internet – be it real or perceived – can be (and has been) legally prosecuted under the extremist and separatist pretext.

In addition, like in Kazakhstan, both the Strategy of Cybersecurity of Ukraine (2016) and the Doctrine of Information Security of Ukraine (2017) extended and justified government's increasing powers in the information domain. The Cybersecurity Strategy, signed by then-President Poroshenko in March 2016, paved a path to the formal identification of Russia as the aggressive state that exploits digital technologies against Ukraine, and thus measures undertaken by the Ukrainian authorities to tackle all pro-Russian could be vindicated. The overall language in the document is, however, restrained. There are only two references to Russia in the Cybersecurity Strategy. First, that Russia's aggression continues and thus a national system of cybersecurity should be established. Second, that the security and key spheres in Ukraine are becoming increasingly vulnerable to cyberespionage and sabotage by foreign security services. This happens, according to the document, due to the dominance of the information infrastructure of Ukraine by groups and individuals directly and indirectly linked with Russia. Thus, the Strategy implicates that numerous citizens arrested in Ukraine for separatist calls and propaganda on the internet are navigated and coordinated by the Russian Security Committee.

However, if the anti-Russian stance was thinly veiled in the 2016 Cybersecurity Strategy, then the Information Security Doctrine of Ukraine signed by Poroshenko in February 2017 was explicit in its accusation: Russia is the number one enemy that has thrown all efforts to undermine Ukraine's statehood. Hence, Russia is blamed for all crimes in the information sphere as, according to the doctrine, the Kremlin has been applying the newest information technologies to manipulate Ukrainians' minds, to incite ethnic and religious hatred, to propagate the aggressive war, to forcibly change the constitutional order, and to violate Ukraine's sovereignty and territories. Consequently, the whole doctrine is based on outlining how to contain and resist the Russian aggression in the information sphere – formulated as vital interests of Ukrainian society and state. Most importantly, the doctrine has extended the state authority in the digital domain: now the blockage of pro-Russian internet resources is justified because Russia's hybrid warfare has reportedly transferred the information sphere into the conflict zone against Ukraine.

In other words, Russia is the main villain and thus all information, including on the internet, supportive of Russia must be targeted: authors to be detained, websites to be blocked. To make things simpler, the Parliament of Ukraine in 2018 formally recognised Russia as the aggressor country and occupant of Ukrainian territories by passing a Law on State Policy in Donetsk and Luhansk Oblasts (2018). If in Kazakhstan general security threats were vaguely referred to in order to justify sweeping state powers in the digital domain, in Ukraine the threat to national security was made explicit. Therefore, since the menace became known, all efforts should be thrown to counter it – a convenient justification for the increasing number of both arrests of internet users and blocked websites in Ukraine.

In July 2017, other attempts to further expand already extensive state powers in controlling the dissemination of digital information were made. On July 11, 2017, a Law on Amendments to Some Legislative Acts of Ukraine to Counteract the Threats to National Security in the Information Sphere N6676 (2017) was proposed, though it was not considered in the Parliament and was withdrawn in the following day. On July 12, 2017, an identical law with the same title (but the different number and authors) was again proposed and eventually considered in June 2018 (Law on Amendments to Some Legislative Acts of Ukraine to Counteract the Threats to National Security in the Information Sphere N6688 (2017).

The new law, attracting considerable criticism from NGOs and civil society, envisaged following key amendments that were increasingly in line with Russian and Kazakh practices of internet control. In particular, the authors of N6688, referring to the necessity to improve cyber-defence of the country, proposed to allow a temporary blockage of websites during a pre-trial investigation or by the investigator's or prosecutor's instruction in case of emergency situations. In the latter case, like in Kazakhstan, the court's decision would not be needed. Another amendment was to create a single registry (blacklist) of banned websites, like in Russia. To implement the blockage of websites, internet providers must purchase all necessary equipment at their own expense; in failing to comply, providers would be fined. Thus, the Ukrainian authorities would have a legal instrument to put pressure on internet operators.

Overall, proposed amendments would significantly facilitate state control over information on the internet. However, perhaps due to the lack of explicit reference to Russia (there was the reference to cyber threats without naming any actors) and given wide criticism of proposed amendments (The Ukrainian Helsinki Human Rights Union 2018), the N6688 law was not supported by the majority in the Parliament and was eventually withdrawn in August 2019. Yet, even without this law, discussed above legislation and Presidential Decrees proved to be sufficient to shape and restrict the digital flow of information within national borders.

The latest endeavour that would significantly curb the freedom of expression in Ukraine and further extend state control over the dissemination of digital information has been legislation on fighting disinformation proposed by the Ministry of Culture and Information Policy of Ukraine in January 2020. Specifically, recommended amendments envisage to create a voluntary index of trust of mass media outlets and to initiate a position of a special commissioner with the authority to decide whether the information is fake. The latter, among other things, would also oversee the reliability and accuracy of distributed information in the media and, if needed, seek a court's decision to restrict access to disinformation content distributed on the internet and via messengers. In general, the commissioner would have a wide range of powers over the dissemination of information in the country.

In addition, according to legislative proposals, media outlets would face huge fines for the distribution of disinformation materials; if a media outlet voluntarily refuted disinformation then there would be no fines for the first two cases. Individuals, found of the systematic (more than three times within a year) distribution of disinformation that poses a threat to Ukraine's national security and territorial integrity (basically, all separatist and anti-Ukrainian content), would face a huge fine or correctional works up to two years. However, those distributing disinformation via bots or fake accounts would be imprisoned from two to five years. In other words, proposed legislation is even harsher than Yanukovych's anti-protest laws.

The disinformation law has not been yet accepted, though the Criminal Code, the Cybersecurity Strategy, and the Information Security Doctrine along with Presidential Decrees (discussed in sub-section 3.1.) have already rendered state agencies with the necessary means to exercise control over the flow of digital information.

3.4. Empowered state agencies

Although the legislative framework seeks to justify the blockage of websites and arrests and imprisonments of internet users, internet service providers are private in Ukraine. The largest provider that owns most of the internet infrastructure in the country, Ukrtelecom, unlike in Kazakhstan, is not owned by the state. Consequently, the government has no direct control over the internet infrastructure and operators – the first-hand actors that can restrict access to websites. Nevertheless, state agencies, being in charge of state regulation of the digital sphere in Ukraine and shielded by legislation, managed to obtain leverage over internet intermediaries.

One of the central actors is the National Commission for the State Regulation of Communications and Informatization created in 2011, which is responsible directly to the President and accountable before the Parliament (Decree of the President of Ukraine 2011). The Commission regulates and oversees the spheres of communications and informatization. One of its responsibilities is to issue licences to communication operators so that they can function in Ukraine. The agency also controls whether internet and mobile operators follows legislation of Ukraine. For example, in the wake of Poroshenko's sanctions on Russia, local internet providers were asked to deny access to numerous Russian websites. The Commission reminded all telecommunication operators that they are liable to abide by Ukraine's laws, warning that fines could follow (National Commission for the State Regulation of Communications and Informatization n/d). Consequently, Russian social media platforms and websites were all blocked in Ukraine. Despite the state-free telecommunication market, restrictive laws, doctrines, and decrees will nonetheless put pressure on private internet actors, extending state control over information on the internet.

Another state agency that has an impact on the dissemination of digital information in Ukraine is the Ministry of Information Policy[162]. The Ministry was officially formed in January 2015 with the main aim to contain and counter the Russian aggression in the information sphere: its official top priority is to win the information war against Russia (Decree of the Cabinet of Ministers of Ukraine 2015). Interestingly, the Ministry in its program on the development of the information space of Ukraine argues that Ukraine has the most impartial Russian-language media in the world (Ministry of Information Policy n/d). However, as discussed in sub-sections 3.1. and 3.2., many Russian-language news outlets functioning in Ukraine were banned and/or intimidated by Ukraine's law enforcement agencies after the Euromaidan revolution. In addition, the Law on the Ukrainian Language (2019) significantly diminished the sphere of influence of Russian "unbiased" mass media.

The Ministry is also in charge of monitoring information distributed by domestic and foreign mass media outlets. Although the Ministry of Information Policy, the key institution that forms and executes the state policy in the information domain, formally declared its function as to fight the information war with Russia, it is in essence just another tool of the government to endorse the anti-Russian stance in the country and abroad. Consequently, the Ministry, in line with the proclaimed goal, has been constantly offering to restrict access to internet resources that are perceived as favourable of Russia. In 2017, it offered to restrict access to twenty, in 2018 – to twenty-one, and in 2019 – also to twenty-one reportedly anti-Ukrainian websites (Ministry of Information Policy 2017).

All three lists (sixty-two websites altogether) were given to the Security Service of Ukraine[163] (SBU), a successor to the Soviet-era Committee for State Security (KGB) (Decree of the Verkhovna Rada 1991). The agency, responsible for information security of the country, is another state actor that affects the extent of internet control in Ukraine. Given its subordination to the President and the anti-Russian position of the political establishment, it is natural that the Security Service has become one of the main actors in Ukraine's information war against Russia. Moreover, one of the agency's main functions is to conduct the informational and analytical work in line with the interests of Ukraine's foreign and domestic (that is, anti-Russian) policies (Law on the Security Service of Ukraine 1992).

[162] The head of the Ministry of Information Policy from 2015 to 2019 was Yuriy Stets, a henchman of Poroshenko. In 2020, the newly created Ministry of Culture and Information Policy took over the regulation of the information sphere in Ukraine.

[163] The Security Service was headed from 2015 to 2019 by Vasyl Hrytsak, Poroshenko's associate.

Accordingly, the spy agency has been monitoring social media websites, targeting the authors of anti-Ukrainian materials. As discussed above, numerous internet users were arrested and imprisoned for their activities in cyberspace. Even those who comment on or repost pro-Russian content were targeted, with some individuals receiving real sentences in prison. In addition, (online) journalists and media outlets deemed to be sympathetic to both Russia and separatists were also intimidated by the Security Service. The main goal of such an approach is to demonstrate that the support in any forms of the aggressor-state (Russia) and separatist regions (the Donbas) will be punished. In essence, the agency, fully subordinated to the President, has become an effective instrument against the ostensibly anti-Ukrainian and pro-Russian rhetoric on social media. By instilling a sense of fear – not everybody will want to spend up to five years in prison for what is regarded anti-Ukrainian calls and propaganda – the Security Service has severely affected the freedom of expression and information in the country. Yet in addition, the government also resorts to censorship through noise to shape the digital flow of information.

3.5. Manipulation of public opinion and communications surveillance

Manipulation of public opinion via social media is another tactic of internet control present in Ukraine, especially at the time of forthcoming elections and political instability. However, it has been overshadowed by the emphasis on Russia's involvement. Although the first reports about the possible distortion of political discourse in Ukraine by paid-for commentators emerged in 2011 (Bishchuk 2011), the main attention was on Russia as a key intruder of Ukraine's information sphere with the main aim to spread the anti-Ukrainian sentiments (Toler 2014, Jankowicz 2019). Moreover, as a result of the 2014 overt confrontation with Russia, the latter was increasingly castigated in the local and international media for propaganda and disinformation campaigns (Toler 2015, Nakashima 2017). As a result, given that the focus was on exposing Kremlin-orchestrated propaganda in Ukraine – a special website (stopfake.org) to debunk Russian disinformation was also created – the involvement of the government of Ukraine in social media manipulation was largely underreported.

Nonetheless, in the shadow of numerous articles on how Russian paid-for commentators and bots shape political narratives in Ukraine, some authors (Skliarevska 2018) revealed that the same tactics are used by the Ukrainian political actors, too. In addition, in 2016, reportedly due to its independent stance and investigative materials, a Ukrainian online media outlet was exposed to attacks on social media by bots and commentators, who undermined critical reports with pro-government messages

(Gorchinskaya 2016). In other words, pro-government commentators tried to influence anti-government content on the internet.

In another example, Lozovyi and Davidenko (2017) found that Poroshenko employed an army of more than 1 500 bots on Facebook, which actively commented on President's posts, shaping public perception of his messages. Overall, from 2014 to 2017, at least every sixth comment on Poroshenko's posts was written not by human but by an automaton. Consequently, all supporters of Poroshenko on social media, including bots, paid-for commentators, bloggers, and ordinary people, were dubbed "porokhobots" (Holub 2017, Bakhteev 2019). However, Poroshenko is not the only politician investing in bots' farms; bots also quickly promoted Yulia Tymoshenko's public page on Facebook, making it one of the largest in Ukraine (Bobritsky 2018).

Furthermore, in 2019, a journalist, after intruding a "troll farm" in Kiev, discovered how paid commentators, using multiple fake accounts, manipulate public opinions of Ukrainians. The undercover journalist "was expected to produce around 300 comments, posted either on the politicians' personal Facebook pages or under posts of articles published by popular Ukrainian news sites" (Motorevska et al 2019). Similarly, Bradshaw and Howard, after analysing "government or political party use of social media to manipulate public opinion" (2018: 9) across the world, found evidence of public manipulation in eighty-four countries, including Ukraine and four other post-Soviet states. At least one state agency has been involved in social media manipulation in Ukraine since 2014, according to the authors' findings. The strategies for spreading pro-government posts and attacks on the opposition on the internet were employed via the use of fake accounts run by human operators and bots. In terms of capacity, the state agency appeared to employ and coordinate a large number of people, from twenty to forty thousand full-time employers[164]. Thus, Ukraine happened to have the factory of paid-for commentators like the infamous Russian Internet Research Agency.

The agency that Bradshaw and Howard (2018) meant is the Ministry of Information Policy created in January 2015 to combat Russian propaganda and disinformation. For that reason, the Ministry began recruiting a voluntary "information army" (Ukrainskaya Pravda 2015), reaching the number of forty thousand internet warriors by May 2015 (Korrespondent 2015). Consequently, waging the information war against Russia, the Ministry itself began shaping public opinion of Ukrainians (extending internet control) as pro-Russian content was censored by default. It is no coincidence

[164] Ukraine is in the group of countries with the medium capacity of cyber troops, according to Bradshaw and Howard (2018).

that the Ministry was quickly called “the ministry of truth”, implying the Orwellian-style censorship (Lokot 2014).

In addition to anti-Russian propaganda waged in the wake of the 2014 political crisis, social media manipulation, in line with my findings, took place around elections in Ukraine. The latest incident was the 2019 presidential elections, in which porokhobots were heavily involved. After the first round, two front-runners, the incumbent (Poroshenko) and a comedian with no political experience (Zelensky), remained on the list. In the lead-up to the elections, Poroshenko, who was losing popularity among voters, began co-opting influential bloggers who produced positive reports about the President (Kovalenko and Zhartovskaya 2018). Besides, during the election campaign, Poroshenko’s and Zelensky’s associates tried to accuse one another, sometimes resorting to “black PR” (very popular in the post-Soviet region). For instance, pro-Poroshenko communities on social media were increasingly portraying Zelensky as Kremlin’s puppet, urging not to vote for him (Spirin 2019). Poroshenko’s team clearly emphasised Zelensky’s alleged ties with Russia: after the first round, billboards with Poroshenko facing Putin instead of Zelensky as a presidential candidate were installed on the streets (Shumilin 2019). Furthermore, a Telegram channel of Poroshenko presidential campaign published an edited video that unambiguously implicated that Zelensky is a drug addict (Rudyk 2019).

On the other hand, shortly before the first round, a TV channel (1+1) owned by Kolomoisky, who is closely associated with Zelensky, released a “sensational” video-investigation claiming that Poroshenko was involved in the organisation of murders, including of his own brother (Ivanova 2019). The video was also published on YouTube under the provocative title of “50 shades of Poroshenko”, having currently more than 1.6 million views[165]. After the 2019 presidential election, Ott and Lozovyi (2019) also found that current President Zelensky had the largest number of bots (almost twenty-eight thousand) who followed his page on Facebook; Poroshenko was the second with twenty thousand bots. In other words, political actors and institutions in Ukraine do not hesitate to exploit the tool of social media propaganda and disinformation, by default attributed to the Kremlin, to shape the public discourse in the country.

As can be seen, the aforementioned tactics of internet control began proliferating largely after the critical juncture in 2014. Probably, the only tactic that was continuously evident in Ukraine before the 2014 political crisis, despite the constant power battles between political actors, is covert surveillance of communications. As early as 2002, all

[165] The video is available from https://www.youtube.com/watch?v=vNDmnRbxkGQ&feature=emb_logo

internet and communication operators that dealt with the state information were required to install Russian SORM-like systems, in accordance with the Order of the State Committee of Informatization and Communication (2002). The SORM monitoring equipment, installed at providers' expense, was able to intercept telephone and internet traffic. Thus, the order gave sweeping powers to the Security Service of Ukraine as it had access to communication providers' and thus subscribers' data. Although the order was repealed in 2006, the Security Service retained surveillance capabilities as the SORM equipment remained in place (Soldatov and Borogan 2012). Furthermore, the warning SMS selectively sent to mobile phones of Euromaidan protesters in January 2014 demonstrates that the Security Service can intercept mobile signals and locations without turning to mobile operators (Soldatov and Borogan 2017: 138-139).

The repeated interception of phone conversations between the Donbas separatists and consequent leaking to the media also showcase surveillance capabilities of the Ukrainian Security Service in the post-Maidan years. In one of such examples in September 2014, the agency intercepted and made public a phone call of separatists in which they shared a recent attack on a village (Korrespondent 2014b). The SBU also intercepted phone conversations of people suspected in shooting the Malaysian Airlines' Boeing (MH17) in July 2014 (Krutov 2019). Besides, the Security Service exploited covert surveillance to target pro-Russian individuals: by wiretapping telephone talks of Donbas citizens, those who expressed anti-government and pro-separatist sentiments were eventually detained (Makarenkov and Galskaya 2019).

Yet, compared to other tactics of internet control, practices of covert surveillance of communications did not intensify because of a political crisis or upcoming leadership contest. Exceptionally, surveillance powers of the Security Service were evident in Ukraine before 2014, though numerous attempts to extend them were taken during the Poroshenko period (e.g. laws N6688 and N6676 proposed in 2017). Currently, law enforcement agencies conducting investigative operations need a court order to monitor communication channels, though "a lack of comprehensive legislation to protect the privacy and prevent abuse of surveillance powers" (Freedom House Ukraine 2019) is still a problem in Ukraine.

4. CONCLUSION

To summarise, the nature of political institutions in Ukraine from 1991 onwards, including the 2014-2019 period, has been continuously inclusive: the authority of the chief executive is restrained, the parliamentary and presidential elections are competitive, and a large segment of society can participate in political processes. Given the regional divisions in the country (pro-European west and pro-Russian south-east), the political elite was fragmented and thus it was always challenging for the incumbent Presidents to consolidate significant powers in their hands. Even if they succeeded, it did not last too long. In contrast to Kazakhstan, Ukrainian politics, due to a more competitive political landscape and constraints on what Presidents could and could not do (the latter always had to take into account the Parliament and government), has been more democratic.

Nevertheless, despite the inclusive nature of political institutions in Ukraine, the extent of state involvement in the digital sphere – limited in the past – has significantly increased since 2014. In Kazakhstan, the extractive institutional setup became the main condition of substantial control over digital information: a small-coalition leader, feared of the democratising potential of the internet and online media, employed information controls to avoid any threats to his reign. In Ukraine, however, the situation was different: political instability provoked by the regional confrontation with Russia resulted in the extensive usage of internet control tactics. Consequently, the information war with Russia conveniently justified the far-reaching state interference with digital information, notwithstanding the existing fair rules of the political game.

After Russia's annexation of Crimea in 2014 and its subsequent support of separatist regions in the Donbas, the anti-Russian current has absorbed Ukrainian politics. The Parliament and President, despite many disagreements in the past (as showcased in section 2), have in many instances worked together to contain Russia's aggression – be it real or perceived. As Bueno de Mesquita et al (2003: 27) note, "former competitors coordinate with one another to solve a shared problem: the (usually financial or military) crisis of confidence encourages them to cooperate for the moment, putting aside their divergent concerns … [t]heir incentive to cooperate at a moment of crisis exceeds their divergent interests". This is what happened in Ukraine. The logic of collective survival of main political actors, exacerbated by the overt conflict with Russia, has eventually resulted in the extension of internet control.

In almost all instances, internet control tactics were covered by the necessity to fight the enemy (Russia was officially declared as such) that reportedly exploits information technologies against Ukraine. As a result, pro-Russian websites and social media platforms were blocked by numerous Presidential Decrees of Poroshenko. Freeing hands to ostensibly tackle pro-Russian content, the local authorities effectively (and systematically) censored anti-Ukrainian and anti-government information. Besides, ordinary internet users and (online) journalists were targeted, receiving real prison sentences for content perceived as supportive of Russia and/or separatists. The number of persecution and prosecution of those who express political views on the internet increased while offices of online media outlets were raided. In addition, state agencies such as the Security Service and the Ministry of Information Policy obtained sweeping powers in the digital domain, negatively affecting the dissemination of digital information. All of the above is very similar to what happened (and continues to happen) in Kazakhstan, but if in Kazakhstan extensive control of information on the internet began in the early 2000s, in Ukraine it largely started in 2014.

To justify increasing internet control, legislation was passed in due course. In particular, the 2016 Cybersecurity Strategy and the 2017 Information Security Doctrine along with the 2001 Criminal Code[166] and 2017, 2018, and 2019 Presidential Decrees rented state agencies with the necessary means to control the dissemination of digital information by targeting reportedly pro-Russian internet resources, narrative, and individuals. In this regard, compared to comprehensively restrictive legislation of Kazakhstan, Ukraine's internet-related legal framework can appear to be inadequate. After all, Kazakhstan's government has been stamping laws and regulations since the end of the 1990s – from the very beginning of internet proliferation in the country. Yet even those already passed laws and decrees in Ukraine proved sufficient to limit the online flow of information within national borders.

Besides, Ukrainian politicians, including ex-President Poroshenko and current President Zelensky, did not refrain from using bots and paid-for commentators to shape public opinion. Although it was revealed that the leading Ukrainian politicians exploit bots and fake accounts to promote their pages on social media and comment on their posts, distorting the perception of actual events, the main emphasis in the domestic and international media is yet on Russia and its disinformation campaigns. The latter fact, actually, serves very well those in power in Ukraine, switching attention from their manipulation of social media to Russia. In addition, the undercover journalist discovered a factory of trolls, like in Russia (the IRA) and Kazakhstan (Nurbots), tasked with writing positive pro-government messages on the internet. Moreover, a 40 000-strong army of internet warriors was officially gathered by the Ministry of Information Policy reportedly to contain the Russian aggression in cyberspace. In other words, Ukrainian political actors themselves engage in manipulation of public opinions of Ukrainians, despite a continuous reference to the Russian threat.

Having conceptualised the enemy in the form of Russia and highlighting the Russian aggression in the information sphere, Ukraine's President and Parliament and their subordinated agencies (the Security Service and the Ministry of Information Policy, respectively) themselves began shaping the country's information space. Justifying all actions of internet control as countermeasures to prevent national security threats,

[166] Although there is no reference to the internet in the Criminal Code, its articles were used to persecute and prosecute numerous internet users for online publications in the wake of the 2014 Ukraine crisis.

Ukraine's authorities have substantially strengthened control over the dissemination of digital information. Yet, despite all these attempts to capitalise on the Russian threat, Poroshenko's regime did not manage to stay in office. The increasing employment of information controls did not help Poroshenko win in the 2019 presidential election.

Nonetheless, the main lesson that can be drawn from the case study of Ukraine is that the inclusive nature of political institutions does not necessarily serve as a hindrance to the substantial extent of internet control. This is because political instability provoked by an external shock such as the 2014 overt confrontation with Russia – and despite institutional constraints on the President's authority and the strong Parliament and civil society – has led to the repeated employment of information controls. Following the results of the comparative analysis (chapter 5), this chapter demonstrated that not only countries with extractive political institutions, like Kazakhstan, but countries with inclusive institutions, like Ukraine, tend to considerably control the dissemination of digital information within national borders. This finding, as I argue in the concluding chapter, broadens our understanding of state control over information on the internet and respectively supplements the scholarly literature.

CHAPTER 8. CONCLUSION

1. INTRODUCTION

In this chapter, I conclude my study of tactics and conditions of internet control. The main focus is on the findings of the comparative analysis of sixty-five countries and two case studies and consequent contributions to the scholarly literature. First, I briefly outline the research design of my study. Then, I discuss the comparative analysis and two identified causal paths leading to substantial internet control. These are the extractive nature of political institutions and political instability and/or a leadership contest within inclusive institutions. After that, I review the case studies of Kazakhstan and Ukraine that represent both causal paths, respectively. In this regard, the case studies helped deepen the analysis of state control over digital information. Next, contributions to internet control scholarship are provided. The main contribution is the identification and analysis of conditions of state interference with information on the internet. Finally, after reflecting on the internet's effects on democracy, I provide the main limitations of my study.

2. MAIN FINDINGS AND CONTRIBUTIONS OF THE STUDY

2.1. Addressing tactics and conditions of internet control

Internet control, defined as state-based efforts to shape and limit the digital flow of information, has become a recurrent feature of contemporary politics. Many governments across the world seek to control the dissemination of digital information within national borders by various means. My study addressed these means, identifying the following tactics of internet control: censorship and blocking of online content, internet shutdowns, communications surveillance, legislation that expands state's powers in the digital domain, cyberattacks[167], social media manipulation of public opinion, crackdown on internet users and journalists, and dominance of internet infrastructure.

In addition to state-employed tactics of internet control, widely covered by scholars (Sanovich et al 2018, Hussain and Howard 2013), I also addressed a less studied area in the literature: conditions of state control over digital information. The question of what has led states to control information online in the first place, as argued in the literature review (chapter 2), has not been thoroughly examined. This is because many scholars (e.g. Deibert 2015, Singer and Brooking 2018) have taken authoritarianism as the main source of internet control, concluding that it is authoritarian regimes that employ information controls. The main limitation of these conclusions is that

[167] For example, cyberattacks directed against websites and/or individuals (e.g. dissidents). However, as noted in chapters 1 and 4, it is challenging to prove that these attacks were organised by governments.

the same scholars have also provided examples of how democracies interfered with the digital flow of information. As a result, underlying conditions of internet control have not been studied in a comparative manner.

Despite the existing gap in the literature, it was possible to infer that the logic of political survival is the main driver of the substantial usage of information controls (Wagner 2018, Roberts 2018). The chief executives, fearing that the free flow of (negative) information on the internet can empower the political opposition and/or civil society and thus shake the foundations of their (privileged) positions, have opted to internet control. Of note, this incentive to hold onto power takes roots in institutionalist theory that maintains that institutions shape the logic of political survival (Shirk 1993, Bueno de Mesquita et al 2003). Consequently, drawing insights from prior research and the (new) institutionalism, the assumption was that the nature of political institutions – such as extractive and inclusive (Acemoglu and Robinson 2013) – by shaping survival strategies of political leaders, affects the extent to which governments control information online.

I defined political institutions as the formal and informal rules, practices, and processes that influence the domestic balance of political power[168]. Institutions are, in other words, the "rules of the political game" (North 1990) that can be either fairer (more inclusive) or unfairer (more extractive). Overall, three main aspects define the nature of political institutions: constraints on the chief executive's authority, regulation and openness of elections, and specifics and restrictiveness of political participation. Thus, if political leader's powers are institutionally restricted, elections are free and fair, and political participation is open to a large part of society, political institutions are inclusive. On the other hand, if the authority of the chief executive is hardly limited, elections are unfair and unfree, and political participation is restricted whereas the opposition is suppressed, political institutions are extractive.

Following institutional theory (Bueno de Mesquita et al 2003, Acemoglu and Robinson 2013), the initial propositions (hypotheses) were that (1) digital information is substantially controlled within extractive institutions, whereas (2) the extent of internet control is limited under inclusive institutional setups.

I set two research objectives to test (confirm/disconfirm) the outlined propositions and address the research questions[169]. The first objective was to conduct a comparative

[168] This definition is based on definitions of institutions given in institutional research (Lowndes 2018, Acemoglu and Robinson 2013, Bueno de Mesquita et al 2003).

[169] The research questions of the study were as follows. Under what conditions do states control information on the internet? In particular, what is the relationship between political institutions and internet control? Do political institutions affect the extent of internet control? If not, what are other (additional) conditions of state control over digital information, apart from institutions?

analysis of sixty-five countries to identify possible general patterns in internet control. The method used to reach the objective was a qualitative comparative analysis (QCA) (Ragin 2000, 2008). To study the extent of internet control, I identified the following extents of state interference with digital information: limited (0-2 employed tactics), significant (3-4 employed tactics), and extensive (5-6 out of 6 employed tactics[170]); the last two categories are considered substantial internet control. The second research objective was to examine state control of digital information in detail, further scrutinising the main findings drawn from the comparative analysis. For that reason, I studied Kazakhstan, a country with extractive institutions, and Ukraine, a country with inclusive institutions.

Overall, such an approach of conducting the case studies after a comparative study allowed more valid conclusions about underlying conditions of internet control. As a result, I found two main causal paths leading to substantial state control over information on the internet.

2.2. Causal paths of (substantial) internet control

The comparative analysis (chapter 5), a preliminary step of the study, allowed the identification of main patterns in governments' approach to digital information. By studying the interplay between the nature of political institutions (the main proposed condition) and the extent of internet control (the expected outcome), I was able to test and refine the research propositions and address the research questions of the study.

The first proposition that extractive institutional settings lead to substantial internet control was confirmed. With the robust rate of both consistency and coverage, I found that the extractive institutional nature is a sufficient condition of strict control over digital information. Countries with more restricted political participation, unfair executive selection procedures, and unconstrained (or hardly limited) political leaders, experience an intensive usage of information controls. Overall, out of sixty-five analysed countries, twenty-three have extractive political institutions. None of them has a limited extent of internet control.

An important issue related to countries with extractive institutions is that their leaders, due to the lack of electoral legitimacy (Frantz 2018), are sensitive to the free and uncontrollable dissemination of information over the internet. Independent and critical opinions are seen as a potential threat to the political survival of the chief executive. In such a context, digital technologies can empower grassroots movements

[170] These six tactics are: (1) censorship of online content, (2) internet shutdowns, (3) social media manipulation of public opinion, (4) punishment of internet users, (5) legislation that facilitates state control of digital information, and (6) dominance of internet infrastructure and actors.

and anti-government protests by serving as a medium for coordination of efforts. This said, it does not mean that criticism distributed via digital technologies and platforms will necessarily lead to the demolition of extractive settings but that leaders with unconstrained political powers and no (or fragmented) political opposition are sensitive to uncensored and alternative information on the internet to a great extent. As a result, they seek to control it.

Authoritarian leaders, having suppressed the political opposition, fear the internet perceiving it as a democratising medium that can coordinate and strengthen collective action against their regimes. That is why independent online media and investigative journalists are systematically targeted and pressured via raids, closures, court hearings, co-optation, harassment, detainments, and arrests. The free press and free internet are therefore a rare phenomenon in countries with extractive institutions. The comparative analysis of sixty-five countries and the case study of Kazakhstan (chapters 5 and 6) demonstrate the tendency: information distributed over the internet is substantially controlled in countries with extractive political institutions.

On the other hand, I did not find sufficient evidence to confirm the second research proposition as the inclusive nature of institutions is inconsistent with a low number of state-employed information controls. Most countries with inclusive institutional arrangements (twenty-nine out of forty-two) considerably shape and limit the digital flow of information within national borders. As it turned out, constraints on the executive authority, a more competitive political landscape, and fair elections do not necessarily lead to the limited extent of internet control. However, although the proposition was not confirmed, I was able to refine it. Following the comparative analysis, two additional intervening conditions were identified. Countries with inclusive institutions resort to internet control tactics in the wake of (1) political instability caused by regional tensions, street protests, mass demonstrations, and health emergencies, among other things and (2) a forthcoming leadership contest in the form of elections.

The political survival of leaders operating within inclusive institutions is vulnerable to information flows if coupled with a political crisis that can undermine the popularity and authority of incumbents. An intense political situation is like a social “bomb” that can be triggered and fuelled by angry comments and negative information, given that people “turn to the internet as a source of news and information in times of political crisis” (Howard 2010: 10). Even if not a direct threat to their rule, negative information amplified by a political crisis can be very costly to their prestige and popularity. Mishandling of an emergency can cost votes in the following elections. As a result, the number of employed information controls often grows.

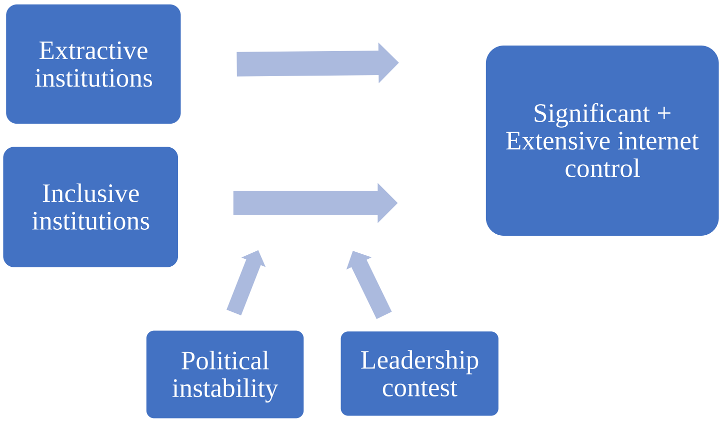
Such a tendency is supported by the findings of this study, which reveal that democratically elected leaders, that is, those operating within inclusive institutions, tend to resort to internet control tactics in the wake of politically unstable events. For instance, as shown in chapter 5, Presidents of South Korea, Brazil, and Ukraine and Prime Ministers of India, Pakistan, and Malaysia – countries with restrained executives, open political participation, and (relatively) democratic elections – encouraged the intolerant attitude toward information on the internet. The inclusive nature of institutions did not stop governments and their agencies from seeking to censor online content, restrict access to websites and applications, repeatedly disrupt internet and mobile services, engage in manipulation of public opinion on social media, enact legislation that expands state powers in the digital domain, and/or penalise internet users and online journalists for their publications on the internet.

The global outbreak of Covid-19 also has affected the extent of internet control in countries with inclusive institutional arrangements. As I discuss in chapter 5, many countries (e.g. India, Hungary, the Philippines, South Africa, Malaysia) have limited the digital flow of information via restrictive legislation and/or a crackdown on internet users and online journalists, ostensibly to fight the distribution of virus-related false information. Overall, half of the UN members restricted the free flow of information due to the coronavirus spread (Reporters without Borders 2020c). However, such behaviour of governments is reasonable if seen through the findings of this study: the implementation of information controls increases as a result of politically volatile events.

The same logic to control information on the internet also plays out at the time of forthcoming presidential or parliamentary elections. Evidently, winning a leadership contest determines whether a chief executive and his coalition will stay in office. Seen in this light, it becomes clear why the number of internet control tactics grows in the lead-up to elections. The comparative analysis showcased that leadership contests in analysed countries were accompanied by strengthening of control over digital information. Prior to and during elections, key political actors (such as governments and political parties) increasingly resort to manipulation of public opinion of potential voters via social media disinformation campaigns and with the help of paid-for commentators and bots. In addition, regular internet users and online journalists are arrested, (opposition) websites are blocked, and online content is censored. As a result, the dissemination of digital information becomes considerably restricted.

All in all, the main rationale of strict internet control is that digital technologies are viewed as an infrastructure for the dissemination of information that can threaten the political survival of executives if not properly controlled. All political leaders wish to stay in office but if leaders presiding over extractive institutions *constantly* seek control over digital information (as they constantly fear mass protests and ouster), leaders operating within inclusive institutions opt to information controls largely *in the wake* of politically unstable situations and forthcoming elections (figure 18).

Figure 18. Model of conditions of internet control[171]



2.3. Case studies: validating conditions of internet control

I conducted the case studies of Kazakhstan and Ukraine (chapters 6 and 7) to further supplement and refine the findings drawn from the comparative analysis and scrutinise the causal relationship between political institutions and internet control. Kazakhstan is a country with the extractive institutional setup and the authoritarian leader and, as a result, comprehensive control over digital information. Ukraine, in contrast, has inclusive institutions and democratically elected executives, yet also a substantial extent of state control of the internet.

Both cases have a different nature of political institutions. In Kazakhstan, only one person, Nursultan Nazarbayev, dominated the political scene being a post-independence president for twenty-eight years and even now, in retirement, still holding a significant range of political powers in the country. In Ukraine, we observe the opposite situation in which political actors fight for the presidential office and the majority in the legislature, unbeknownst who would win. Even after getting to office, the incumbent's position is never stable as two regime changes forced by revolutions in 2004 and 2014 prove the point.

[171] The proposition that inclusive institutions are conducive to limited internet control was not confirmed.

The Ukrainian Parliament, although itself beset by the electoral system and party politics, has nevertheless become independent vis-à-vis the Ukrainian President. The legislative branch has obtained formal powers sufficient to oppose the chief executive as numerous conflicts and compromises between the President, Parliament, and government in the post-independence era demonstrate. Consequently, having a counterweight on the political arena, none of the Ukrainian Presidents, despite the various attempts to consolidate political power – by inter alia weakening the political opposition – has succeeded. In Kazakhstan, on the other hand, the legislature became unable to challenge the Kazakh President already by the mid-1990s. Thereafter, the President only expanded his sphere of influence, eventually amassing almost the unlimited extent of political power.

In stark contrast to Kazakhstan, none of the Ukrainian Presidents has served the (unconstitutional) third term (actually, all but Leonid Kuchma served only one term), none has eliminated the political opposition, and none has acquired full control of the Parliament, government, and/or media. Although President Viktor Yanukovych (in office 2010-2014) commanded a political party with the majority of seats in the Verkhovna Rada (the Parliament) and notoriously tried to suppress the representatives of political opposition[172], he nevertheless had to leave the presidential office unable to contain the mass protests and consequent regime change in 2014. This huge difference between Kazakhstan and Ukraine is due to the established institutional nature of politics: Parliament was subdued by the President in one country while managed to resist the Presidents in another. As a result, we have an authoritarian Kazakhstan and a (comparatively) democratic Ukraine.

Despite the opposite nature of political institutions, both Kazakhstan and Ukraine demonstrate a highly intolerant attitude toward the dissemination of digital information. In Kazakhstan, such an attitude was constantly present: first in regard to the free press (suppressed by the end of the 1990s) and then to the internet (being under the close state supervision since the early 2000s). In Ukraine, substantial control of information on the internet has resulted from an acute political crisis: a regional conflict with Russia in 2014. In line with the findings that countries with inclusive institutions in the wake of political instability resort to internet control tactics (chapter 5), the case of Ukraine further strengthens the results of the comparative analysis.

In both Kazakhstan and Ukraine, government agencies, empowered by restrictive legislation, censor online content and block access to websites. The Kazakh

[172] For example, in 2011, Yulia Tymoshenko, the oppositionist who came second in the 2010 presidential elections, was arrested and sentenced to seven years (Sakwa 2016: 56-57).

authorities began employing these tactics in the early 2000s when the use of the internet began growing in the country. The Ukrainian government, though, started in 2014 – shortly after Russia annexed the Crimean Peninsula; previously, there was limited (occasional) control over the digital flow of information. In addition, state agencies and political actors, including presidents, in both Kazakhstan and Ukraine resort to social media manipulation of public opinion by organising and financing armies of paid-for trolls and commentators. The latter, bombarding national cyberspace with pro-government messages, shapes political narratives in the country. Censorship through noise, in other words, is present in both countries.

The repeated persecution and prosecution of internet users and journalists is also a common feature of internet control in both Kazakhstan and Ukraine. The detainment and prison sentence (usually, between three and five years) can follow even commenting on and reposting of online content on social media platforms. Unsurprisingly, both governments have substantially restricted the free flow of digital information within national borders as the goal "to produce an environment of fear and strategies of deterrence that aim to control and contain political debate" (Lacy and Mookherjee 2020: 300) was subsequently achieved. Also, Security Services in both countries acquired sufficient capacities for surveillance of domestic communication networks. Additionally, the Ukrainian politicians, including then-incumbent President Petro Poroshenko and his successor Volodymyr Zelensky, did not refrain from shaping the narrative in cyberspace in the lead-up to a leadership contest.

Although the extent of internet control is similar in both countries, there are a few distinctions. It is of note that the methodical employment of information controls in Kazakhstan has begun since the early 2000s (when the internet emerged in the country) while in Ukraine – since 2014 (when the conflict with Russia intensified). Another difference between the two states is that the Kazakh regime also repeatedly disrupts internet and mobile access in some regions or the whole country in the wake of anti-government protests, demonstrations, or unrests. Furthermore, Kazakhstan's government owns the main internet provider whereas in Ukraine internet operators are private. Yet, Ukrainian state agencies managed to influence private actors via restrictive legislation, subsequently dominating the digital domain in the country.

In brief, internet control is extensive in both countries. In the case of Kazakhstan, the main condition of state control over digital information is the extractive nature of political institutions. In the case of Ukraine, the main condition of substantial internet control is political instability emanating from the 2014 overt conflict with Russia. In addition, information controls were applied at the time of the 2019 presidential election in Ukraine. Thus, both case studies, following the comparative analysis, validate the findings on conditions of internet control. All these, as I discuss in the following sub-section, supplement the scholarly literature.

Last but not least, based on numerous examples, cases, and findings discussed in this thesis, it can be said that state-employed information controls will stay with us on a global as well as regional scale in the observable future. Moreover, there is no doubt that internet control will further evolve as more and more countries, including democratic ones, turn to it. In other words, internet disruptions, online mobs of bots and paid commentators, encroachment on internet users and journalists, restrictive digital laws, and other attributes of state control over the digital domain are becoming a new normal in our life.

2.4. Supplementing the literature on internet control

It is no exaggeration to suggest that the findings of the comparative analysis and case studies help to broaden the main narrative of internet control studies. As discussed in the literature review (chapter 2), many scholars (e.g. Deibert 2015, Singer and Brooking 2018, Roberts 2018) have concluded that it is predominantly authoritarian regimes that control the internet via the implementation of numerous information controls[173]. Recent studies (e.g. Rosenbach and Mansted 2019, Kendall-Taylor et al 2020) have continued this tendency, arriving at similar conclusions. According to the aforementioned scholars, democratic states are assumed to not control the dissemination of digital information.

However, the study of sixty-five countries demonstrated that many democracies (countries with inclusive political institutions) employ internet control tactics almost on the same scale[174] as authoritarian regimes (countries with extractive political institutions). For instance, India – the largest democracy in the world – indiscriminately employs various tactics of internet control such as censorship of online content and the blocking of websites and applications, manipulation of public opinion via social media, methodical arrests of digital users and journalists, and adoption of restrictive legislation. Most importantly, India is also the world leader in terms of internet shutdowns. Even authoritarian regimes disconnect the internet and communications less often than India. Such an approach is, however, not an exception but rather a tendency as India is not the only democratic state that exercises substantial control over digital information. Overall, as identified in this study (chapter 5), there are at least twenty-nine (out of forty-two)

[173] This conclusion, as I discuss in the literature review, is contradictory as the same scholars have also acknowledged practices of internet control in democracies.

[174] In the previous chapters, following the narrative of internet control scholars, I suggested that the extent of internet control in democracies appears to be selective, that is, limited.

countries with inclusive institutions that continuously implement information controls within national borders.

In other words, borrowing Roberts' (2018) terminology, I found that democracies have engaged in internet control through the "fear", "friction", and "flooding" mechanisms. Alternatively, using the vocabulary of Deibert (2015), these democracies have employed the first, second, and third generations of internet control. Applying the classification of Singer and Brooking (2018), democratic countries resort to the "control of the signal", "control of the body", "control the spirit", and "daze and confuse" tactics. Yet, in contrast to Roberts', Deibert's, and Singer and Brooking's accounts (discussed in chapter 2), all these (twenty-nine) countries with significant or extensive control over the digital flow of information are not authoritarian.

Specifics of internet control appeared to be more nuanced. It is thus inaccurate to analyse control of digital information as the modus operandi of exclusively authoritarians[175]. This is because many democratically elected leaders tolerate the application of information controls often as regularly as their non-democratic counterparts. Consequently, the existing approach in the literature significantly reduces the scope and focus of internet control studies. In this context, it is probably more accurate to consider the issue of internet control as an "authoritarian practice" (Glasius 2018). The main advantage of the latter concept is its analytical flexibility. The authoritarian practice is not bound to a particular location or nation-state (as assumed by the commonly used terms such as "authoritarian regimes/countries") and can be, in turn, attributed to authoritarian as well as democratic states.

In other words, the common wisdom about internet control and the "authoritarian resurgence", "authoritarian cyberspace", and "digital authoritarianism" can be misleading. However, rephrasing these terms to the "resurgence of authoritarian practices", "authoritarian practices in cyberspace" and "digital authoritarian practices" would be more accurate as now we do not mean only authoritarian regimes such as China, Iran, or Russia (the typical suspects of many pundits) but also non-authoritarian governments such as South Korea, India, or Ukraine – countries that are usually absent in internet control studies.

All in all, the comparative analysis followed by two case studies (chapters 5-7) supplements the literature on internet control, broadening the narrow scope of the extant research. In addition to authoritarian countries – the common reference of scholars – this

[175] As noted in Chapter 2, some authors (e.g. Greenwald 2014, Bradshaw and Howard 2017, Hintz et al 2019) study practices of information control in democracies. However, their focus is mainly on one of tactics such disinformation and propaganda on social media or covert mass surveillance and its implications for human rights. Rakhmetov and Valeriano (2020) discuss the need to extend the study of internet control.

study also focused on democracies, which are by default not considered as initiators of internet control. Such an approach was novel, given that there have been no comparative analyses of internet control in both autocracies and democracies in recent years. The study, as a result, offered a broader and deeper perspective of the dynamics of state control over digital information, acknowledging that internet control is also becoming a recurring problem in democratic states. I demonstrated that democracies should be accounted for in studies of the internet.

Also, as noted in chapter 4, scholarship in both English and Russian languages tends to neglect internet politics in the post-Soviet region. Previously, Deibert et al (2010) studied specifics of cyberspace control in the non-Baltic post-Soviet countries. Currently, scholars largely focus on Russia and its aggressive behaviour in the cyber and information space internationally and domestically[176]. Meanwhile, the case studies conducted in this thesis broaden the scholarly literature by unfolding specifics of internet control in the former Soviet Union republics. The comprehensive analysis of different aspects of internet control in both Ukraine and Kazakhstan helped to understand how and to what extent the local authorities censor online content, block access to websites, disconnect the internet (only Kazakhstan), adopt restrictive legislation, arrest digital users and journalists, are capable of communications surveillance, and dominate the internet infrastructure and actors. In this regard, the case studies of internet politics in Ukraine and Kazakhstan also demonstrate that the former Soviet Union states are well-versed in controlling information online. Consequently, the post-Soviet region should secure more attention and scrutiny from scholars.

In addition to including democratic (and post-Soviet) countries in the analysis, this study also offered two main explanations for government-employed information controls (discussed in the previous sub-sections). In this regard, the findings of the study contribute to the scholarly literature by providing a better understanding of underlying conditions of internet control. As noted in chapter 5, many scholars present an agency-centred account of why some (democratic) countries experience a repeated usage of internet control tactics. If the issue is seen against the perspective of one or few cases within a limited time frame and without a comparative overview, the explanation that the number of information controls increases as a result of the advent of authoritarianism-prone leaders might sound convincing.

For instance, Ben-Ghiat (2020) argues that some democratic governments have resorted to tactics of internet control (as one of the tools to fight the coronavirus outbreak)

[176] One of the exceptions is the annual reports on internet freedom in ten post-Soviet countries by Freedom House.

because they are ruled by autocratic leaders. According to the author, the enactment of restrictive legislation, pressure on journalists, or the spread of misinformation in Hungary, the US, Brazil, and India are a result of actions of authoritarians (such as Viktor Orban, Donald Trump, Jair Bolsonaro, and Narendra Modi, respectively). Likewise, extensive control over digital information in India via regular internet shutdowns, a crackdown on the media and (online) journalists, and filtering of online content has been attributed to the authoritarian premiership of Modi (Gettleman et al 2019, Goel and Gettleman 2020). Thus, following the aforementioned authors – and despite their tautological assumption of democratic governments being ruled by the authoritarians – if there were democrats in power, then there would be no internet control.

However, as demonstrated in chapter 5, in many cases the substantial extent of internet control was still present before so-called "autocratic" political leaders came to power and after they left office. For example, according to the comparative analysis, Brazil experienced a significant extent of internet control (between 2016-2018) before Bolsonaro began his presidency in January 2019. The same situation is with Modi, who became the Indian Prime Minister in 2014. Prior to Modi's advent, Indian agencies systematically censored online content and pressured (online) journalists (Deibert et al 2012b). South Korea is another example of the continuous employment of information controls, irrespective of who is in power. As early as 2006, during the presidency of Roh Moo-hyun (2003-2008), digital materials in South Korea were censored whereas regular users were arrested for anti-state content (Deibert et al 2008). These did not change during the time of Roh's successors, Lee Myung-bak (2008-2013), Park Geun-hye (2013-2017), and Moon Jae-in (since 2017).

It is thus possible to conclude that although political actors are undoubtedly important, the agency-based account lacks the explanatory power. Such a line of thinking appears to be flawed as this study of internet control demonstrates that (democratically elected) leaders might come and leave but the "necessity" to employ various tactics to affect the dissemination of digital information is still in place, regardless of who is currently in power. This is because the structural factors in the form of (1) extractive political institutions and (2) political instability along with forthcoming leadership contests play a more determinative role in internet control. As such, this thesis attempted to engage with the literature and bring new insights into the issue of internet control. In the following sections, I reflect on the internet's effects on democracy and discuss the main limitations of my study.

2.5. On the internet and democracy

Twitter's permanent ban of Donald Trump in January 2021 was one of the latest events that has revitalised the old debate about the new technologies' implications for democracy (Conger and Isaac 2021). As argued in Chapter 2, there have long been discussions and polarising views with regard to the impact of new technologies on democracy. As such, the advent of the internet has caused a stir among scholars, journalists, and officials, creating two broad intellectual camps: so-called cyber-optimists and cyber-pessimists. The ban of Trump's Twitter account has only contributed to these divisions. Some supported the ban, holding that Trump groundlessly rejected the results of the democratic elections and encouraged his supporters to commit unlawful actions (Frier 2021). Others were against the ban, contending that arbitrarily censorship by a tech giant is not good for a democratic process (Clayton 2021, Teachout 2021).

It is, however, of note that concerns about the possible impact of new technology on society, government, and politics have accompanied technological development long before the advent of social media and the internet. This was not though expressed in utopian-dystopian thoughts and empirical studies (as with regard to the internet) but in then-political leaders' actions, who distrusted new information technologies from the very beginning, limiting their dissemination within national borders (Chapter 3). The internet, after becoming a mass product, also has not become an exception, slowly but inevitably finding itself under state regulation. As a result, the internet, due to its (perceived) liberating and empowering potential, was and in many regions is still treated with suspicion being under extensive government's control, as the case studies and numerous examples in this thesis demonstrated.

In addition, the growing role and political influence of tech corporations also contributed to the debate about the interplay between technologies and democracy. Currently, the tech companies like Amazon, Google, Facebook, and Apple have become extremely powerful having swept the twenty-century dominance of oil companies and banks. Tech entrepreneurs are among the richest people on the planet whereas the tech industry is the best performing in the world (Cai 2021). Moreover, during the Covid-19 pandemic, while other businesses suffered a great loss, tech companies managed to increase their market value, gaining even more political and economic influence (The Wall Street Journal 2021). As a result of such a rise of big tech, which is ruled hierarchically from top to down, questions about their effects on democracy eventually followed suit (Runciman 2018, Moore 2018). The main concern is that hardly controlled but highly rich and powerful tech corporations inflict damage to a democratic system through the spread of fake news and disinformation on their digital platforms. In addition, their assistance to state authorities (for example, in the US) to conduct mass surveillance of communication networks also undermines the democratic process (Foroohar 2019). As such, big tech is currently on the radar of pundits, journalists, officials, and regulators.

Yet, despite the ongoing debate (and recent developments in the world) about the internet's impact on democracy, what this thesis has demonstrated is that democracies themselves do not refrain from imposing controls on the internet. Many democratic governments, like their authoritarian counterparts, censor online content, block websites and applications, arrest digital users and journalists, pass restrictive internet legislation, finance mobs of trolls and bots to manipulate public opinion on social media, or disrupt internet connection in order to control the digital domain.

The risks for democracy are then twofold: the rising reach and powers of tech corporations ruled by unelected CEOs and the increasing extent of control over the internet in democracies themselves. All these only worsen and complicate the existing perception of the current interplay between the internet and democracy. Yet, as this thesis posits, scholars first need to shift their research focus and also concentrate on how democracies and hybrid regimes across the world – in addition to authoritarian states – control the internet.

3. LIMITATIONS OF THE STUDY AND SUGGESTIONS FOR FUTURE RESEARCH

The comparative analysis included sixty-five countries that altogether represented almost 90% of world internet users. However, the number of countries can be increased. Patterns of governments' behaviour identified in a larger sample can strengthen the findings. In this regard, the limited number of analysed countries is one of the limitations of this study. The main reason to focus on only sixty-five countries was that the comparative analysis was a preliminary step in the study of conditions of internet control[177].

Another possible weakness of the study can be Polity IV data collected to measure the nature of political institutions. Although I argued that Polity IV, compared to other sources, is the most relevant to study research variables under my consideration (chapter 4), data used for a large number of countries cannot be completely accurate. Relatedly, although the method of qualitative comparative analysis (QCA) helps to explore causal conditions leading to a particular outcome, it does not allow in-depth analysis of casual paths. That is, the QCA is a great tool for a preliminary study of a research problem but additional case studies are needed to thoroughly address the research question of the study. That is why, in a comparative analysis of global dynamics

[177] Also, data collection for a very large sample might be challenging as, apart from Freedom House, no organisations systematically report on practices of internet control across the world.

of internet control, in which Polity IV data and the QCA method were used, I preferred a more cautious language with regard to the causal interplay between political institutions and internet control, emphasising that confirmed and refined propositions are robust tendencies rather than iron laws. To mitigate the potential limitations in the number of and data on analysed countries as well as the method, I resorted to the (qualitative) case studies[178].

Consequently, I conducted two case studies (Kazakhstan and Ukraine). The case study of Kazakhstan represented a common approach of authoritarian regimes to information on the internet, whereas the deviant case of Ukraine served to illustrate how more democratic states also control information online. Nevertheless, in-depth studies of other deviant cases with inclusive institutions but substantial state control over digital information – for example, India or South Korea – also can contribute to our understanding of conditions of internet control. In this regard, the lack of both expertise in respective languages and knowledge in (South Asian and East Asian) regional politics did not allow for in-depth analysis of the cases. The deviant cases, however, can be studied within future research.

In addition, to further understand specifics of internet control, the focus can also be made on non-state actors such as international organisations (e.g. the Internet Corporation for Assigned Names and Numbers, the International Telecommunication Union) and private technological companies (such as Facebook, Google, Twitter). Private companies play an important role in the first-hand implementation or non-implementation of information controls. Analysis of relations between states, private sector, and NGOs, by adding an extra layer, will help unravel peculiarities of internet regulation on a micro-level. Although I focused on domestic private actors (such as internet service providers), I did not thoroughly study the role of international companies. This is because the main focus was on state-employed tactics of internet control within national borders.

Finally, given that the initial emphasis was on studying political institutions and their expected causal relationship with the extent of internet control, less attention was eventually paid to the phenomena of political instability as an additional condition that also affects the behaviour of political entities in the digital domain. In this regard, future research on the (causal) interplay between political crises and state-employed information controls will help verify the findings of this study, further advancing our understanding of internet control.

[178] In this regard, the case studies strengthened the findings drawn from the comparative analysis.

All in all, subsequent research should expand the scope and include democratic states in the analysis of tactics and conditions of internet control. As this study argued, the focus only on authoritarian countries, however precise the details of state control over digital information can be, offers a partial perspective of the issue under consideration. This study demonstrated that it is not just the authoritarians (small-coalition leaders) who control information on the internet. Their democratic counterparts (large-coalition leaders) also often do not refrain from considerable control of the online flow of information, specifically in the wake of political instability and in the lead-up to a forthcoming leadership contest.

APPENDIX 1

Appendix 1. Implementation of internet control tactics during the coverage period (2016-2018) in 65 countries

(E = tactic was employed; N/E = tactic was not employed)

N	Country	Censorship of online content	Internet shutdown	Social media manipulation	Crackdown on internet users	Restrictive legislation	Dominance of internet infrastructure	Total number of employed tactics
1	Angola	N/E	N/E	E	E	E	N/E	**3**
2	Argentina	N/E	N/E	E	E	E	N/E	**3**
3	Armenia	E	N/E	E	N/E	N/E	N/E	**2**
4	Australia	N/E	N/E	E	N/E	E	N/E	**2**
5	Azerbaijan	E	E	E	E	E	E	**6**
6	Bahrain	E	E	E	E	E	E	**6**
7	Bangladesh	E	E	N/E	E	E	N/E	**4**
8	Belarus	E	E	E	E	E	E	**6**
9	Brazil	E	N/E	E	E	E	N/E	**4**
10	Cambodia	N/E	N/E	E	E	E	N/E	**3**
11	Canada	N/E	N/E	N/E	N/E	E	N/E	**1**
12	China	E	E	E	E	E	E	**6**
13	Colombia	N/E	N/E	E	N/E	N/E	N/E	**1**
14	Cuba	E	N/E	E	E	N/E	E	**4**
15	Ecuador	N/E	N/E	E	E	E	N/E	**3**
16	Egypt	E	E	E	E	E	E	**6**
17	Estonia	N/E	N/E	N/E	N/E	N/E	N/E	**0**
18	Ethiopia	E	E	E	E	E	E	**6**
19	France	N/E	N/E	N/E	E	E	N/E	**2**
20	Georgia	E	N/E	N/E	E	N/E	N/E	**2**
21	Germany	N/E	N/E	E	E	E	N/E	**3**
22	Hungary	N/E	N/E	E	E	E	N/E	**3**
23	Iceland	N/E	N/E	N/E	N/E	N/E	N/E	**0**
24	India	E	E	E	E	E	N/E	**5**
25	Indonesia	E	E	E	E	E	N/E	**5**
26	Iran	E	E	E	E	E	E	**6**
27	Italy	N/E	N/E	E	N/E	E	N/E	**2**
28	Japan	N/E	N/E	E	N/E	N/E	N/E	**1**
29	Jordan	E	N/E	N/E	E	E	N/E	**3**
30	Kazakhstan	E	E	E	E	E	E	**6**
31	Kenya	N/E	N/E	E	E	E	N/E	**3**
32	Kyrgyzstan	N/E	N/E	E	E	N/E	E	**3**
33	Lebanon	E	E	N/E	E	N/E	E	**4**
34	Libya	E	E	N/E	E	N/E	E	**4**
35	Malawi	N/E	N/E	N/E	E	E	N/E	**2**
36	Malaysia	E	N/E	E	E	E	N/E	**4**

37	Mexico	N/E	N/E	E	E	E	N/E	**3**
38	Morocco	E	N/E	N/E	E	N/E	E	**3**
39	Myanmar	N/E	N/E	E	E	E	E	**4**
40	Nigeria	E	N/E	E	E	E	N/E	**4**
41	North Sudan	N/E	N/E	E	E	E	N/E	**3**
42	Pakistan	E	E	E	E	E	E	**6**
43	Philippines	N/E	E	E	E	N/E	N/E	**3**
44	Russia	E	N/E	E	E	E	E	**5**
45	Rwanda	E	N/E	E	E	E	N/E	**4**
46	Saudi Arabia	E	N/E	E	E	E	E	**5**
47	Singapore	N/E	N/E	E	E	E	E	**4**
48	South Africa	N/E	N/E	E	N/E	E	N/E	**2**
49	South Korea	E	N/E	E	E	E	N/E	**4**
50	Sri Lanka	E	E	N/E	E	N/E	E	**4**
51	Syria	E	N/E	E	E	N/E	E	**4**
52	Thailand	E	N/E	E	E	E	E	**5**
53	The Gambia	N/E	N/E	N/E	E	N/E	E	**2**
54	Tunisia	N/E	N/E	N/E	E	E	E	**3**
55	Turkey	E	E	E	E	E	N/E	**5**
56	Uganda	E	N/E	E	E	E	N/E	**4**
57	Ukraine	E	N/E	E	E	E	E	**5**
58	United Arab Emirates	E	N/E	E	E	E	E	**5**
59	United Kingdom	N/E	N/E	E	E	E	N/E	**3**
60	United States	N/E	N/E	E	E	E	N/E	**3**
61	Uzbekistan	E	N/E	E	E	E	E	**5**
62	Venezuela	E	N/E	E	E	E	E	**5**
63	Vietnam	E	E	E	E	E	E	**6**
64	Zambia	N/E	E	N/E	E	E	N/E	**3**
65	Zimbabwe	E	N/E	E	E	E	N/E	**4**

BIBLIOGRAPHY

Acemoglu, D. and Robinson, J. A. (2013). *Why Nations Fail: The Origins of Power, Prosperity and Poverty.* London: Profile Books.

Acemoglu, D. and Robinson, J. A. (2019). *The Narrow Corridor: States, Societies and the Fate of Liberty*. London: Penguin Books.

Adil Soz (2019). Statistika Del po Vozbuzhdeniyu Socialnoi, Natsionalnoi, Rodovoi, Rasovoi, Soslovnoi ili Religioznoi Rozni za 2014-2018. [Statistics of Cases for Inciting of Social, National, Tribal, Racial, Class or Religious Hatred between 2014 and 2018]. *Adil Soz*, 19 July. Available at: http://www.adilsoz.kz/politcor/show/id/257 (Accessed 27 April 2020).

Adil Soz (2020). Situatsiya so Svobodoi Slova v Kazahstane v 2019. Analiticheskii Doklad. [Situation with the Freedom of Speech in Kazakhstan in 2019. Analytical Report]. *Adil Soz*, 17 February. Available at: http://www.adilsoz.kz/politcor/show/id/283 (Accessed 27 April 2020).

Alimonti, V. (2020). Brazil's Fake News Bill Would Dismantle Crucial Rights Online and Is on a Fast Track to Become Law. *Electronic Frontier Foundation*, 24 June. Available at: https://www.eff.org/deeplinks/2020/06/current-brazils-fake-news-bill-would-dismantle-crucial-rights-online-and-fast (Accessed 1 July 2020).

Aljazeera (2020). Bangladesh Cartoonist, Writer Charged For Anti-Government Posts. *Aljazeera*, 7 May. Available at: https://www.aljazeera.com/news/2020/05/bangladesh-cartoonist-writer-charged-anti-government-posts-200507102957266.html (Accessed 30 June 2020).

Ames, B. (1987). *Political Survival: Politicians and Public Policy in Latin America*. Berkeley: University of California Press.

Amnesty International (2015). Ukraine's Spate of Suspicious Deaths Must Be Followed by Credible Investigations. *Amnesty International*, 17 April. Available at: https://www.amnesty.org/en/latest/news/2015/04/ukraine-suspicious-deaths-need-credible-investigations/ (Accessed 9 April 2020).

Amnesty International (2017a). Kazakhstan: Think Before You Post: Closing Down Social Media Space in Kazakhstan. *Amnesty International*, 9 February. Available at: https://www.amnesty.org/en/documents/eur57/5644/2017/en/ (Accessed 27 December 2018).

Amnesty International (2017b). Kazakhstan: Further Information: Prisoners of Conscience’s Conviction Upheld: Maks Bokaev And Talgat Ayan. *Amnesty International*, 31 January. Available at: https://www.amnesty.org/en/documents/eur57/5599/2017/en/ (Accessed 26 April 2020).

Amnesty International (2020). Hungary: Government Must Not Be Granted Unlimited Powers by New Covid19 Law. *Amnesty International,* 27 March. Available at: https://www.amnesty.org/en/latest/news/2020/03/hungary-government-must-not-be-granted-unlimited-powers-by-new-covid19-law/ (Accessed 30 June 2020).

Anoshin, A. (2019). Kirill Vyshinskii: Politicheskii Uznik, Kotoryi Pobedil. [Kirill Vyshinsky: A Political Prisoner Who Won]. *Ukraina*, 7 September. Available at: https://ukraina.ru/exclusive/20190907/1024894796.html (Accessed 10 April 2020).

Anstead, N. and Chadwick, A. (2009). Parties, Election Campaigning, and the Internet: Toward a Comparative Institutional Approach. In: Chadwick, A. and Howard, P. N. (ed), *The Routledge Handbook of Internet Politics*. London: Routledge, 56-71.

Apuzzo, M. and LaFraniere S. (2018). 13 Russians Indicted as Mueller Reveals Effort to Aid Trump Campaign. *New York Times*, 16 February. Available at: https://www.nytimes.com/2018/02/16/us/politics/russians-indicted-mueller-election-interference.html (Accessed 28 June 2020).

Arguments and Facts (2017). SBU: Sud Vynes Obvineniya 37 Administratoram Grupp v Sotssetyah. [SBU: Court Charged 37 Administrators of Groups on Social Media]. *Arguments and Facts*, 30 October. Available at: https://aif.ua/society/law/sbu_sud_vynes_obvineniya_37_administratoram_grupp_v_socsetyah (Accessed 10 April 2020).

Awasthi, P. (2020). Stop Criminalising Free Speech, Protect Journalism: PUCL. *The Week*, 23 June. Available at: https://www.theweek.in/news/india/2020/06/23/stop-criminalising-free-speech-protect-journalism-pucl.html (Accessed 3 July 2020).

Baituova, G. and Atoyanz-Larina, V. (2016). Kazak State Tightens Grip on Internet. *IWPR Central Asia*, 15 February. Available at: https://iwpr.net/global-voices/kazak-state-tightens-grip-internet (Accessed 26 April 2020).

Bakhteev, B. (2019). Pochemu “Porohoboty”?. [Why “Porokhobots”?]. *Novoe Vremya*, 17 April. Available at: https://nv.ua/opinion/pochemu-porohoboty-50017048.html (Accessed 15 April 2020).

Bannikov, P. and Li, V. (2019). Ferma Vozhdya: Kto Upravlyaet Nurbotami i Nurnyashkami. [The Farm of the Chief: Who Rules Nurbots and Nursweethearts]. *Factcheck KZ*, 2 April. Available at: https://factcheck.kz/glavnoe/ferma-vozhdya-kto-upravlyaet-nurbotami-i-nurnyashkami/ (Accessed 27 April 2020).

Barlow, J. P. (1996). A Declaration of the Independence of Cyberspace*. Electronic Frontier Foundation.* Available at: https://www.eff.org/cyberspace-independence (Accessed 14 June 14, 2020).

Bastians, D., Gettleman, J., and Schultz, K. (2019). Blasts Targeting Christians Kill Hundreds in Sri Lanka. *New Your Times*, 21 April. https://www.nytimes.com/2019/04/21/world/asia/sri-lanka-bombings.html (Accessed 19 February 2020).

BBC (2014). Polls Test South Korea Mood After Ferry Disaster. *BBC*, 5 June. Available at: https://www.bbc.co.uk/news/world-asia-27694776 (Accessed 20 February 2020).

BBC (2015). Nazarbaev Obyavil Dosrochnye Vybory Prezidenta. [Nazarbayev Declared Extraordinary Elections of the President]. *BBC*, 25 February. Available at: https://www.bbc.com/russian/international/2015/02/150225_kazakhstan_elections (Accessed 27 April 2020).

BBC (2019). Russia Internet: Law Introducing New Controls Comes into Force. *BBC*, 1 November. Available at: https://www.bbc.co.uk/news/world-europe-50259597 (Accessed 26 June 2020).

Bekbasova, A. (2016). Blogery Prosyat Deneg u Gosudarstva. [Bloggers Ask Money from the Government]. *Ratel*, 3 June. Available at:

http://www.ratel.kz/raw/blogery_prosjat_deneg_u_gosudarstva (Accessed 27 April 2020).

Ben-Ghiat, R. (2020). COVID-19 Tempts Would-Be Authoritarians. *Foreign Affairs*, 5 May. Available at: https://www.foreignaffairs.com/articles/world/2020-05-05/covid-19-tempts-would-be-authoritarians (Accessed 5 July 2020).

Benkler, Y. (2011). Free Irresponsible Press: Wikileaks and the Battle over the Soul of the Networked Fourth Estate. *Harvard Civil Rights-Civil Liberties Law Review*, 46/2: 311-398.

Benkler, Y., Faris, R. and Roberts, H. (2018). *Network Propaganda: Manipulation, Disinformation, and Radicalization in American Politics.* Oxford: Oxford University Press.

Berman, S. (2019). *Democracy and Dictatorship in Europe: from the Ancien Régime to the Present Day*. New York: Oxford University Press.

Bimber, B. (1998). The Internet and Political Transformation: Populism, Community, and Accelerated Pluralism. *Polity*, 31/1: 133-160.

Bishchuk, V. (2011). E Vakansiya: Internet-Ukrainofob na Pivstavki. [There is a Vacancy: A Part-time Internet-Ukrainophobe]. *Credo Digest*, 19 August. Available at: https://credo.pro/2011/08/49432 (Accessed 10 April 2020).

Bloodworth, J. (2015). Katie Hopkins' Views Are Now Considered Matters for Law Enforcement, and It Is Utterly Terrifying. *The Independent*, 1 January. Available at: https://www.independent.co.uk/voices/comment/katie-hopkins-views-are-now-considered-matters-for-law-enforcement-and-it-is-utterly-terrifying-9953339.html (Accessed 22 February 2020).

Bobritsky, D. (2018). Dengi Protiv Deneg. Bitva za Million. Kak Timoshenko i Poroshenko ispolzuyut Facebook. [Money vs Money. Struggle for a Million. How Tymoshenko and Poroshenko Use Facebook]. *Liga.net*, 26 June. Available at: https://www.liga.net/politics/articles/bitva-za-million-kak-timoshenko-i-poroshenko-ispolzuyut-facebook (Accessed 16 April 2020).

Bohdanova, T. and Lokot, T. (2014). Ukraine's New Law Cracks Down on Free Speech, Protests and The Internet. *Global Voices*, 18 January. Available at: https://www.pri.org/stories/2014-01-18/ukraines-new-law-cracks-down-free-speech-protests-and-internet (Accessed 7 April 2020).

Bolshakov, S. and Solovyov, V. (2007). Nursultan Nazarbaev Popalsya v Set. [Nursultan Nazarbayev Was Caught into Web]. *Kommersant*, 25 October. Available at: https://www.kommersant.ru/doc/818581 (Accessed 25 April 2020).

Borisov, N. (2018). *Prezidentstvo na Postsovetskom Prostranstve: Protsessy Genezisa i Transformatsii.* [*Presidency in the Post-Soviet Space: Processes of Genesis and Transformation*]. Moscow: The Russian State University for the Humanities.

Bradshaw, S. and Howard, P. N. (2017). *Troops, Trolls, and Troublemakers: A Global Inventory of Organized Social Media Manipulation*. Oxford: Oxford Internet Institute. Working Paper.

Bradshaw, S. and Howard, P. N. (2018). *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. COMRPOP Working Paper Series.

Bradshaw, S. and Howard, P. N. (2019). *The Global Disinformation Order: 2019 Global Inventory of Organised Social Media Manipulation.* COMRPOP Working Paper Series.

Bremmer, I. (2020). What Happens Next as Pakistan Lurches from Crisis to Crisis. *Time*, 20 June. Available at: https://time.com/5856416/what-happens-next-as-pakistan-lurches-from-crisis-to-crisis/ (Accessed 5 July 2020).

Briggs, A. and Burke, P. (2017). *A Social History of the Media: from Gutenberg to the Internet.* 3rd ed. Cambridge: Polity Press.

Brown, I. and Marsden, C. T. (2013). *Regulating Code: Good Governance and Better Regulation in the Information Age*. Cambridge, MA: MIT Press

Browning, G. (1996). *Electronic Democracy: Using the Internet to Influence American Politics.* Austin: Pemberton Press.

Bueno De Mesquita, B., Smith, A., Siverson, R. M. and Morrow. J. D. (2003). *The Logic of Political Survival*. Cambridge, MA: MIT Press.

Bueno De Mesquita, B. and Smith, A. (2011). *The Dictator's Handbook: Why Bad Behavior Is Almost Always Good Politics*. New York: PublicAffairs.

Burdin, V. (2018). Vse, Chto Nuzhno Znat Ob Obyazatelnoi Registratsii Sotovyh Telefonov v Kazahstane. [All You Need to Know About the Mandatory Registration of Mobile Phones in Kazakhstan]. *Forbes Kazakhstan*, 19 September. Available at: https://forbes.kz/process/technologies/vse_chto_nujno_znat_ob_obyazatelnoy_registratsii_sotovyih_telefonov_v_kazahstane/ (Accessed 15 October 2020).

Bushuyev, M. (2009). Neglasnaya Blokirovka LiveJournal i Oppozitsionnyh Saitov v Kazahstane Prodolzhaetsya. [Unofficial Blocking of LiveJournal and Opposition Sites in Kazakhstan Continues]. *DW*, 16 February. Available at: https://www.dw.com/ru/негласная-блокировка-liveJournal-и-оппозиционных-сайтов-в-казахстане-продолжается/a-4034874 (Accessed 26 April 2020).

Cai, K. (2021). Here Are The Richest Tech Billionaires In 2021. *Forbes*, 6 April. Available at: https://www.forbes.com/sites/kenrickcai/2021/04/06/here-are-the-richest-tech-billionaires-in-2021/?sh=225d82294d70 (Accessed 4 July 2021).

Castells, M. (2015) *Networks of Outrage and Hope: Social Movements in the Internet Age.* Cambridge: Polity Press.

Cavelty, M. D. (2009). National Security and the Internet: Distributed Security through Distributed Responsibility. *International Studies Review*, 11: 214-218.

Channel 24 (2017). SBU Provodit Obysk v Redaktsii "Strana.ua" i v Kvartirah Zhurnalistov. [SBU Searches the Office of "Strana.ua" and Flats of Journalists]. *Channel 24*, 9 August. Available at: https://kyiv.24tv.ua/ru/sbu_provodit_obysk_v_redakcii_stranaua_i_v_kvartirah_zhurnalistov_n850788 (Accessed 10 April 2020).

Chase-Lubitz, J. (2017). South Korean Spy Agency Admits to Meddling in 2012 Election. *Foreign Policy*, 4 August. Available at: https://foreignpolicy.com/2017/08/04/south-korean-spy-agency-admits-to-meddling-in-2012-election/ (Accessed 20 February 2020).

Chaturvedi, S. (2019). *I Am a Troll: Inside the Secret World of the BJP's Digital Army*. New Delhi: Juggernaut Publication.

Chebotarev, A. (2015). *Politicheskaya Mysl Suverennogo Kazahstana: Dinamika, Idei, Otsenki.* [*Political Thought of Sovereign Kazakhstan: The Dynamics, Ideas, Assessments*]. Astana: IWEP.

Chen, A. (2015). The Agency. *New York Times*, 2 June. Available at: https://www.nytimes.com/2015/06/07/magazine/the-agency.html (Accessed 28 June 2020).

Chernyavskiy, A. (2019). Kak Vlasti Kazahstana Pytayutsya Prikryt Svoi Proval s Vnedreniem Sertifikata. [How the Kazakh Authorities Are Trying to Conceal Their Failure to Implement the Certificate]. *Habr*, 8 August. Available at: https://habr.com/ru/post/462969/ (Accessed 18 May 2020).

Choe, S-H. (2014). South Korean Leader Accepts Resignation of Premier Over Ferry Disaster. *New York Times*, 27 April. Available at: https://www.nytimes.com/2014/04/28/world/asia/south-korean-premier-resigns-over-ferry-disaster.html (Accessed 22 February 2020).

Choe, S-H. (2018). Park Geun-hye, South Korea's Ousted President, Gets 24 Years in Prison. *New York Times*, 6 April. Available at: https://www.nytimes.com/2018/04/06/world/asia/park-geun-hye-south-korea.html (Accessed 22 February 2020).

Choe, S-H. (2019). South Korean Leader's Ally Convicted of Illegal Pre-Election Influence Campaign. *New York Times*, 30 January. Available at: https://www.nytimes.com/2019/01/30/world/asia/south-korea-president-moon-jae-in.html (Accessed 20 February 2020).

Choucri, N. (2012). *Cyberpolitics in International Relations*. Cambridge, MA: MIT Press.

Clarke, R. A. and Knake, R. (2019). The Internet Freedom League: How to Push Back Against the Authoritarian Assault on the Web. *Foreign Affairs*, 98/5: 184-192.

Clayton, J. (2021). Twitter Boss: Trump Ban Is ‘Right’ But ‘Dangerous’. *BBC*, 14 January. Available at: https://www.bbc.com/news/technology-55657417 (Accessed 4 July 2021).

Committee to Protect Journalists (2020). South Africa Enacts Regulations Criminalizing ‘Disinformation’ On Coronavirus Outbreak. *Committee to Protect Journalists*, 19 March. Available at: https://cpj.org/2020/03/south-africa-enacts-regulations-criminalizing-disi/ (Accessed 30 June 2020).

Conger, K. and Isaac, M. (2021). Twitter Permanently Bans Trump, Capping Online Revolt. *New York Times*, 8 January. Available at: https://www.nytimes.com/2021/01/08/technology/twitter-trump-suspended.html (Accessed 4 July 2021).

Constitutional Law of Kazakhstan (2010). *Konstitutsionnyi Zakon Respubliki Kazahstan ot 14 Iyunya 2010 Goda N289-IV*. Available at: https://online.zakon.kz/document/?doc_id=30762094#pos=1;-75 (Accessed 17 October 2020).

Coppins, M. (2020). The Billion-Dollar Disinformation Campaign to Reelect the President. *The Atlantic*, 325/2: 28-39.

Cummings, S. N. (2005). *Kazakhstan: Power and Elite*. New York: I.B. Tauris.

Curran, J., Fenton, N. and Freedman, D. (2016). *Misunderstanding the Internet*. London: Routledge.

D’Anieri, P. (2011). Structural Constraints in Ukrainian Politics. *East European Politics and Societies,* 25/1: 28-46.

D’Anieri, P. (2019). *Ukraine and Russia: From Civilized Divorce to Uncivil War*. Cambridge: Cambridge University Press.

Davis, R., Baumgartner, J. C., Francia, P. L. and Morris, J. S. (2009). The Internet in U.S. Election Campaigns. In: Chadwick, A. and Howard, P. N. (ed), *The Routledge Handbook of Internet Politics*. London: Routledge, 13-24.

Decree of the Acting Minister of Information (2018). *Prikaz i.o. Ministra Informatsii i Kommunikatsii Respubliki Kazahstan ot 23 Maya 2018 Goda N226.* Available at: http://online.zakon.kz/Document/?doc_id=32989072#pos=43;-20 (Accessed 16 January 2019).

Decree of the Cabinet of Ministers of Ukraine (2015). *Postanova Kabinet Ministriv Pro Pitannya Diyalnosti Ministerstva Informatsiinoi Politiki Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/en/2-2015-%D0%BF (Accessed 14 April 2020).

Decree of the Government of Kazakhstan (2018*). Postanovlenie Pravitelstva Respubliki Kazahstan ot 25 Oktyabrya 2018 Goda N659*. Available at: https://tengrinews.kz/zakon/pravitelstvo-respubliki-kazahstan-premer-ministr-rk/svyaz/id-P1800000679/ (Accessed 17 October 2020).

Decree of the Minister of Information (2019). *Prikaz Ministra Informatsii i Obshestvennogo Razvitiya Respubliki Kazahstan ot 29 Aprelya 2019 Goda N84*. Available at: https://tengrinews.kz/zakon/pravitelstvo-respubliki-kazahstan-premer-ministr-rk/kultupa/id-V1900018617/ (Accessed 17 October 2020).

Decree of the President of Kazakhstan (2019). *Ukaz Prezidenta Respubliki Kazahstan ot 9 Oktyabrya 2019 Goda N184*. Available at: https://online.zakon.kz/m/Document/?doc_id=33619997 (Accessed 27 April 2020).

Decree of the Verkhovna Rada (1991). *Postanova Verhovnoi Radi Ukraini Pro Stvorennya Sluzhbi Natsionalnoi Bezpeki Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/1581-12 (Accessed 14 April 2020).

Decree of the Verkhovna Rada (2014). *Postanova Verhovnoi Radi Ukraini Pro Samousunennya Prezidenta Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/757-18?lang=ru (Accessed 27 March 2020).

Decree of the President of Ukraine (2011). *Ukaz Prezidenta Ukraini N1067/2011*. Available at: https://zakon.rada.gov.ua/laws/show/1067/2011 (Accessed 14 April 2020).

Decree of the President of Ukraine (2017). *Ukaz Prezidenta Ukraini N133/2017*. Available at: https://www.president.gov.ua/documents/1332017-21850 (Accessed 7 April 2020).

Decree of the President of Ukraine (2018). *Ukaz Prezidenta Ukraini N126/2018*. Available at: https://www.president.gov.ua/documents/1262018-24150 (Accessed 7 April 2020).

Decree of the President of Ukraine (2019). *Ukaz Prezidenta Ukraini N82/2019*. Available at: https://www.president.gov.ua/documents/822019-26290 (Accessed 8 April 2020).

Deibert, R. (2009). The Geopolitics of Internet Control: Censorship, Sovereignty, And Cyberspace. In: Chadwick, A. and Howard, P. N. (ed), *The Routledge Handbook of Internet Politics*. London: Routledge, 323-336.

Deibert, R. and Rohozinski, R. (2010a). Beyond Denial: Introducing Next-Generation Information Access Controls. In: Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 3-13.

Deibert, R. and Rohozinski, R. (2010b). Control and Subversion in Russian Cyberspace. In: Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed), *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press, 15-34.

Deibert, R. and Rohozinski, R. (2010c). Liberation vs. Control: The Future of Cyberspace. *Journal of Democracy*, 21/4: 43-57.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed) (2008). *Access Denied: The Practice and Policy of Global Internet Filtering*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed) (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, MA: MIT Press.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (2012a). Access Contested: Toward the Fourth Phase of Cyberspace Controls. In: Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed), *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press, 3-20.

Deibert, R., Palfrey, J., Rohozinski, R. and Zittrain, J. (ed) (2012b). *Access Contested: Security, Identity, and Resistance in Asian Cyberspace.* Cambridge, MA: MIT Press.

Deibert, R. (2015). Cyberspace Under Siege. *Journal of Democracy*, 26/3: 64-78.

DeNardis, L. (2014). *The Global War for Internet Governance*. New Haven, CT: Yale University Press.

Dencik, L., Hintz, A. and Cable, J. (2016). Towards Data Justice? The Ambiguity of Anti-Surveillance Resistance in Political Activism. *Big Data and Society*, 3/2: 1-12.

Detector Media (2018). Ukazom o Sanktsiyah Prezident Nezakonno Obyazal Provaiderov Blokirovat 192 Novyh Saita – "Laboratoriya Tsifrovoi Bezopasnosti". [By a Decree, the President Illegally Obliged Providers to Block 192 New Sites – "Laboratory of Digital Security". *Detector Media*, 25 May. Available at: https://detector.media/infospace/article/137834/2018-05-25-ukazom-pro-sanktsii-prezident-nezakonno-zobovyazav-provaideriv-blokuvati-192-novikh-saiti-laboratoriya-tsifrovoi-bezpeki/ (Accessed 8 April 2020).

Diamond, L. (2010). Liberation Technology. *Journal of Democracy*, 21/3: 69-83.

Diamond, L. (2012). Introduction. In: Diamond, L. and Plattner, M. F. (ed), *Liberation Technology: Social Media and the Struggle for Democracy.* Baltimore: The Johns Hopkins University Press, ix-xxvii.

Diamond, L. (2019). *Ill Winds: Saving Democracy from Russian Rage, Chinese Ambition, and American Complacency*. New York: Penguin Books.

Diamond, L. (2020). Democracy Versus the Pandemic. *Foreign Affairs*, 13 June. Available at: https://www.foreignaffairs.com/articles/world/2020-06-13/democracy-versus-pandemic (Accessed 5 July 2020).

Digital Report (2016). Natsionalnyi Sertifikat Bezopasnosti Kazahstana: Zashita Polzovatelei ili Gosudarstva?. [The National Certificate of Security of Kazakhstan: Protection of Users of the State?]. *Digital Report*, 29 January. Available at: https://digital.report/kazakhstan-mitm-security-certificate-update/ (Accessed 27 April 2020).

Djankov, S., Mcliesh, C., Nenova, T. and Shleifer, A. (2003). Who Owns the Media?. *Journal of Law and Economics*, XLVI: 341-381.

Dubovaya, M. (2018). Zachem Sozdali Sistemu Monitoringa Informprostranstva za 1.67 Mlrd Tenge, Obyasnil Abaev. [Why the Monitoring System of Information Space Was Created for 1.67 Bln Tenge, Abayev Explained]. *Informburo*, 12 January. Available at: https://informburo.kz/novosti/zachem-sozdali-sistemu-monitoringa-informprostranstva-za-167-mlrd-tenge-obyasnil-abaev.html (Accessed 16 January 2019).

Ellis-Petersen, H. (2019). Myanmar Frees Reuters Journalists Jailed for Reporting on Rohingya Crisis. *The Guardian*, 7 May. Available at: https://www.theguardian.com/world/2019/may/07/myanmar-frees-reuters-journalists-jailed-for-reporting-on-rohingya-crisis (Accessed 20 February 2020).

Embury-Dennis, T. (2019). Extinction Rebellion: London Tube Wifi Shut Down by Police in Attempt to Disrupt Climate Change Protesters. *The Independent*, 17 April. Available at: https://www.independent.co.uk/news/uk/home-news/london-tube-wifi-down-internet-not-working-underground-protest-extinction-rebellion-a8873681.html (Accessed 20 February 2020).

Enikolopov, R., Petrova M. and Zhuravskaya, E. (2011). Media and Political Persuasion: Evidence from Russia. *The American Economic Review*, 101/7: 3253-3285.

Esfandiari, G. (2010). The Twitter Devolution. *Foreign Policy*, 8 June. Available at: https://foreignpolicy.com/2010/06/08/the-twitter-devolution/ (Accessed 8 January 2020).

Facebook Transparency (2020). *Kazakhstan*. Available at: https://transparency.facebook.com/government-data-requests/country/KZ (Accessed 5 October 2020).

Facebook Transparency (2020). *Ukraine*. Available at: https://transparency.facebook.com/government-data-requests/country/UA (Accessed 5 October 2020).

Farmer, B. and Gillani, W. (2018). Two Christian Brothers Sentenced to Death for Web Blasphemy in Pakistan. *The Telegraph*, 18 December. Available at: https://www.telegraph.co.uk/news/2018/12/18/two-christian-brothers-sentenced-death-web-blasphemy-pakistan/ (Accessed 1 July 2020).

Fokht, E. (2019). Internet vo Vremya Mitingov v Moskve Mogli Glushit’ po Trebovaniyu Silovikov [The Internet During the Moscow Rallies Might Have Been Jammed on Demand of Siloviks]. *BBC*, 6 August. Available at: https://www.bbc.com/russian/features-49255791 (Accessed 14 January 2020).

Forbes Kazakhstan (2015). Posol SSHA v RK: U Nas Net Ofitsialnoi Pozitsii v Otnoshenii Preemnika. [The US Ambassador in Kazakhstan: We Have No Official Position on a Successor]. *Forbes Kazakhstan*, 6 November. Available at: https://forbes.kz//massmedia/posol_ssha_v_rk_u_nas_net_ofitsialnoy_pozitsii_v_otnoshenii_preemnika/ (Accessed 25 April 2020).

Forbes Kazakhstan (2016). Dauren Abaev – o Problemah s Dostupom k Sotssetyam i Ablyazove [Dauren Abaev – about Problems of Access to Social Networks and Ablyazov]. *Forbes Kazakhstan*, 20 December. Available at: http://forbes.kz/process/internet/dauren_abaev_o_problemah_s_dostupom_k_sotssetyam_i_ablyazove (Accessed 15 September 2020).

Foroohar, R. (2019). *Don’t Be Evil: The Case Against Big Tech*. London: Penguin Books.

Frantz, E. (2018). *Authoritarianism: What Everybody Needs to Know*. New York: Oxford University Press.

Freedom House (2012). *Freedom on the Net 2012: A Global Assessment of Internet and Digital Media*. New York: Freedom House.

Freedom House (2013). *Freedom on the Net 2013: A Global Assessment of Internet and Digital Media*. New York: Freedom House.

Freedom House (2014). *Freedom on the Net 2014: Tightening the Net: Governments Expand Online Controls*. New York: Freedom House.

Freedom House (2015). *Freedom on the Net 2015: Privatizing Censorship, Eroding Privacy*. New York: Freedom House.

Freedom House (2017). *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. New York: Freedom House.

Freedom House (2018). *Freedom on the Net 2018: The Rise of Digital Authoritarianism*. New York: Freedom House.

Freedom House Bangladesh (2019). Freedom on the Net 2019: Bangladesh. *Freedom House.* Available at: https://freedomhouse.org/country/bangladesh/freedom-net/2019 (Accessed 14 October 2020).

Freedom House Belarus (2018). Freedom on the Net 2018: Belarus. *Freedom House.* Available at: https://freedomhouse.org/country/belarus/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Canada (2018). Freedom on the Net 2018: Canada. *Freedom House*. Available at: https://freedomhouse.org/country/canada/freedom-net/2018 (Accessed 10 February 2020).

Freedom House China (2018). Freedom on the Net 2018: China. *Freedom House.* Available at: https://freedomhouse.org/country/china/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Georgia (2019). Freedom on the Net 2019: Georgia. *Freedom House.* Available at: https://freedomhouse.org/country/georgia/freedom-net/2019 (Accessed 6 March 2020).

Freedom House India (2017). Freedom on the Net 2017: India. *Freedom House.* Available at: https://freedomhouse.org/country/india/freedom-net/2017 (Accessed 14 October 2020).

Freedom House India (2018). Freedom on the Net 2018: India. *Freedom House.* Available at: https://freedomhouse.org/country/india/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Kazakhstan (2016). Freedom on the Net 2016: Kazakhstan. *Freedom House.* Available at: https://freedomhouse.org/country/kazakhstan/freedom-net/2016 (Accessed 6 March 2020).

Freedom House Kazakhstan (2017). Freedom on the Net 2017: Kazakhstan. *Freedom House.* Available at: https://freedomhouse.org/country/kazakhstan/freedom-net/2017 (Accessed 15 October 2020).

Freedom House Kazakhstan (2019). Freedom on the Net 2019: Kazakhstan. *Freedom House.* Available at: https://freedomhouse.org/country/kazakhstan/freedom-net/2019 (Accessed 15 October 2020).

Freedom House Malaysia (2018). Freedom on the Net 2018: Malaysia. *Freedom House.* Available at: https://freedomhouse.org/country/malaysia/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Nigeria (2018). Freedom on the Net 2018: Nigeria. *Freedom House.* Available at: https://freedomhouse.org/country/nigeria/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Pakistan (2018). Freedom on the Net 2018: Pakistan. *Freedom House.* Available at: https://freedomhouse.org/country/pakistan/freedom-net/2018 (Accessed 14 October 2020).

Freedom House South Africa (2019). Freedom on the Net 2019: South Africa. *Freedom House.* Available at: https://freedomhouse.org/country/south-africa/freedom-net/2019 (Accessed 14 October 2020).

Freedom House South Korea (2016). Freedom on the Net 2016: South Korea. *Freedom House.* Available at: https://freedomhouse.org/country/south-korea/freedom-net/2016 (Accessed 14 October 2020).

Freedom House South Korea (2019). Freedom on the Net 2019: South Korea. *Freedom House.* Available at: https://freedomhouse.org/country/south-korea/freedom-net/2019 (Accessed 14 October 2020).

Freedom House Sri Lanka (2018). Freedom on the Net 2018: Sri Lanka. *Freedom House.* Available at: https://freedomhouse.org/country/sri-lanka/freedom-net/2018 (Accessed 14 October 2020).

Freedom House The Gambia (2017). Freedom on the Net 2017: The Gambia. *Freedom House*. Available at: https://freedomhouse.org/country/gambia/freedom-net/2017 (Accessed 14 October 2020).

Freedom House Ukraine (2016). Freedom on the Net 2016: Ukraine. *Freedom House.* Available at: https://freedomhouse.org/country/ukraine/freedom-net/2016 (Accessed 16 October 2020).

Freedom House Ukraine (2017). Freedom on the Net 2017: Ukraine. *Freedom House.* Available at: https://freedomhouse.org/country/ukraine/freedom-net/2017 (Accessed 16 October 2020).

Freedom House Ukraine (2018). Freedom on the Net 2018: Ukraine. *Freedom House.* Available at: https://freedomhouse.org/country/ukraine/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Ukraine (2019). Freedom on the Net 2019: Ukraine. *Freedom House.* Available at: https://freedomhouse.org/country/ukraine/freedom-net/2019 (Accessed 15 October 2020).

Freedom House United Kingdom (2018). Freedom on the Net 2018: United Kingdom. *Freedom House.* Available at: https://freedomhouse.org/country/united-kingdom/freedom-net/2018 (Accessed 14 October 2020).

Freedom House United States (2018). Freedom on the Net 2018: United States. *Freedom House.* Available at: https://freedomhouse.org/country/united-states/freedom-net/2018 (Accessed 14 October 2020).

Freedom House Uzbekistan (2018). Freedom on the Net 2018: Uzbekistan. *Freedom House.* Available at: https://freedomhouse.org/country/uzbekistan/freedom-net/2018 (Accessed 28 June 2020).

Freedom House Zambia (2017). Freedom on the Net 2017: Zambia. *Freedom House.* Available at: https://freedomhouse.org/country/zambia/freedom-net/2017 (Accessed 14 October 2020).

Frier, S. (2021). Twitter's Trump Ban Deemed Necessary, Derided as Long Overdue. *Bloomberg*, 9 January. Available at: https://www.bloomberg.com/news/articles/2021-01-09/twitter-s-trump-ban-deemed-necessary-derided-as-long-overdue (Accessed 4 July 2021).

Gallagher, R. (2020). Belarusian Officials Shut Down Internet with Technology Made by U.S. Firm. *Bloomberg*, 28 August 2020. Available at: https://www.bloomberg.com/news/articles/2020-08-28/belarusian-officials-shut-down-internet-with-technology-made-by-u-s-firm (Accessed 08 October 2020).

Galperin, E., Quintin, C., Marquis-Boire M., and Guarnieri, C. (2016). I Got a Letter From the Government the Other Day… Unveiling a Campaign of Intimidation, Kidnapping, and Malware in Kazakhstan. *Electronic Frontier Foundation*. Available at: https://www.eff.org/files/2016/08/03/i-got-a-letter-from-the-government.pdf (Accessed 26 April 2020).

Garmazhapova, A. (2013). Gde Zhivut Trolli. I Kto Ih Kormit. [Where Trolls Live. And Who Feeds Them]. *Novaya Gazeta,* 7 September. Available at: https://novayagazeta.ru/articles/2013/09/07/56253-gde-zhivut-trolli-i-kto-ih-kormit (Accessed 28 June 2020).

Gavrilov, E. (2014). SBU Izyala Servera Gazety "Vesti". [SBU Withdrew Servers of the "Vesti" Newspaper]. *ZN Ukraine*, 11 September. Available at: https://zn.ua/UKRAINE/sbu-izyala-servera-gazety-vesti-152834_.html (Accessed 7 April 2020).

Geddes, B. (1994). *Politician's Dilemma: Building State Capacity in Latin America*. Berkeley: University of California Press.

George, A. L. and Bennet, A. (2005). *Case Studies and Theory Development in the Social Sciences*. Cambridge, MA: MIT Press.

Gerovitch, S. (2008). InterNyet: Why the Soviet Union Did Not Build a Nationwide Computer Network. *History and Technology*, 24/4: 335-350.

Gerring, J. (2011). The Case Study: What It Is and What It Does. In: Goodin, R. E. (ed), *The Oxford Handbook of Political Science*. Oxford: Oxford University Press, 1133-1148.

Gettleman, J. (2019). Tensions Over Kashmir Rise But India Says No Plans for War. *New York Times*, 30 August. Available at: https://www.nytimes.com/2019/08/30/world/asia/kashmir-india-pakistan.html (Accessed 3 September 2019).

Gettleman, J., and Abi-Habib, M. (2019). As Protests Rage on Citizenship Bill, Is India Becoming a Hindu Nation?. *New York Times*, 16 December. Available at: https://www.nytimes.com/2019/12/16/world/asia/india-citizenship-protests.html (Accessed 20 February 2020).

Gettleman, J., Goel, V. and Abi-Habib, M. (2019). India Adopts the Tactic of Authoritarians: Shutting Down the Internet. *New York Times*, 17 December. Available at: https://www.nytimes.com/2019/12/17/world/asia/india-internet-modi-protests.html (Accessed 20 February 2020).

Gettleman, J., Kumar, H. and Yasir S. (2020). Worst Clash in Decades on Disputed India-China Border Kills 20 Indian Troops. *New York Times*, 16 June. Available at: https://www.nytimes.com/2020/06/16/world/asia/indian-china-border-clash.html (Accessed 1 July 2020).

Gibson, R. K., Margolis, M., Resnick, D. and Ward, S. J. (2003). Election Campaigning on the WWW in the USA and UK: A Comparative Analysis. *Party Politics*, 9/1: 47-75.
Gilder, G. (2000). *Telecosm: How Infinite Bandwidth Will Revolutionize Our World.* New York: The Free Press.

Gladwell, M. (2010). Small Change: Why the Revolution Will Not Be Tweeted. *New Yorker*, 27 September. Available at: https://www.newyorker.com/magazine/2010/10/04/small-change-malcolm-gladwell (Accessed 8 January 2020).

Glasius, M. (2018). What Authoritarianism Is … And Is Not: A Practice Perspective. *International Affairs*, 94/3: 515-533.

Glasius, M., and Michaelsen, M. (2018). Prologue: Illiberal and Authoritarian Practices in the Digital Sphere. *International Journal of Communication*, 12: 3795–3813.

Global Commission on Internet Governance (2016). *One Internet*. The Centre for International Governance Innovation and Chatham House.

Glukhov, D. (2017). Internet Assotsiatsiya Ukrainy Obvinila Vlast v Politicheskoi Tsenzure. [The Internet Association of Ukraine Accused the Government of Political Censorship]. *KP Ukraine*, 18 May. Available at: https://kp.ua/politics/576254-ynternet-assotsyatsyia-ukrayny-obvynyla-vlast-v-polytycheskoi-tsenzure (Accessed 8 April 2020).

Glushkova, S. (2011). Portal "Vordpress" Zakryli iz-za Dvuh Blogov. [The "Wordpress" Portal Was Closed Because of Two Blogs]. *Radio Azattyq*, 12 July. Available at: https://rus.azattyq.org/a/worldpress_kazakhtelecom_blocking_blog_/24262786.html (Accessed 25 April 2020).

Goel, V., and Gettleman J. (2020). Under Modi, India's Press Is Not So Free Anymore. *New York Times*, 2 April. Available at: https://www.nytimes.com/2020/04/02/world/asia/modi-india-press-media.html (Accessed 3 July 2020).

Goldsmith, J. and Wu, T. (2006). *Who Controls the Internet? Illusions of a Borderless World.* Oxford: Oxford University Press.

Google Transparency Report (n/d). *Kazakhstan (by country)*. Available at: https://transparencyreport.google.com/government-removals/by-country/KZ?hl=en (Accessed 5 October 2020).

Google Transparency Report (n/d). *Kazakhstan (overview)*. Available at: https://transparencyreport.google.com/government-removals/overview?hl=en&authority_search=country:Kazakhstan&lu=authority_search (Accessed 5 October 2020).

Google Transparency Report (n/d). *Ukraine (by country)*. Available at: https://transparencyreport.google.com/government-removals/by-country/UA?hl=en (Accessed on 5 October 2020).

Google Transparency Report (n/d). *Ukraine (overview)*. Available at: https://transparencyreport.google.com/government-removals/overview?hl=en&authority_search=country:Ukraine&lu=authority_search (Accessed 5 October 2020).

Gorchinskaya, K. (2016). The Rise of Kremlin-Style Trolling in Ukraine Must End. *The Guardian*, 27 July. Available at: https://www.theguardian.com/world/2016/jul/27/kremlin-style-troll-attacks-are-on-the-rise-in-ukraine-hromadske (Accessed 15 April 2020).

Greenwald, G. (2014). *No Place to Hide: Edward Snowden, the NSA and the Surveillance State*. London: Penguin Books.

Greenwald, G. (2015). With Power of Social Media Growing, Police Now Monitoring and Criminalizing Online Speech. *The Intercept*, 6 January. Available at: https://theintercept.com/2015/01/06/police-increasingly-monitoring-criminalizing-online-speech/ (Accessed 27 August 2020).

Grobler, R. (2020). Man Who Posted Fake 'Contaminated Covid-19 Test Kits' Video Arrested. *News 24*, 7 April. https://www.news24.com/news24/southafrica/news/man-who-posted-fake-contaminated-covid-19-test-kits-video-arrested-20200407 (Accessed 30 June 2020).

Gubin, V. (2017). I Gullivery Stanut Liliputami. K Chemu Privedut Vcherashnie Obyski v "Vestyah" i u "Struktur Klimenko". (And Gullivers Will Become Lilliput. Where Yesterday's Searches of "Vesti" and "Klimenko's Structures" Will Lead To]. *Strana*, 15 July. Available at: https://strana.ua/articles/analysis/81675--zakryt-vesti-i-prevratit-gullivera-v-liliputa-dlya-chego-proveli-vtoruyu-seriyu-obyskov-po-delu-klimenkovcev.html (Accessed 10 April 2020).

Guriev, S. M. and Treisman, D. (2015). How Modern Dictators Survive: Cooptation, Censorship, Propaganda, and Repression. *Centre for Economic Policy Research,* Discussion Paper no. DP10454.

Hall, P. A. and Taylor, R. S. R. (1996). Political Science and the Three New Institutionalisms. *Political Studies*, XLIV: 936-957.

Halperin, S. and Heath, O. (2012). *Political Research: Methods and Practical Skills*. Oxford: Oxford University Press.

Hancocks, P. (2019). Why North Korea Wants Nothing to Do With South Korea. *CNN*, 20 December. Available at: https://edition.cnn.com/2019/12/19/asia/north-korea-south-korea-intl-hnk/index.html (Accessed 23 February 2020).

Hay, C. (2002). *Political Analysis: A Critical Introduction*. London: Palgrave.

Hintz, A. and Milan, S. (2018). "Through a Glass, Darkly": Everyday Acts of Authoritarianism in the Liberal West. *International Journal of Communication*, 12: 3939-3959.

Hintz, A., Dencik, L. and Wahl-Jorgensen, K. (2019). *Digital Citizenship in a Datafied Society*. Cambridge: Polity Press.

Hiro, D. (2009). *Inside Central Asia: A Political and Cultural History of Uzbekistan, Turkmenistan, Kazakhstan, Kyrgyzstan, Tajikistan, Turkey, and Iran*. New York: Overlook Duckworth.

Holub, A. (2017). Poroshenko vs The Memes: How Ukrainian Social Media Users React to The President. *The Ukrainian Week*, 8 June. Available at: https://ukrainianweek.com/Politics/194118 (Accessed 15 April 2020).

Howard, P. N. (2010). *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press.

Howard, P. N. and Hussain, M. M. (2013). *Democracy's Fourth Wave? Digital Media and the Arab Spring.* Oxford: Oxford University Press.

Human Rights Watch (2004). Political Freedoms in Kazakhstan. *Human Rights Watch*, 16/3D: 1-53. Available at: https://www.hrw.org/sites/default/files/reports/kazakhstan0404.pdf (Accessed 25 April 2020).

Human Rights Watch (2015). South Korea: Cold War Relic Law Criminalizes Criticism. *Human Rights Watch*, 28 May. Available at: https://www.hrw.org/news/2015/05/28/south-korea-cold-war-relic-law-criminalizes-criticism (Accessed 20 February 2020)

Human Rights Watch (2016). Kazakhstan: 2 Activists Sentenced to 5 Years. *Human Rights Watch*, 28 November. Available at: https://www.hrw.org/news/2016/11/28/kazakhstan-2-activists-sentenced-5-years (Accessed 26 April 2020)

Human Rights Watch (2017). Ukraine: Revoke Ban on Dozens of Russian Web Companies. *Human Rights Watch*, 16 May. Available at: https://www.hrw.org/news/2017/05/16/ukraine-revoke-ban-dozens-russian-web-companies (Accessed 7 April 2020).

Hussain, M. M. and Howard, P. N. (2013). What Best Explains Successful Protest Cascades? ICTs and the Fuzzy Causes of the Arab Spring. *International Studies Review*, 15: 48-66.

Hussain, M. M., Howard, P. N. and Agarwal S. D. (2013). Introduction: State Power 2.0. In: Hussain, M. M. and Howard, P. N. (ed), *State Power 2.0: Authoritarian Entrenchment and Political Engagement Worldwide*, Surrey: Ashgate, 1-16.

Informburo (2016a). Vse Chto Nuzhno Znat o Natsionalnom Sertifikate Bezopasnosti RK. [All You Need to Know About the National Certificate of Security of Kazakhstan]. *Informburo*, 29 Jule. Available at: https://informburo.kz/cards/vsyo-chto-nuzhno-znat-o-nacionalnom-sertifikate-bezopasnosti-rk.html (Accessed 17 October 2020).

Informburo (2016b). Maks Bokaev i Talgat Ayan Poluchili po Pyat Let Lisheniya Svobody. [Max Bokayev and Talgat Ayan Received Five Years of Imprisonment]. *Informburo*, 28 November. Available at: https://informburo.kz/novosti/maks-bokaev-i-talgat-ayan-poluchili-po-pyat-let-lisheniya-svobody.html (Accessed 26 April 2020).

Internet Freedom (2018). Zayavlenie Obshestvennyh Organizatsii Otnositelno Trebovaniya Blokirovat Saity v Sootvetstvii s Novym Sanktsionnogo Ukaza Prezidenta Ukrainy N126/2018. [Statement of Public Organisations with Regard to Demands to Block Sites in Accordance with the N126/2018 New Sanction Decree of the Ukrainian President]. *Internet Freedom*, 25 May. Available at: https://netfreedom.org.ua/article/zayava-gromadskih-organizacij-shchodo-vimogi-blokuvati-sajti-vidpovidno-do-novogo-sankcijnogo (Accessed 8 April 2020).

Internet Live Stats (n/d). *Twitter Usage Statistics*. Internetlivestats.com. Available at: https://www.internetlivestats.com/twitter-statistics/ (Accessed 15 September 2020).

Internet Shutdown Tracker (n/d). *Internet Shutdowns*. Internetshutdowns.in. Available at: https://internetshutdowns.in/ (Accessed 14 October 2020).

Ivanova, N. (2019). Na Kanale “1+1” Zayavili, Chto Poroshenko Ubil Sobstvennogo Brata: Reaktsiya Sotssetei. [Poroshenko Killed His Own Brother, Was Declared on the “1+1” Channel: Reaction of Social Media]. *Ukrainian News*, 24 March. Available at: https://ukranews.com/news/621772-na-kanale-1-1-zayavili-chto-poroshenko-ubil-sobstvennogo-brata-reaktsiya-sotssetej (Accessed 16 April 2020).

Jankowicz, N. (2019). Ukraine’s Election Is an All-Out Disinformation Battle. *The Atlantic*, 17 April. Available at: https://www.theatlantic.com/international/archive/2019/04/russia-disinformation-ukraine-election/587179/ (Accessed 16 April 2020).

Jordan, E., Gross, M. E., Javernick-Will, A. M. and Garvin, M. J. (2011). Use and Misuse of Qualitative Comparative Analysis. *Construction Management and Economics*, 29/11: 1159-1173.

Jordan, T. (2015). *Information Politics: Liberation and Exploitation in the Digital Society*. London: Pluto Press.

Kalathil, S. and Boas, T. C. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Washington: Carnegie Endowment for International Peace.

Kalyukov, E., Parfentieva, I., Balashova, A., Li, I., and Aleksenko, P. (2017). Poroshenko Zablokiroval “Yandeks”, “Odnoklassniki” i “VKontakte”. [Poroshenko Blocked “Yandex”, “Odnoklassniki”, and “VKontakte”]. *RBC*, 16 May. Available at: https://www.rbc.ru/politics/16/05/2017/591aae3e9a79473f81fb65b7 (Accessed 7 April 2020).

Karpenko, O. (2014). SBU Zavela Ugolovnoe Delo Na Troih Polzovatelei “VKontakte” Za Separatizm. [SBU Opened Criminal Cases on Three Users of “Vkontakte” for Separatism]. *AIN Ukraine*, 18 March. Available at: https://ain.ua/2014/03/18/sbu-zavela-ugolovnoe-delo-na-polzovatelej-vkontakte-za-separatizm/ (Accessed 9 April 2020).

Karpenko, O. (2015). Siloviki Izymayut Servery Krupnogo Registratora NIC.UA iz-za Saitov Separatistov. [Siloviks Withdraw Servers of the Large Registrar NIC.UA Because of Sites of Separatists]. *AIN Ukraine*, 7 April. Available at: https://ain.ua/2015/04/07/siloviki-izymayut-servery-krupnogo-registratora-nic-ua/ (Accessed 7 April 2020).

Kazinform (2014). V Kazahstane Zakryli Dostup k 596 Saitam, Propagandiruyushim Ekstremism i Terrorism. *Kazinform*, 17 January. Available at: https://www.inform.kz/ru/v-kazahstane-zakryli-dostup-k-596-saytam-propagandiruyuschim-ekstremizm-i-terrorizm_a2622199 (Accessed 25 April 2020).

Kendall-Taylor, A., Frantz, E. and Wright, J. (2020). The Digital Dictators: How Technology Strengthens Autocracy. *Foreign Affairs*, 99/2: 103-115.

Kennan, G. F. (X) (1947). The Sources of Soviet Conduct. *Foreign Affairs*, 25/4: 566-582.

Kcell (n/d). *Ustanovka Doverennogo Sertifikata Qaznet.* [*The Installation of the Trusted Certificate Qaznet*]. Kcell.kz. Available at: https://www.kcell.kz/ru/product/trust-certificate (Accessed 17 October 2020).

Khabarov, M. (2015). Trendy FB. Alyans Blogerov Prosit Otmenit Prezidentskie Vybory. [Facebook Trends. Alliance of Bloggers Asks to Cancel Presidential Elections]. *Zona KZ*, 19 February. Available at: https://zonakz.net/2015/02/19/trendy-fb-aljans-blogerov-prosit-otmenit-prezidentskie-vybory-kandidaty-v-prezidenty-zhgut-i-v-fb/ (Accessed 27 April 2020).

Kichanova, V. (2014). Sait Meduza Zablokirovali v Kazahstane za Reportazh o Separatistah. [The Meduza Site Was Blocked in Kazakhstan Due to the Reporting About Separatists]. *Republic*, 21 October. Available at: https://republic.ru/posts/l/1174186 (Accessed 25 April 2020).

Kim, S. (2019). Yeonpyeong: Tiny South Korean Island Watching the Horizon. *BBC*, 22 December. Available at: https://www.bbc.co.uk/news/world-asia-50808326 (Accessed 23 February 2020).

King, G., Pan J., and Roberts M. E. (2014). Reverse-engineering Censorship in China: Randomized Experimentation and Participant Observation. *Science*, 345/6199: 1251722-1-1251722-10.

King, G., Pan J., and Roberts M. E. (2017). How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, Not Engaged Argument. *American Political Science Review*, 111/3: 484-501.

Kommersant (2007). Chem Zakonchilsya Referendum v 2000 Godu. [How the 2000 Referendum Ended]. *Kommersant*, 2 July. Available at: https://www.kommersant.ru/doc/779321 (Accessed 26 March 2020).

Korrespondent (2014a). Na Dnepropetrovshine Osudili Muzhchinu za Separatistskie Prizyvy v Sotssetyah. [In the Dnipropetrovsk Region, a Man Was Convicted for Separatist Calls on Social Media]. *Korrespondent*, 14 July. Available at: https://korrespondent.net/ukraine/politics/3392467-na-dnepropetrovschyne-osudyly-muzhchynu-za-separatystskye-pryzyvy-v-sotssetiakh (Accessed 9 April 2020).

Korrespondent (2014b). SBU Perehvatila Razgovor Separatistov ob Obstrele Avdeevki. [SBU Intercepted Conversation of Separatists About the Shooting of Avdeevka]. *Korrespondent*, 11 September. Available at: https://korrespondent.net/ukraine/3417589-sbu-perekhvatyla-razghovor-separatystov-ob-obstrele-avdeevky (Accessed 30 July 2020).

Korrespondent (2015). V Informatsionnye Voiska Ukrainy Vstupili Uzhe Okolo 40 Tysyach Dobrovoltsev. [Around 40 Thousand Volunteers Have Already Joined the Information Troops of Ukraine]. *Korrespondent*, 13 May. Available at: https://korrespondent.net/ukraine/events/3514255-v-ynformatsyonnye-voiska-ukrayny-vstupyly-uzhe-okolo-40-tysiach-dobrovoltsev (Accessed 15 April 2020).

Korrespondent (2016a). V Kieve Zaderzhali Zhenshinu za Separatizm v Sotssetyah. [In Kiev, a Woman Was Detained for Separatism on Social Media]. *Korrespondent*, 12 September. Available at: https://korrespondent.net/city/kiev/3743871-v-kyeve-zaderzhaly-zhenschynu-za-separatyzm-v-sotssetiakh#2 (Accessed 9 April 2020).

Korrespondent (2016b). Separatizm v Sotssetyah. Kogo Sudyat za Posty v Seti. [Separatism on Social Media. Who is Convicted for Posts in the Web]. *Korrespondent*, 14 September. Available at: https://korrespondent.net/ukraine/3744858-separatyzm-v-sotssetiakh-koho-sudiat-za-posty-v-sety (Accessed 9 April 2020).

Kosenov, A. (2011a). V Kazahstane Zakryli Dostup k 125 Saitam. [Access to 125 Sites Was Blocked in Kazakhstan]. *Tengrinews*, 1 October. Available at: https://tengrinews.kz/kazakhstan_news/v-kazahstane-zakryili-dostup-k-125-saytam-198106/ (Accessed 25 April 2020).

Kosenov, A. (2011b). Chislo Zhertv Besporyadkov v Zhanaozene Dostiglo 16. [The Number of Victims from Riots in Zhanaozen Reached 16]. *Tengrinews*, 25 December. Available at: https://tengrinews.kz/kazakhstan_news/chislo-jertv-besporyadkov-v-janaozene-dostiglo-16-204559/ (Accessed 25 April 2020).

Kosenov, A. (2015). 700 Internet-Resursov Priznany Nezakonnymi v Kazahstane – Genprokuratura. [700 Internet-Resources Have Been Declared Illegal in Kazakhstan – The General Prosecutor's Office]. *Tengrinews*, 23 January. Available at: https://tengrinews.kz/internet/700-internet-resursov-priznanyi-nezakonnyimi-kazahstane-268841/ (Accessed 6 February 2017).

Kotkin, S. (2001). *Armageddon Averted: The Soviet Collapse, 1970-2000*. Oxford: Oxford University Press.

Kovalenko, O. and Zhartovskaya, M. (2018). Do Vyborov Ostalos 166 Dnei. Poroshenko Rabotaet s Facebook-Blogerami. [166 Days Left Before Elections. Poroshenko Is Working with Facebook-Bloggers]. *Babel*, 16 October. Available at: https://babel.ua/ru/texts/20534-vybory-v-detalyah-detal-1-poroshenko-i-facebook-lomy (Accessed 15 April 2020).

Kozhanova, N. (2019). Finding Kazakhstan's Troll Farms. *The Diplomat*, 20 February. Available at: https://thediplomat.com/2019/02/finding-kazakhstans-troll-farms/ (Accessed 27 April 2020).

Kristof, N. D. (2005). Death by a Thousand Blogs. *New York Times*, 24 May. Available at: https://www.nytimes.com/2005/05/24/opinion/death-by-a-thousand-blogs.html (Accessed 7 January 2020).

Kremlin (2018). Otkrytie Avtodorozhnoi CHasti Krymskogo Mosta. [Opening of the Highway of the Crimean Bridge. *Kremlin*, 15 May. Available at: http://kremlin.ru/events/president/news/57472 (Accessed 10 April 2020).

Krishnan, V. (2020). The Callousness of India's COVID-19 Response: The Government Is Showing How Not to Handle A Pandemic. *The Atlantic*, 27 March. Available at: https://www.theatlantic.com/international/archive/2020/03/india-coronavirus-covid19-narendra-modi/608896/ (Accessed 3 July 2020).

Krutov, M. (2019). Poimennyi Spisok. [List of Names]. *Radio Freedom*, 19 June. Available at: https://www.svoboda.org/a/30007156.html (Accessed 30 July 2020).

Kulshmanov, A. (2017). S Nashei Storony Nikakih Deistvii Ne Bylo – Abaev o Blokirovke Foreign Policy. [There Were No Actions from Our Side – Abayev about the Blockage of Foreign Policy]. *Tengrinews*, 20 June. Available at: https://tengrinews.kz/kazakhstan_news/nashey-storonyi-nikakih-deystviy-byilo-abaev-blokirovke-320646/ (Accessed 25 April 2020).

Kurbalija, J. (2016). *An Introduction to Internet Governance.* 7th ed. DiploFoundation.

Kursiv (2019). Zhiteli Nur-Sultana Negativno Vosprinyali Soobshenie ot Sotovyh Operatorov. [Citizens of Nur-Sultan Negatively Perceived a Message from Mobile Operators]. *Kursiv*, 19 July. Available at: https://kursiv.kz/news/obschestvo/2019-07/zhiteli-nur-sultana-negativno-vosprinyali-soobschenie-ot-sotovykh (Accessed 27 April 2020).

Kurtov, A. (2000). Demokratiya Vyborov v Kazahstane: Avtoritarnaya Evolyutsiya. [Democracy of Elections in Kazakhstan: The Authoritarian Evolution]. *Vostochnoevropeiskoe obozrenie*, 2/31: 2-10.

Lacy, M. (2014). *Security, Technology and Global Politics: Thinking with Virilio*. Oxford: Routledge.

Lacy, M. (2018). Dhaka: How Speeding Bus Drivers Sparked A Student Insurrection. *The Conversation*, 18 September. Available at: https://theconversation.com/dhaka-how-speeding-bus-drivers-sparked-a-student-insurrection-102744 (Accessed 22 August 2020).

Lacy, M. and Mookherjee, N. (2020). ‘Firing Cannons to Kill Mosquitoes’: Controlling ‘Virtual Streets’ and the ‘Image of the State’ In Bangladesh. *Contributions to Indian Sociology*, 54/2: 280–305.

Lacy, M. and Prince, D. (2013). *The Future of Digital Disrupters: Rethinking the Digital Divide*. Lancaster: Lancaster University.

Lacy, M. and Prince, D. (2018). Securitization and the Global Politics of Cybersecurity. *Global Discourse*, 8/1: 100-115.

Lake, D. A. and Baum M. A. (2001). The Invisible Hand of Democracy: Political Control and the Provision of Public Services. *Comparative Political Studies*, 34/6: 587-621.

Law on Amendments to the Constitution of the Ukrainian SSR (1990). *Zakon Pro Zmini i Dopovnennya Konstitutsii Ukrainskoi RSR*. Available at: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=404-12 (Accessed 29 March 2020).

Law on Amendments to the Constitution (2004). *Zakon Pro Vnesennya Zmin do Konstitutsii Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/2222-15?lang=ru (Accessed 26 March 2020).

Law on Amendments to the Constitution (2007). *Zakon Respubliki Kazahstan ot 21 Maya 2007 Goda N254-III “O Vnesenii Izmenenii i Dopolnenii v Konstitutsuiyu Respubliki Kazahstan”*. Available at: https://www.zakon.kz/87556-zakon-respubliki-kazakhstan-ot-21-maja.html (Accessed 30 September 2019).

Law on Amendments to the Constitution (2011). *Zakon Respubliki Kazahstan ot 2 Fevralya 2011 Goda N403-IV “O Vnesenii Dopolnenii v Konstitutsuiyu Respubliki Kazahstan”.* Available at: https://tengrinews.kz/zakon/parlament_respubliki_kazahstan/konstitutsionnyiy_stroy_i_osnovyi_gosudarstvennogo_upravleniya/id-Z1100000403/ (Accessed 30 September 2019).

Law on Amendments to Legislative Acts on the Activities of Internal Affairs Agencies (2014). *Zakon Respubliki Kazahstan ot 23 Aprelya 2014 Goda N200-V “O Vnesenii Izmenenii i Dopolnenii v Nekotorye Zakonodatelnye Akty po Voprosam Deyatelnosti Organov Vnutrennih Del”.* Available at:

https://tengrinews.kz/zakon/parlament_respubliki_kazahstan/konstitutsionnyiy_stroy_i_osnovyi_gosudarstvennogo_upravleniya/id-Z1400000200/ (Accessed 22 December 2018).

Law on Amendments to Legislative Acts on Issues of Countering Extremism and Terrorism (2016). *Zakon Respubliki Kazahstan ot 22 Dekabrya 2016 Goda N28-VI "O Vnesenii Izmenenii i Dopolnenii v Nekotorye Zakonodatelnye Akty po Voprosam Protivodeistviya Ekstremizmu i Terrorizmu".* Available at: http://online.zakon.kz/Document/?doc_id=34199995#pos=3;-250 (Accessed 23 December 2018).

Law on Amendments to Some Laws of Ukraine (2014). *Zakon Pro Vnesennya zmin do Zakonu "Pro Sudoustrii i Status Suddiv" ta Protsesualnih Zakoniv Shodo Dodatkovih Zahodiv Zahistu Bezpeki Gromadyan*. Available at: https://zakon.rada.gov.ua/laws/show/721-18 (Accessed 10 April 2020).

Law on Amendments to Some Legislative Acts of Ukraine to Counteract the Threats to National Security in the Information Sphere N6676 (2017). *Proekt Zakonu Pro Vnesennya Zmin do Deyakih Zakonodavchih Aktiv Ukraini Shodo Protidii Zagrozam Natsionalnii Bezpetsi v Informatsiinii Sferi N6676*. Available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62217 (Accessed 13 April 2020).

Law on Amendments to Some Legislative Acts of Ukraine to Counteract the Threats to National Security in the Information Sphere N6688 (2017). *Proekt Zakonu Pro Vnesennya Zmin do Deyakih Zakonodavchih Aktiv Ukraini Shodo Protidii Zagrozam Natsionalnii Bezpetsi v Informatsiinii Sferi N6688.* Available at: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236 (Accessed 13 April 2020).

Law on Communication (2004). *Zakon Respubliki Kazahstan ot 5 Iyulya 2004 Goda N567-II "O svyazi" (S Izmeneniyami i Dopolneniyami na 05.10.2018g.).* [*Law of The Republic of Kazakhstan of July 5, 2004, N567-II "On Communication" (With Amendments and Additions as of October 5, 2018)*]. Available at: https://online.zakon.kz/Document/?doc_id=1049207 (Accessed 22 December 2018).

Law on Elections (2004). *Zakon Pro Vibori Narodnih Deputativ Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/1665-15/ed20040325?lang=ru (Accessed 27 March 2020).

Law on Elections (2011). *Zakon Pro Vibori Narodnih Deputativ Ukraini*. Available at: https://zakon1.rada.gov.ua/laws/show/4061-17/print1439300349194235?lang=ru (Accessed 27 March 2020).

Law on Informatization (2015). *Zakon Respubliki Kazahstan ot 24 Noyabrya 2015 Goda N418-V “Ob Informatizatsii” (S Izmeneniyami i Dopolneniyami na 04.07.2018g.* [*Law of the Republic of Kazakhstan of November 24, 2015, N418-V “On Informatization” (With Amendments and Additions as of July 4, 2018)*]. Available at: https://online.zakon.kz/Document/?doc_id=33885902 (Accessed 22 December 2018).

Law on National Security (2012). Zakon Respubliki Kazahstan ot 6 Yanvarya 2012 Goda N527-IV “O Natsionalnoi Bezopasnosti (*S Izmeneniyami i Dopolneniyami na* 05.07.2018g.) [*Law of the Republic of Kazakhstan of January 6, 2012, N527-IV “On National Security of the Republic of Kazakhstan” (With Amendments and Additions as of July 5, 2018*]. Available at: https://online.zakon.kz/document/?doc_id=31106860 (Accessed 22 December 2018).

Law on Personal Data (2013). *Zakon Respubliki Kazahstan ot 21 Maya 2013 Goda N94-V “O Personalnyh Dannyh i ih Zashite” (S Izmeneniyami i Dopolneniyami na 28.12.2017g.).* [*Law of the Republic of Kazakhstan of May 21, 2013, N94-V “On Personal Data and its Protection” (with amendments and additions as of December 28, 2017)*] Available at: http://online.zakon.kz/Document/?doc_id=31396226#pos=43;-256 (Accessed 21 December 2018).

Law on Recognising Some Laws of Ukraine as Invalid (2014). *Zakon Pro Viznannya Takimi, Sho Vtratili Chinnist, Deyakih Zakoniv Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/732-18#n2 (Accessed 13 April 2020).

Law on State Policy in Donetsk and Luhansk Oblasts (2018). *Zakon Pro Osoblivosti Derzhavnoi Politiki iz Zabezpechennya Derzhavnogo Suverenitetu Ukraini na Timchasovo Okupovanih Teritoriyah u Dotetskii ta Luganskii Oblastyah*. Available at: https://zakon.rada.gov.ua/laws/show/2268-19 (Accessed 18 April 2020).

Law on Mass Media (1999). *Zakon Respubliki Kazahstan ot 23 Iyulya 1999 Goda N451-I "O Sredstvah Massovoi Informatsii" (S Izmeneniyami i Dopolneniyami na 24.05.2018g.).* [*Law of The Republic of Kazakhstan of July 23, 1999, N451-I "On Mass Media" (With Amendments and Additions as of May 24, 2018)*]. Available at: https://online.zakon.kz/Document/?doc_id=1013966 (Accessed 22 December 2018).

Law on the President and Amendments to the Constitution (1991). *Zakon Pro Zasnuvannya Posta Prezidenta Ukrainskoi RSR i Vnesennya Zmin ta Dopovnen do Konstitutsii Ukrainskoi RSR*. Available at: https://zakon.rada.gov.ua/laws/show/1293-12/ed19910705 (Accessed 26 March 2020).

Law on the Restoration of Some Provisions of the Constitution (2014). *Zakon Pro VIdnovlennya Dii Okremih Polozhen Konstitutsii Ukraini.* Available at: https://zakon.rada.gov.ua/laws/show/742-18?lang=ru (Accessed 27 March 2020).

Law on the Security Service of Ukraine (1992). *Zakon Pro Sluzhbu Bezpeki Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/2229-12 (Accessed 14 April 2020).

Law on the Ukrainian Language (2019). *Zakon Pro Zabespechennya Funktsionurovannya Ukrainskoi Movi Yak Derzhavnoi*. Available at: https://zakon.rada.gov.ua/laws/show/2704-19 (Accessed 14 April 2020).

Lawson, C. H. (2002). *Building the Fourth Estate: Democratization and the Rise of a Free Press in Mexico*. Berkeley: University of California Press.

Lenta (2015). Rada Potrebovala Zakryt Kanal "Inter" Iz-za Ugrozy Natsbezopasnosti. [The Rada Demanded to Close the "Inter" Channel Because of National Security Threats]. *Lenta*, 20 May. Available at: https://lenta.ru/news/2015/05/20/denyinter/ (Accessed 7 April 2020).

Letter of the Ministry of Information and Communication (2016). *Pismo Ministerstva Informatsii i Kommunikatsii Respubliki Kazahstan ot 15 Iyulya 2016 Goda N03-14/3м-л-73*. Available at: http://online.zakon.kz/Document/?doc_id=36894958#pos=0;73 (Accessed 21 December 2018).

Levitsky, S. and Ziblatt, D. (2018). *How Democracies Die: What History Reveals about Our Future*. New York: Penguin Books.

Lewin, M. (2016). *The Soviet Century*. London: Verso.

Lewis, D. (2016) Blogging Zhanaozen: Hegemonic Discourse and Authoritarian Resilience in Kazakhstan. *Central Asian Survey*, 35/3: 1-18.

Lillis, J. (2014). Kazakhstan Arrests Four Bloggers in a Week. *Eurasianet*, 11 February. Available at: https://eurasianet.org/kazakhstan-arrests-four-bloggers-in-a-week (Accessed 27 April 2020).

Lillis, J. (2019). *Dark Shadows: Inside the Secret World of Kazakhstan*. London: I.B. Tauris.

Lipow, A. and Seyd, P. (1996). The Politics of Anti-Partyism. *Parliamentary Affairs*, 49/2: 273-284.

Lokot, T. (2014). Ukraine's New "Ministry of Truth" Ridiculed on Social Media. *Global Voices*, 4 December. Available at: https://globalvoices.org/2014/12/04/ukraines-new-ministry-of-truth-ridiculed-on-social-media/ (Accessed 15 April 2020).

Lowndes, V. and Roberts, M. (2013). *Why Institutions Matter: The New Institutionalism in Political Science*. New York: Palgrave.

Lowndes, V. (2018). Institutionalism. In: Lowndes, V., Marsh, D. and Stoker G. (ed), *Theory and Methods in Political Science*. 4th ed. London: Palgrave, 54-74.

Lozovyi, V. and Davidenko, B. (2017). Pole Bitvy – Facebook. Skolko Botov "Zhivet" na Stranitse Petra Poroshenko. [The Battlefield – Facebook. How Many Bots "Live" on the Page of Petro Poroshenko]. *Vox Ukraine*, n/d. Available at: https://voxukraine.org/longreads/bots/article-ru.html (Accessed 15 April 2020).

Luhn, A. (2017). Ukraine Blocks Popular Social Networks as Part of Sanctions on Russia. The Guardian, 16 May. Available at: https://www.theguardian.com/world/2017/may/16/ukraine-blocks-popular-russian-websites-kremlin-role-war (Accessed on 14 October 2020).

Lynch, M. (2011). After Egypt: The Limits and Promise of Online Challenges to the Authoritarian Arab State. *Perspectives on Politics*, 9/2: 301-310.

MacKinnon, R. (2012). *Consent of the Networked: The Worldwide Struggle for Internet Freedom*. New York: Basic Books.

Makarenkov, N. and Galskaya, O. (2019). Ukrainskie Spetssluzhby Otkryli Sezon “Ohoty” na “Telefonnyh Separatistov”. [Ukrainian Special Forces Opened “Hunting” Season on “Telephone Separatists”. *Komsomolskaya Pravda*, 3 December 2019. Available at: https://www.kuban.kp.ru/daily/27063/4131771/ (Accessed 30 July 2020).

Mamashuly, A. (2011). Napravlenie “Karavana” Menyalos Kazhdyi Raz so Smenoi Vladeltsa. [The Direction of “Karavan” Changed Every Time with the Change of the Owner]. *Radio Azattyq*, 27 July. Available at: https://rus.azattyq.org/a/karawan_newspaper_/24277868.html (Accessed 26 October 2019).

Mamashuly, A. (2016a). Zablokirovan Sait s Petitsiei ob Otstavke Masimova. [A Website with a Petition of Masimov’s Resignation Was Blocked]. *Radio Azattyq*, 17 August. Available at: https://rus.azattyq.org/a/petitciya-ob-otstavke-masimova/27929203.html (Accessed 15 October 2020).

Mamashuly, A. (2016b). Tyuremnye Sroki Aktivistam Zamenili na Ogranichenie Svobody. [Jail Sentences of Activists Were Replaced with Freedom Restriction]. *Radio Azattyq*, 30 March. Available at: https://rus.azattyq.org/a/mabetalin-narymbaev-organichenie-svobody/27643606.html (Accessed 26 October 2020).

Mamyshev, Z. (2019). Sistemu Monitoringa Zapreshennogo Kontenta Prezentuyut Osenyu. [The Monitoring System Will Be Presented in Autumn]. *Kursiv*, 6 June. Available at: https://kursiv.kz/news/obschestvo/2019-06/sistemu-monitoringa-zapreschennogo-kontenta-prezentuyut-osenyu (Accessed 18 May 2020).

March, J. G. and Olsen, J. P. (1984). The New Institutionalism: Organizational Factors in Political Life. *The American Political Science Review*, 78/3: 734-749.

March, J. G. and Olsen, J. P. (1989). *Rediscovering Institutions*. New York: Free Press.

March, J. G. and Olsen, J. P. (2008). Elaborating the “New Institutionalism”. In: Binder, S. A., Rhodes, R. A. W. and Rockman, B. A. (ed), *The Oxford Handbook of Political Institutions*. Oxford: Oxford University Press, 3-20.

March, J. G. and Olsen, J. P. (2011). The Logic of Appropriateness. In: Goodin, R. E. (ed), *The Oxford Handbook of Political Institutions*. Oxford: Oxford University Press, 478-497.

Marczak, B., Guarnieri, C., Marquis-Boire, M. and Scott-Railton, J. (2014). Mapping Hacking Team's "Untraceable" Spyware. *The Citizen Lab*, 17 February. Available at: https://citizenlab.org/2014/02/mapping-hacking-teams-untraceable-spyware/ (Accessed 6 January 2019).

Marshall, T. (2016). *Prisoners of Geography: Ten Maps that Tell You Everything You Need to Know About Global Politics*. London: Elliot and Thompson Limited.

Marshall, M. G., Gurr, T. R. and Jaggers, K. (2018). *Polity IV Project: Political Regime Characteristics and Transitions, 1800-2017. Dataset Users' Manual*. Center for Systemic Peace.

Mayhew, D. R. (1974). *Congress: The Electoral Connection*. New Haven: Yale University Press.

Mayhew, D. R. (2004). *Congress: The Electoral Connection*. 2nd ed. New Haven: Yale University Press.

McGlinchey, E. and Johnson, E. (2007). Aiding the Internet in Central Asia. *Democratization*, 14/2: 273-288.

McMillan, J. and Zoido, P. (2004). How to Subvert Democracy: Montesinos in Peru. *Journal of Economic Perspectives,* 18/4: 69-92.

Mearsheimer, J. J. (2018). *The Great Delusion: Liberal Dreams and International Realities*. New Haven: Yale University Press.

Menn, J. (2016). Kazakh Dissidents and Lawyers Hit by Cyber Attacks: Researchers. *Reuters*, 2 August. Available at: https://www.reuters.com/article/us-kazakhstan-cyber/kazakh-dissidents-and-lawyers-hit-by-cyber-attacks-researchers-idUSKCN10D1N2 (Accessed on 21 June 2020).

Ministry of Information Policy (n/d). *Razvitie Informatsionnogo Prostranstva Ukrainy*. [*The Development of Information Space of Ukraine*]. Available at: https://mip.gov.ua/files/preza_2_ru.pdf (Accessed 14 April 2020).

Ministry of Information Policy (2017). *Perelik Saitiv, Yaki Mistya Informatsiyu, Sho Mae Oznaki Takoi, Sho Zaboronena do Rozpovsyudzhennya Normami Ukrainskogo Zakonodavstva*. [*List of Sites That Contain Information That Has Features That Are Prohibited from Dissemination by Norms of Ukrainian Lelislation*]. Available at: http://mip.gov.ua/documents/116.html (Accessed 14 April 2020).

Modi, N. (2020). PM Interacts with Print Media Journalists and Stakeholders. *Narendramodi.in*, 24 March. Available at: https://www.narendramodi.in/prime-minister-narendra-modi-interacts-with-print-media-journalists-and-stakeholders-548937 (Accessed 3 July 2020).

Moldabekov, D. (2015). Kak Prohodili Prezidentskie Vybory v Kazahstane: ot 1991 do 2015. [How Presidential Elections Were Held in Kazakhstan: From 1991 to 2015]. *Vlast*, 16 February. Available at: https://vlast.kz/politika/kak_prohodili_prezidentskie_vybory_v_kazahstane_ot_1991_do_2015-9681.html (Accessed 14 October 2014).

Moldabekov, D. (2017). Istorii Lyudei, Arestovannyh za Svoi Vzglyady. [Stories of People Arrested for Their Views]. *Vlast*, 14 November. Available at: https://vlast.kz/obsshestvo/25695-istorii-ludej-arestovannyh-za-svoi-vzglady.html (Accessed 26 April 2020).

Moore, M. (2018). *Democracy Hacked: Political Turmoil and Information Warfare in the Digital Age*. London: Oneworld Publications.

Morozov, E. (2011). *The Net Delusion: How Not to Liberate the World*. London: Penguin Books.

Morozov, E. (2012). Whither Internet Control?. In: Diamond, L. and Plattner, M. F. (ed), *Liberation Technology: Social Media and the Struggle for Democracy.* Baltimore: The Johns Hopkins University Press, 47-59.

Moses, J. W. and Knutsen, T. L. (2012). *Ways of Knowing: Competing Methodologies in Social and Political Research*. New York: Palgrave.

Motorevska, Y., Replianchuk, D., and Bidun, V. (2019). Inside a Ukrainian Troll Farm. *OCCRP*, 20 September. Available at: https://www.occrp.org/en/investigations/inside-a-ukrainian-troll-farm (Accessed 16 April 2020).

Mozilla (2019). Mozilla Takes Action to Protect Users in Kazakhstan. *The Mozilla Blog*, 21 August. Available at: https://blog.mozilla.org/blog/2019/08/21/mozilla-takes-action-to-protect-users-in-kazakhstan/ (Accessed 27 April 2020).

Mueller, M. (2002). *Ruling the Root: Internet Governance and the Taming of Cyberspace*. Cambridge, MA: MIT Press.

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

Mueller, M. (2017). *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity Press.

Mueller, M. (2019). Against Sovereignty in Cyberspace. *International Studies Review*, 0: 1-23.

Mukankyzy, M. (2013). Blogery Pridumali Slovosochetanie “Spisok Tazhina”. [Bloggers Made Up the Phrase “Tazhin’s List”]. *Radio Azattyq*, 27 February. Available at: https://rus.azattyq.org/a/blogery-kritikuyut-initsiativu-marata-tazhina/24913675.html (Accessed 27 April 2020).

Najar, N. (2017). Kashmir Shuts Down Social Networks for a Month. *New York Times*, 26 April. Available at: https://www.nytimes.com/2017/04/26/world/asia/kashmir-shuts-down-social-networks-for-a-month.html (Accessed 20 February 2020).

Nakashima, E. (2017). Inside a Russian Disinformation Campaign in Ukraine in 2014. *The Washington Post*, 25 December. Available at: https://www.washingtonpost.com/world/national-security/inside-a-russian-disinformation-campaign-in-ukraine-in-2014/2017/12/25/f55b0408-e71d-11e7-ab50-621fe0588340_story.html (Accessed 15 April 2020).

National Commission for the State Regulation of Communications and Informatization (n/d). *Informatsiine Povidomlennya do Uvagi Operatoriv, Provaideriv*. [*Information message to the attention of operators, telecommunications providers*]. Available at: https://nkrzi.gov.ua/index.php?r=site/index&pg=99&id=1516&language=uk (Accessed 14 April 2020).

National Security Committee (2019). V Otnoshenii Sertifikata Bezopasnosti. [With Regard to the Security Certificate]. *National Security Committee*, 6 August. Available at: http://knb.gov.kz/ru/news/v-otnoshenii-sertifikata-bezopasnosti (Accessed 18 May 2020).

Naughton, J. (2012). *From Gutenberg to Zuckerberg: What You Really Need to Know About the Internet.* London: Quercus.

Negroponte, N. (1995). *Being Digital*. London: Coronet.

Nekrasov, V. (2018). WebMoney Pod Sanktsiyami: Zachem Zapretili Servis i Kak Spasti Svoi Dengi. [WebMoney Under Sanctions: Why the Service Was Banned and How to Save Money]. *Ekonomicheskaya Pravda*, 28 May. Available at: https://www.epravda.com.ua/rus/publications/2018/05/28/637205/ (Accessed 8 April 2020).

Nielsen, N. (2018). Brexit Vote Manipulated, Says Data Whistleblower. *EUobserver*, 28 March. Available at: https://euobserver.com/justice/141470 (Accessed 4 July 2021).

North, D. C. and Thomas, R. P. (1973). *The Rise of the Western World: A New Economic History*. New York: Cambridge University Press.

North, D. C. (1990). *Institutions, Institutional Change and Economic Performance*. Cambridge: Cambridge University Press.

Novoe Vremya (2015). SBU Zaderzhala v Raione Provedeniya ATO Administratorov Antiukrainskih Soobshestv. [SBU Detained Administrators of Anti-Ukrainian Communities in the Area of ATO]. *Novoe Vremya*, 22 May. Available at: https://nv.ua/ukr/ukraine/events/sbu-zaderzhala-v-rayone-provedeniya-ato-administratorov-antiukrainskih-socsetey-49869.html (Accessed 9 April 2020).

NTV (2014). Ukraina Zapretila 14 Rossiiskih Televizionyh Kanalov. [Ukraine Banned 14 Russian TV Channels]. *NTV*, 19 August. Available at: https://www.ntv.ru/novosti/1199101/ (Accessed 7 April 2020).

Nurmakov, A. (2015). Mneniya Ekspertov o Prekrashenii Blokirovki LiveJournal v Kazahstane. [Expert Opinions on the Blockage Termination of LiveJournal in Kazakhstan]. *Digital Report*, 11 November. Available at: https://digital.report/livejournal-unblocked-in-kz-111115/ (Accessed 26 April 2020).

Nurmakov, A. (2016). Siloviki Kazahstana Poluchat Polnomochiya Po Otklyucheniyu Svyazi. [Security Forces of Kazakhstan Will Receive the Authority To Cut Off Communications]. *Digital Report*, 14 October. Available at: https://digital.report/siloviki-kazahstana-smogut-otklyuchat-svyazi/ (Accessed 6 February 2017).

Nurmukhanbetov, M. (2016). Sertifikat Bezopasnosti Kak Metod Kontrolya Nad Sotssetyami. [The Security Certificate as a Method of Control of Social Media]. *Central Asia Monitor*, 29 July. Available at: https://camonitor.kz/24618-sertifikat-bezopasnosti-kak-metod-kontrolya-nad-socsetyami.html (Accessed 26 April 2020).

Nye, J. (2011). *The Future of Power.* New York: Public Affairs.

Oates, S. (2013). *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere.* Oxford: Oxford University Press.

Olcott, M. B. (2005). *Central Asia's Second Chance*. Washington: Carnegie Endowment for International Peace.

Olcott, M. B. (2010). *Kazakhstan: Unfulfilled Promise?*. Washington: Carnegie Endowment for International Peace.

Oltermann, P. (2018). Tough New German Law Puts Tech Firms and Free Speech in Spotlight. *The Guardian*, 5 January. Available at: https://www.theguardian.com/world/2018/jan/05/tough-new-german-law-puts-tech-firms-and-free-speech-in-spotlight (Accessed 1 July 2020).

Ott, M. and Lozovyi, V. (2019). Erase This If You Can. What Ukrainian Bots Are Doing on Ukrainian Politicians' Pages. *Vox Ukraine*, 7 August. Available at:

https://voxukraine.org/en/erase-this-if-you-can-what-ukrainian-bots-are-doing-on-ukrainian-politicians-pages/ (Accessed 16 April 2020).

Palfrey, J. (2010). Four Phases of Internet Regulation. *Social Research*, 77/3: 981-996.

Palmer, M. (2003). *Breaking the Real Axis of Evil: How to Oust the World's Last Dictators by 2025.* Oxford: Rowman and Littlefield Publishers.

Pennings, P. (2003). Beyond Dichotomous Explanations: Explaining Constitutional Control of the Executive with Fuzzy-Sets. *European Journal of Political Research*, 42: 541-567.

Peters, B. (2017). *How Not to Network a Nation: The Uneasy History of the Soviet Internet*. Cambridge, MA: MIT Press.

Peters, B. G. (2019). *Institutional Theory in Political Science: The New Institutionalism*. 4th ed. Cheltenham: Edward Edgar Publishing.

Pfeifle, M. (2009). A Nobel Peace Prize for Twitter?. *The Christian Science Monitor*, 6 July. Available at: https://www.csmonitor.com/Commentary/Opinion/2009/0706/p09s02-coop.html (Accessed 8 January 2020).

Phartiyal, S., Kalra, A. and Shah, A. (2020). India Bans 59 Mostly Chinese Apps Amid Border Crisis. *New York Times*, 29 June. Available at: https://www.nytimes.com/reuters/2020/06/29/technology/29reuters-india-china-apps.html (Accessed 1 July 2020).

Picheta, R. and Halasz, S. (2020). Hungarian Parliament Votes to Let Viktor Orban Rule by Decree in Wake of Coronavirus Pandemic. *CNN*, 30 March. Available at: https://edition.cnn.com/2020/03/30/europe/hungary-viktor-orban-powers-vote-intl/index.html (Accessed 30 June 2020).

Plokhy, S. (2017). *Lost Kingdom: A History of Russian Nationalism from Ivan the Great to Vladimir Putin*. London: Penguin Books.

Poludenko-Young, A. (2015). Ukraine's Security Service Takes Down 30,000 Websites to Fight 'Pro-Russian Propaganda'. *Global Voices*, 28 April. Available at:

https://globalvoices.org/2015/04/28/ukraine-censorship-russia-propaganda-hosting/ (Accessed 7 April 2020).

Pomerantsev, P. (2019a). The Disinformation Age: A Revolution in Propaganda. *The Guardian*, 27 July. Available at: https://www.theguardian.com/books/2019/jul/27/the-disinformation-age-a-revolution-in-propaganda (Accessed 28 June 2020).

Pomerantsev, P. (2019b). *This is Not Propaganda: Adventures in the War Against Reality*. London: Faber & Faber.

Powers, S. M. and Jablonski, M. (2015). *The Real Cyber War: The Political Economy of Internet Freedom*. Chicago: University of Illinois Press.

Presidential Order to Discuss Constitutional Amendments (2003). *Ukaz Prezidenta Ukraini Pro Vnesennya na Vsenarodne Obgovorennya Proektu Zakonu Ukraini "Pro Vnesennya Zmin do Konstitutsii Ukraini"*. Available at: https://zakon.rada.gov.ua/laws/show/197/2003?lang=ru (Accessed 26 March 2020)

Privacy International (2014). *Private Interests: Monitoring Central Asia*. London: Privacy International. Available at: https://privacyinternational.org/sites/default/files/2017-12/Private%20Interests%20with%20annex_0.pdf (Accessed 14 October 2020).

Putz, C. (2019). Kazakhstan and Uzbekistan: A Tale of Blocking and Unblocking. *The Diplomat*, 13 May. Available at: https://thediplomat.com/2019/05/kazakhstan-and-uzbekistan-a-tale-of-blocking-and-unblocking/ (Accessed 22 February 2020).

Radchenko, S. and Rakhmetov, B. (2020). Putin Is Ruling Russia Like a Central Asian Dictator. *Foreign Policy*, 6 August. Available at: https://foreignpolicy.com/2020/08/06/putin-ruling-russia-like-a-kazakhstan-kyrgyzstan-uzbekistan-tajikistan-belarus-central-asian-dictator/ (Accessed 17 October 2020).

Radio Azattyq (2011). Na Stantsii Shetpe Izbit Bloger Murat Tungishbaev. [Blogger Murat Tungishbayev Was Beaten at the Shetpe Station]. *Radio Azattyq*, 18 December. Available at: https://rus.azattyq.org/a/24425730.html (Accessed 26 April 2020).

Radio Azattyq (2014). Sait s Petitsiei "Ob Impichmente Nazarbaeva" Zablokirovan. [The site with a Petition "of Nazarbayev Impeachment" Was Blocked]. *Radio Azattyq*, 13

February. Available at: https://rus.azattyq.org/a/peticia-onlain-otstavka-nazarbaeva/25262258.html (Accessed 15 October 2020).

Radio Azattyq (2015). Shevtsova-Valova Prigovorena k Uslovnomu Sroku. [Shevtsova-Valova is Sentenced to a Conditional Sentence]. *Radio Azattyq*, 31 March. Available at: https://rus.azattyq.org/a/26929851.html (Accessed 26 April 2020).

Radio Free Europe (2005). Kazakhstan Suspends Website of British Comedian. *Radio Free Europe*, 13 December. Available at: https://www.rferl.org/a/1063792.html (Accessed 25 April 2020).

Radio Free Europe (2018a). Fugitive Tycoon's Political Movement Found 'Extremist' in Kazakhstan. *Radio Free Europe*, 13 March. Available at: https://www.rferl.org/a/kazakhstan-ablyazov-extremist-nazarbaev-democratic-choice/29096171.html (Accessed 27 December 2018).

Radio Free Europe (2018b). Fugitive Kazakh Banker, Nazarbaev Foe Sentenced To Life In Prison. *Radio Free Europe*, 27 November. Available at: https://www.rferl.org/a/fugitive-kazakh-banker-nazarbaev-foe-sentenced-to-life-in-prison/29623588.html (Accessed 27 December 2018).

Rafal, A. (2017). "Mogerini Skazala Poroshenko: "Libo Vy Otpuskaete Kotsabu, Libo Bolshe Syuda Ne Priezshaete". ["Mogerini Told Poroshenko: "Either You Free Kotsaba, Or You Never Come Here"]. *Strana*, 30 May. Available at: https://strana.ua/articles/analysis/73424-ruslan-kocaba-luchshe-uzhasnyj-konec-chem-uzhas-bez-konca.html (Accessed 9 April 2020).

Ragin, C. C. (1987). *The Comparative Method: Moving Beyond Qualitative and Quantitative Strategies*. California: University of California Press.

Ragin, C. C. (2000). *Fuzzy-Set Social Science*. Chicago: University of Chicago Press.

Ragin, C. C. (2008). *Redesigning Social Inquiry: Fuzzy Sets and Beyond*. Chicago: University of Chicago Press.

Rakhmetov, B. and Valeriano, B. (2020). Widening the Aperture on the Study of Internet Control. *Council on Foreign Policy (Net Politics)*, 12 November. Available at:

https://www.cfr.org/blog/widening-aperture-study-internet-control (Accessed 18 November 2020).

Raman, R. S., Evdokimov, L., Wustrow, E., Halderman, A., and Ensafi, R. (2019). Kazakhstan's HTTPS Interception. *Censored Planet*, 23 July. Available at: https://censoredplanet.org/kazakhstan (Accessed 18 May 2020).

Rappler (2020). PNP Files Complaint vs Cavite Town Mayor For 'Causing Coronavirus Scare'. *Rappler*, 28 March. Available at: https://www.rappler.com/nation/256209-pnp-files-criminal-charges-noveleta-cavite-mayor-coronavirus-scare (Accessed on 1 July 2020).

Rasmussen, S. E. (2017). Pakistan: Man Sentenced to Death for Blasphemy on Facebook. *The Guardian*, 11 June. Available at: https://www.theguardian.com/world/2017/jun/11/pakistan-man-sentenced-to-death-for-blasphemy-on-facebook (Accessed 21 June 2020).

Ratcliffe, R. (2020). Journalist Maria Ressa Found Guilty of 'Cyberlibel' in Philippines. *The Guardian*, 15 June. Available at: https://www.theguardian.com/world/2020/jun/15/maria-ressa-rappler-editor-found-guilty-of-cyber-libel-charges-in-philippines (Accessed 28 June 2020).

Rayman, N. (2014). Putin: The Internet Is a 'CIA Project'. *Time*, 24 April. Available at: https://time.com/75484/putin-the-internet-is-a-cia-project/ (Accessed 22 January 2020).

Razina, A. (2016). 25 Let Nezavisimosti. 1995 God – Novaya Konstitutsiya, Sobstvennye Tenge i Prodlenie Polnomochii Prezidenta. [25 Years of Independence. 1995 – New Constitution, Own Tenge, And Extension of President's Authorities]. *Informburo*, 9 December. Available at: https://informburo.kz/stati/25-let-nezavisimosti-1995-god-novaya-konstituciya-sobstvennye-tenge-i-prodlenie-polnomochiy-prezidenta.html (Accessed 27 September 2019).

RBC (2011). Dosrochnye Vybory Prezidenta Kazahstana Naznacheny na Aprel. [Extraordinary Presidential Elections of Kazakhstan Are to be Held in April]. *RBC*, 4 February. Available at: https://www.rbc.ru/politics/04/02/2011/5703e30e9a79473c0df19e84 (Accessed 18 May 2020).

Reed, T. V. (2014). *Digitized Lives: Culture, Power and Social Change in the Internet Era.* New York: Routledge.

Republic Act (2020). *Republic Act No. 11469 (The Bayanihan to Heal as One Act)*. Available at: https://www.senate.gov.ph/Bayanihan-to-Heal-as-One-Act-RA-11469.pdf (Accessed 1 July 2020).

Reporters without Borders (n/d). Detailed Methodology. *Reporters without Borders*. Available at: https://rsf.org/en/detailed-methodology (Accessed 27 December 2018).

Reporters without Borders (2003a). Sergei Duvanov Sentenced, On Appeal, To Three and A Half Years in Prison – Reporters Without Borders Denounces What It Considers A Parody of Justice. *Reporters without Borders*, 11 March. Available at: https://rsf.org/en/news/sergei-duvanov-sentenced-appeal-three-and-half-years-prison-reporters-without-borders-denounces-what (Accessed 26 April 2020).

Reporters without Borders (2003b). Journalist Still Facing Up to Seven Years in Prison For "Inciting Hatred". *Reporters without Borders*, 15 July. Available at: https://rsf.org/en/news/journalist-still-facing-seven-years-prison-inciting-hatred (Accessed 26 April 2020).

Reporters without Borders (2004). Third Annual Worldwide Press Freedom Index (2004). *Reporters without Borders.* Available at: https://rsf.org/en/third-annual-worldwide-press-freedom-index-2004 (Accessed 9 April 2020).

Reporters without Borders (2005). Worldwide Press Freedom Index 2005. *Reporters without Borders.* Available at: https://rsf.org/en/worldwide-press-freedom-index-2005 (Accessed 26 April 2020).

Reporters without Borders (2009). World Press Freedom Index 2009. *Reporters without Borders.* Available at: https://rsf.org/en/world-press-freedom-index-2009 (Accessed 9 April 2020).

Reporters without Borders (2010). Worldwide Press Freedom Index 2010. *Reporters without Borders.* Available at: https://rsf.org/en/world-press-freedom-index-2010 (Accessed 26 April 2020).

Reporters without Borders (2013a). RWB Supports Independent Probe into Brutal Attack on Reporter. *Reporters without Borders*, 27 December. Available at: https://rsf.org/en/news/rwb-supports-independent-probe-brutal-attack-reporter (Accessed 9 April 2020).

Reporters without Borders (2013b). World Press Freedom Index 2013. *Reporters without Borders.* Available at: https://rsf.org/en/world-press-freedom-index-2013 (Accessed 9 April 2020).

Reporters without Borders (2015). 2015 World Press Freedom Index. *Reporters without Borders.* Available at: https://rsf.org/en/ranking/2015 (Accessed 26 April 2020).

Reporters without Borders (2017). RSF Urges Ukraine To Scrap Ban on Russian Social Media Sites. *Reporters without Borders*, 23 May. Available at: https://rsf.org/en/news/rsf-urges-ukraine-scrap-ban-russian-social-media-sites (Accessed 8 April 2020).

Reporters without Borders (2018). 2018 World Press Freedom Index. *Reporters without Borders.* Available at: https://rsf.org/en/ranking/2018 (Accessed 9 April 2020).

Reporters without Borders (2019). 2019 World Press Freedom Index. *Reporters without Borders.* Available at: https://rsf.org/en/ranking/2019 (Accessed 9 April 2020).

Reporters without Borders (2020a). RSF Unveils 20/2020 List of Press Freedom's Digital Predators. *Reporters without Borders*, 10 March. Available at: https://rsf.org/en/news/rsf-unveils-202020-list-press-freedoms-digital-predators (Accessed 5 July 2020).

Reporters without Borders (2020b). How India's Government Tries to Suppress All Covid-19 Reporting. *Reporters without Borders*, 12 April. Available at: https://rsf.org/en/news/how-indias-government-tries-suppress-all-covid-19-reporting (Accessed 3 July 2020).

Reporters without Borders (2020c). Nearly Half of UN Member Countries Have Obstructed Coronavirus Coverage. *Reporters without Borders*, 29 June. Available at: https://rsf.org/en/news/nearly-half-un-member-countries-have-obstructed-coronavirus-coverage (Accessed 3 July 2020).

Reporters without Borders (2020d). 2020 World Press Freedom Index. *Reporters without Borders.* Available at: https://rsf.org/en/ranking/2020 (Accessed 26 April 2020).

Ressa, M. (2016). Propaganda War: Weaponizing the Internet. *Rappler*, 3 October. Available at: https://www.rappler.com/nation/148007-propaganda-war-weaponizing-internet (Accessed 28 June 2020).

Rets, I. (2019). "Ne Bylo Somnenii, Chto Nas Ubyut": Kak "Berkut" Izbival Zhurnalistov. [There Were No Doubts We Would be Killed": How "Berkut" Beat Journalists]. *Segodnya*, n/d. Available at: https://www.segodnya.ua/longread/izbienie-zhurnalistov-na-bankovoy/index.html (Accessed 9 April 2020).

RIA Novosti (2018a). V Kremle Prokommentirovali Vozmozhnost Obmena Vyshinskogo. [The Kremlin Commented on the Exchange of Vyshinsky]. *RIA Novosti*, 22 May. Available at: https://ria.ru/20180522/1521071559.html (Accessed 10 April 2020).

RIA Novosti (2018b). Shef-Redaktor Ukrainskogo Radio "Vesti" Nazval Zahvat Ofisa Reiderstvom. [Chief-Editor of Ukrainian Radio "Vesti" Called the Seizure of the Office Raid]. *RIA Novosti*, 8 February. Available at: https://ria.ru/20180208/1514234733.html (Accessed 10 April 2020).

RIA Novosti (2019). Delo Kirilla Vyshinskogo. [The Case of Kirill Vyshinsky]. *RIA Novosti*, 28 August. Available at: https://ria.ru/20190828/1557987985.html (Accessed 10 April 2020).

Roberts, M.E. (2018). *Censored: Distraction and Diversion Inside China's Great Firewall*. Princeton and Oxford: Princeton University Press.

Rød and Weidmann (2015). Empowering Activists or Autocrats? The Internet in Authoritarian Regimes. *Journal of Peace Research*, 52/3: 338-351.

Romanov, A. (2018). Kak v Ukraine Sazhayut za Posty v Facebook. Ot Treh Do Pyati Let – Realnye Prigovory Za Publikatsiyu "Kramoly" v Sotssetyah. [How People Are Imprisoned for Posts on Facebook on Ukraine. From Three to Five Years – Real Sentences for the Publication of "Sedition" on Social Media]. *Strana*, 24 March. Available at: https://strana.ua/articles/rassledovania/131274-sudy-v-ukraine-nachali-vynosit-realnye-prihovory-za-posty-v-facebook.html (Accessed 10 April 2020).

Rosenbach, E. and Mansted, K. (2019). How to Win the Battle Over Data: The United States Dithers While Authoritarians Seize the Day. *Foreign Affairs,* 17 September. Available at: https://www.foreignaffairs.com/articles/2019-09-17/how-win-battle-over-data (Accessed 17 October 2020).

Rosenberger, L. (2020). Making Cyberspace Safe for Democracy: The New Landscape of Information Competition. *Foreign Affairs*, 99/3: 146-159.

Rudyk, A. (2019). V Telegram Poroshenko Opublikovali Video, Kak Zelenskogo Sbivaet Fura. [In Poroshenko's Telegram, a Video How Zelensky Is Hit By a Truck Has Been Published]. *Ukrainian News*, 11 April. Available at: https://ukranews.com/news/625591-u-poroshenko-smontirovali-video-na-kotorom-fura-sbivaet-zelenskogo (Accessed 16 April 2020).

Runciman, D. (2018). *How Democracy Ends*. London: Profile Books.

Ryan, M. (2018). The Comparative Method. In: Lowndes, V., Marsh, D. and Stoker G. (ed), *Theory and Methods in Political Science*. 4th ed. London: Palgrave, 271-289.

Rzheutskaya, L. (2019). Bez "Vkontakte" i Mail.ru: Chto Dala Blokirovka Rossiiskih Saitov i Nuzhno Li Menyat Strategiyu. [Without "Vkontakte" and Mail.ru: What the Blockage of Russian Sites Gave and Whether the Strategy Should Be Changed]. *WIC*, 16 December. Available at: https://zik.ua/ru/news/2019/12/16/bez_vkontakte_i_mailru_chto_dala_blokirovka_rossiyskih_saytov_i_nuzhno_li_menyat_strategiyu_950233 (Accessed 8 April 2020).

Sanovich, S., Stukal, D. and Tucker J. A. (2018). Turning the Virtual Tables: Government Strategies for Addressing Online Opposition with an Application to Russia. *Comparative Politics*, 50/3: 435-482.

Sagar (2020). Speaking Positivity to Power. *The Caravan*, 31 March. Available at: https://caravanmagazine.in/media/hours-before-lockdown-modi-asked-print-media-owners-editors-refrain-negative-covid-coverage (Accessed 3 July 2020).

Sakwa, R. (2016). *Frontline Ukraine: Crisis in the Borderlands*. London: I.B. Tauris.

Savage-Smith, E. (2003). Islam. In: Porter, R. (ed), *The Cambridge History of Science: Volume 4, Eighteenth-Century Science*. New York: Cambridge University Press, 649-668.

Schneider, C. Q. and Wagemann, C. (2012). *Set-Theoretic Methods for the Social Sciences: A Guide to Qualitative Comparative Analysis*. Cambridge: Cambridge University Press.

Schramm, W. (1956). The Soviet Communist Theory of the Press. In: Seibert, F. S., Peterson, T. and Schramm, W., *Four Theories of the Press: The Authoritarian, Libertarian, Social Responsibility and Soviet Communist Concepts of What the Press Should Be and Do*. Urbana and Chicago: University of Illinois Press, 105-146.

Schumpeter, J. A. (2010). *Capitalism, Socialism and Democracy*. London and New York: Routledge.

Scott, W. R. (2014). *Institutions and Organizations: Ideas, Interests, and Identities*. 4th ed. Los Angeles: SAGE Publications.

Security Service of Ukraine (2017). *The Press Center of Security Service of Ukraine*, 11 July. Available at: https://www.sbu.gov.ua/en/news/338/category/21/view/3685#.5fePl7fj.dpbs (Accessed 8 April 2020).

Security Service of Ukraine (2018a). *The Press Center of Security Service of Ukraine*, 22 December. Available at: https://sbu.gov.ua/en/news/5/category/302/view/5545#.20ckGiWj.dpbs (Accessed 10 April 2020).

Security Service of Ukraine (2018b). *The Press Center of Security Service of Ukraine,* 22 February*.* https://ssu.gov.ua/en/news/1/category/2/view/4424#.6WJx6CwL.dpbs (Accessed 10 April 2020).

Security Service of Ukraine (2018c). *The Press Center of Security Service of Ukraine*, 22 March. https://ssu.gov.ua/en/news/1/category/1/view/4544#.26J9XCcO.dpbs (Accessed 10 April 2020).

Security Service of Ukraine (2019a). *The Press Center of Security Service of Ukraine*, 16 April. Available at: https://ssu.gov.ua/en/news/1/category/1/view/5971#.sx8cgmSS.dpbs (Accessed 10 April 2020).

Security Service of Ukraine (2019b). *The Press Center of Security Service of Ukraine*, 8 May. Available at: https://www.sbu.gov.ua/en/news/46/category/78/view/6022#.0d0NR6HX.dpbs (Accessed 10 April 2020).

Segal, A. (2016). *The Hacked World Order: How Nations Fight, Trade, Maneuver, and Manipulate in the Digital Age.* New York: Public Affairs.

Segodnya (2019). Ukrainets Poluchil Pyat Let Za Prizyvy k Otdeleniyu Odessy ot Ukrainy. [Ukrainian Was Sentenced to Five Years for Calls of Separation of Odessa from Ukraine]. *Segodnya*, 15 April. Available at: https://www.segodnya.ua/regions/odessa/ukrainec-poluchil-pyat-let-za-prizyvy-k-otdeleniyu-odessy-ot-ukrainy-1253872.html (Accessed 10 April 2020).

Seibert, F. S. (1956). The Authoritarian Theory. In: Seibert, F. S., Peterson, T. and Schramm, W., *Four Theories of the Press: The Authoritarian, Libertarian, Social Responsibility and Soviet Communist Concepts of What the Press Should Be and Do*. Urbana and Chicago: University of Illinois Press, 9-37.

Seibert, F. S., Peterson, T. and Schramm, W. (1956). *Four Theories of the Press: The Authoritarian, Libertarian, Social Responsibility and Soviet Communist Concepts of What the Press Should Be and Do*. Urbana and Chicago: University of Illinois Press.

Selezneva, I. (2018). 9 Tysyach Saitov Zablokirovali v 2017 Godu v Kazahstane. [9 Thousand Sites Were Blocked in 2017 in Kazakhstan]. *Zakon*, 16 Februaty. Available at: https://www.zakon.kz/4904265-9-tysyach-saytov-zablokirovali-v-2017.html (Accessed 6 January 2019).

Skliarevska, G. (2018). Minstets, Arbuzov i Lyshko: Chto Obshego u Politikov v Sotssetyah. [Minstets, Arbuzov, and Lyshko: What Is Common Among Politicians on Social Media]. *Detector Media*, 19 March. Available at:

https://detector.media/infospace/article/135736/2018-03-19-minstets-arbuzov-i-lyashko-chto-obshchego-u-politikov-v-sotssetyakh/ (Accessed 15 April 2020).

Shahid, K. K. (2018). Could Facebook Data Leaks Impact Pakistan's Elections?. *The Diplomat*, 1 May. Available at: https://thediplomat.com/2018/05/could-facebook-data-leaks-impact-pakistans-elections/ (Accessed 20 February 2020).

Shimer, D. (2017). Germany Raids Homes of 36 People Accused of Hateful Postings Over Social Media. *New York Times*, 20 June. Available at: https://www.nytimes.com/2017/06/20/world/europe/germany-36-accused-of-hateful-postings-over-social-media.html (Accessed 22 February 2020).

Shirk, S. L. (1993). *The Political Logic of Economic Reform in China*. Berkeley: University of California Press.

Shirky, C. (2008). *Here Comes Everybody: How Change Happens When People Come Together*. London: Penguin Books.

Shumilin, A. (2017). Rada Podderzhala "Ruchnoe" Naznazhenie Gubernatorov. [Rada Supported the "Manual" Appointment of Governors]. *Ukrainskaya Pravda*, 9 November. Available at: https://www.pravda.com.ua/rus/news/2017/11/9/7161224/ (Accessed 30 March 2020).

Shumilin, A. (2019). Shtab Poroshenko Publikuyet na Bordah i v Gazetah Putina, a ne Zelenskogo. [Poroshenko's HQ Publishes Putin, not Zelensky, on Boards and in Newspapers]. *Ukrainskaya Pravda*, 9 April. Available at: https://www.pravda.com.ua/rus/news/2019/04/9/7211701/ (Accessed 16 April 2020).

Siapera, E. (2018). *Understanding New Media*. 2nd ed. London: SAGE Publications.
Singer, P. W. and Friedman A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know.* New York: Oxford University Press.

Singer, P. W. and Brooking, E. T. (2018). *LikeWar: The Weaponization of Social Media*. New York: Houghton Mifflin Harcourt Publishing Company.

Siripurapu, A. (2020). Trump and Section 230: What to Know. *Council on Foreign Relations*, 2 December. Available at: https://www.cfr.org/in-brief/trump-and-section-230-what-know (Accessed 4 July 2021).

Snyder, T. (2011). *Bloodlands: Europe Between Hitler and Stalin*. London: Penguin Books.

Soldatov, A. and Borogan, I. (2012). In Ex-Soviet States, Russian Spy Tech Still Watches You. *Wired*, 21 December. Available at: https://www.wired.com/2012/12/russias-hand/ (Accessed 16 April 2020).

Soldatov, A. and Borogan, I. (2017). *Bitva za Runet: Kak Vlast Manipuliruet Informatsiei i Sledit Za Kazhdym Iz Nas*. [*The Struggle for Runet: How the Government Manipulates Information and Watches Each of Us*]. Moscow: Alpina Digital.

Soldatov, A. (2019). Why Russia Might Shut Off the Internet: The Kremlin's Long Obsession with Central Control. *Foreign Affairs*, 29 March. Available at: https://www.foreignaffairs.com/articles/russian-federation/2019-03-29/why-russia-might-shut-internet (Accessed 8 January 2020).

Spar D. L. (2001). *Ruling the Waves: Cycles of Discovery, Chaos, and Wealth from the Compass to the Internet*. New York: Harcourt, Inc.

Spirin, E. (2019). 5 Dnei Do Vtorogo Tura. Agentstvo, Kotoroe Vedet Sotsseti Poroshenko, Prodvigaet Roliki o "Narkomane Zelenskom". My Vyyasnili, Skolko Eto Stoit. [5 Day Before the Second Round. The Agency, Which Manages Poroshenko's Social Media, Promotes Videos About "Drug Addict Zelensky". We Found Out How Much It Costs]. *Babel*, 16 April. Available at: https://babel.ua/ru/texts/28810-5-dney-do-vtorogo-tura-agentstvo-kotoroe-vedet-socseti-poroshenko-prodvigaet-roliki-o-narkomane-zelenskom-my-vyyasnili-skolko-eto-stoit?utm_source=page&utm_medium=publication (Accessed 16 April 2020).

Sputnik Kazakhstan (n/d). Hronologiya Vyborov Prezidenta Kazahstana. [Chronology of Elections of President of Kazakhstan]. *Sputnik Kazakhstan,* (n/d). Available at: https://ru.sputniknews.kz/spravka/20190319/9203775/hronologiya-vybory-prezident-kazakhstan.html (Accessed 15 October 2019).

Standage, T. (1999). *The Victorian Internet: The Remarkable Story of the Telegraph and the Nineteenth Century's Online Pioneers*. London: Phoenix.

Statista (2020). *Number of Monthly Active Facebook Users Worldwide as of 2nd Quarter 2020 (In Millions)*. Statista.com. Available at: https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/ (Accessed 15 September 2020).

Stevens, T. (2015). *Cyber Security and the Politics of Time*. Cambridge: Cambridge University Press.

Sukumaran, T. and Jaipragas, B. (2020). Coronavirus: Hundreds Arrested as Malaysia Cracks Down on Migrants in Covid-19 Red Zones. *South China Morning Post*, 1 May. Available at: https://www.scmp.com/week-asia/politics/article/3082529/coronavirus-hundreds-arrested-malaysia-cracks-down-migrants (Accessed 1 July 2020).

Tambini, D. (1999). New Media and Democracy: The Civic Networking Movement. *New Media and Society*, 1/3: 305-329.

Teachout, Z. (2021). We're Better Off Without Trump on Twitter. And Worse Off With Twitter in Charge. *Washington Post*, 14 January. Available at: https://www.washingtonpost.com/outlook/2021/01/14/trump-twitter-ban-big-tech-monopoly-private/ (Accessed 4 July 2021).

The Agreement on the Settlement of the Crisis in Ukraine (2014). Soglashenie ob Uregulirovanii Krisiza na Ukraine. *BBC*, 21 February. Available at: https://www.bbc.com/russian/international/2014/02/140221_ukraine_agreement_text (Accessed 27 March 2020).

The Common Declaration (2007). *Spilna Zayava Prezidenta Ukraini, Golovi Verhovnoi Radi Ukraini i Premer-Ministra Ukraini*. Available at: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=n0009100%2D07 (Accessed 27 March 2020).

The Concept of Cybersecurity (Cybershield of Kazakhstan) (2017). *Ob Utverzhdenii Kontseptsii Kiberbezopasnosti ("Kibershit Kazahstana")*. Available at: https://tengrinews.kz/zakon/pravitelstvo_respubliki_kazahstan_premer_ministr_rk/hozyaystvennaya_deyatelnost/id-P1700000407/ (Accessed 16 January 2019).

The Concept of Information Security of Kazakhstan (2006). *O Kontseptsii Informatsionnoi Bezopasnosti Respubliki Kazahstan*. Available at: https://tengrinews.kz/zakon/prezident_respubliki_kazahstan/hozyaystvennaya_deyatelnost/id-U060000199_/ (Accessed 8 January 2019).

The Concept of Information Security up to 2016 (2011). *O Kontseptsii Informatsionnoi Bezopasnosti Respubliki Kazahstan do 2016 Goda*. Available at: https://tengrinews.kz/zakon/prezident_respubliki_kazahstan/kultupa/id-U1100000174/ (Accessed 8 January 2019).

The Constitutional Agreement (1995). *Konstitutsiinii Dogovir Mizh Verhovnoyu Radoyu Ukaini ta Prezidentom Ukaini*. Available at: https://zakon.rada.gov.ua/laws/show/1%D0%BA/95-%D0%B2%D1%80?lang=ru (Accessed 26 March 2020).

The Constitution of the Kazakh Soviet Social Republic (1978). *Konstitutsiya (Osnovnoi Zakon) Kazahskoi Sovetskoi Sotsialisticheskoi Respubliki.* Available at: https://online.zakon.kz/Document/?doc_id=1027292 (Accessed 27 April 2020).

The Constitution of the Republic of Kazakhstan (1995). Available at: http://www.akorda.kz/en/official_documents/constitution (Accessed 27 September 2019).

The Constitution of Ukraine (1996). *Konstitutsiya Ukrainy*. Available at: https://zakon4.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80 (Accessed 26 March 2020).

The Constitutional Council (2000). *Normativnoe Postanovlenie Konstitutsionnogo Soveta Respubliki Kazahstan N12/2*. [*Normative Resolution of the Constitutional Council of the Republic of Kazakhstan N12/2*]. Available at: http://ksrk.gov.kz/solutions/np-ks-rk-ot-20062000-g-no122-ob-oficialnom-tolkovanii-punkta-5-stati-42-konstitucii (Accessed 9 July 2020).

The Criminal Code of Kazakhstan (2014). *Ugolovnyi Kodeks Respubliki Kazahstan*. Available at: https://online.zakon.kz/document/?doc_id=31575252#pos=5;-110 (Accessed 27 April 2020).

The Criminal Code of Ukraine (2001). *Kriminalnii Kodeks Ukraini*. Available at: https://zakon.rada.gov.ua/laws/show/2341-14 (Accessed 13 April 2020).

The Declaration of State Sovereignty of Ukraine (1990). *Deklaratsiya Pro Derzhavnii Suverenitet Ukrainy*. Available at: https://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=55-12 (Accessed 29 March 2020).

The Doctrine of Information Security of Ukraine (2017). *Pro Doktrinu Informatsiinoi Bezpeki Ukraini*. Available at: https://www.president.gov.ua/documents/472017-21374 (Accessed 13 April 2020).

The Economist (2013). A Giant Cage. *The Economist*, 6 April. Available at: https://www.economist.com/special-report/2013/04/06/a-giant-cage (Accessed 14 January 2020).

The Economist Intelligence Unit (2015). *Democracy Index 2014: Democracy and its Discontents*. London: EIU.

The Economist Intelligence Unit (2018). *Democracy Index 2017: Free Speech Under Attack.* London: EIU.

The Economist Intelligence Unit (2020). *Democracy Index 2019: A Year of Democratic Setbacks and Popular Protest*. London: EIU.

The Guardian (2017). Man Jailed for 35 Years in Thailand for Insulting Monarchy on Facebook. *The Guardian*, 9 June. Available at: https://www.theguardian.com/world/2017/jun/09/man-jailed-for-35-years-in-thailand-for-insulting-monarchy-on-facebook (Accessed 16 November 2019).

The International Telecommunication Union (2019). *2019 Global and Regional ICT Estimates*. Available at: https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx (Accessed 7 January 2020).

The Ministry of Culture and Information Policy of Ukraine (2020). *MKMS Zaproshue do Obgovorennya Proektu Zakonu Shodo Zabespechennya Natsionalnoi Infobezpeki ta Prava na Dostup do Dostovernoi Informatsii.* [*The MCIP invites to discuss the draft law on ensuring national information security and the right to access reliable information*].

The MCIP of Ukraine, 20 January. Available at: http://mkms.gov.ua/news/3343.html?fbclid=IwAR0W0gFSZVAE1KVwWdlBtWJk_dqAuuiKfgfY58wF9U1B6MDvll3m85lr0xo (Accessed 13 April 2020).

The Order of the State Committee of Informatization and Communication (2002). *Nakaz Derzhavnii Komitet Zvyazku ta Informatizatsii Ukraini N122*. Available at: https://zakon.rada.gov.ua/laws/show/z0559-02 (Accessed 16 April 2020).

The Organisation for Security and Co-operation in Europe (1999). Kazakhstan, Presidential Election, 10 January 1999: Final Report. *OSCE,* 5 February. Available at: https://www.osce.org/odihr/elections/kazakhstan/14771 (Accessed 26 October 2019).

The Organisation for Security and Co-operation in Europe (2020). Indefinite Rule by Decree in Hungary's COVID-19 Response a Serious Concern, Say OSCE PA Human Rights Leaders. *OSCE*, 1 April. Available at: https://www.osce.org/parliamentary-assembly/449473 (Accessed 30 June 2020).

The Program of 2020 Informational Kazakhstan (2013). *O Gosudarstvennoi Programme "Informatsionnyi Kazahstan – 2020"*. Available at: https://online.zakon.kz/Document/?doc_id=31324378 (Accessed 16 January 2019).

The Program of Digital Kazakhstan (2017). *Ob Utverzhdenii Gosudarstvennoi Programmy "Tsifrovoi Kazahstan".* Available at: https://online.zakon.kz/Document/?doc_id=37168057 (Accessed 16 January 2019).

The Strategy of Cybersecurity of Ukraine (2016). *Pro Strategiyu Kiberbezpeki Ukraini*. Available at: https://zakon5.rada.gov.ua/laws/show/96/2016 (Accessed 13 April 2020).

The Ukrainian Helsinki Human Rights Union (2018). Spilna Zayva Shodo Proektu Zakonu N6688. [Joint Statement with Regard to the Law N6688]. *UHHRU*, 5 July. Available at: https://helsinki.org.ua/appeals/spilna-zayava-schodo-proektu-zakonu-pro-vnesennya-zmin-do-deyakyh-zakonodavchyh-aktiv-ukrajiny-schodo-zabezpechennya-informatsijnoji-bezpeky-ukrajiny-6688-2/ (Accessed 13 April 2020).

The United Nations Human Rights Council (2017). Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression. *Human*

Rights Council, thirty-fifth session, 30 March 2017. Available at: https://www.undocs.org/A/HRC/35/22 (Accessed 10 November 2020).

The Washington Post (2018). Myanmar Is Now Erasing the Rohingya's Very Name. *The Washington Post*, 16 June. Available at: https://www.washingtonpost.com/opinions/myanmar-is-now-erasing-the-rohingyas-very-name/2018/06/16/e3f66986-6f40-11e8-bf86-a2351b5ece99_story.html (Accessed 20 February 2020).

The Wall Street Journal (2021). How Big Tech Got Even Bigger. *The Wall Street Journal*, 6 February. Available at: https://www.wsj.com/articles/how-big-tech-got-even-bigger-11612587632 (Accessed 4 July 2021).

Tikhiy, F. (2018). SBU Ishet Predatelei v Internet. Ukraintsam Dayut Sroki Za Posty v Sotssetyah. [SBU is Seeking Traitors on the Internet. Ukrainians Are Given Sentences for Posts on Social Media]. *Ukraina*, 15 October. Available at: https://ukraina.ru/exclusive/20181015/1021408582.html (Accessed 9 April 2020).

Today (2018). Rech Ne Idet o Kontrole – Abaev o Sisteme Monitoringa SMI za 1.7 Milliarda Tenge. [There is No Talk About Control – Abayev about the Media Monitoring System for 1.7 Bln Tenge]. *Today*, 12 January. Available at: http://today.kz/news/kazahstan/2018-01-12/757931-rech-ne-idet-o-kontrole-abaev-o-sisteme-monitoringa-smi-za-17-milliarda-tenge/ (Accessed 16 January 2019).

Toguzbayev, K. (2012). "Respubliku" Veleno Zakryt. Chto Dalshe?. [The "Republic" Is to Be Closed. What is Next?]. *Radio Azattyq*, 25 December. Available at: https://rus.azattyq.org/a/respublika-oppositional-press-trial-verdict/24808192.html (Accessed 25 April 2020).

Toguzbayev, K. (2013). Pravozashitnik Obvinyaetsya v Propagande Ateisma, Govorit Advokat. [A Human Rights Defender is Accused of Atheism Propaganda, a Lawyer Says]. *Radio Azattyq*, 21 March. Available at: https://rus.azattyq.org/a/arest-pravozashitnika-alexandra-harlamova/24935112.html (Accessed 26 April 2020).

Toler, A. (2014). Fake 'Ukrainian' News Websites Run by Russian 'Troll Army' Offshoots. *Global Voices*, 19 November. Available at: https://globalvoices.org/2014/11/19/fake-ukrainian-news-websites-run-by-russian-troll-army-offshoots/ (Accessed 15 April 2020).

Toler, A. (2015). Inside the Kremlin Troll Army Machine: Templates, Guidelines, and Paid Posts. *Global Voices*, 14 March. Available at: https://globalvoices.org/2015/03/14/russia-kremlin-troll-army-examples/ (Accessed 15 April 2020).

Trenin, D. (2014). *The Ukraine Crisis and the Resumption of Great-Power Rivalry*. Moscow: Carnegie Moscow Center.

Trotsenko, P. (2015). Blog v Zakone: Za Chto Popadayut Pod Arest Internet-Polzovateli v Kazahstane?. [Blog in Law: Why Are Internet Users Arrested in Kazakhstan?]. *Vlast*, 24 December. Available at: https://vlast.kz/obsshestvo/14943-internet.html (Accessed 26 April 2020).

Tsagarousianou, R., Tambini, D. and Bryan, C. (1998). *Cyberdemocracy: Technology, Cities and Civic Networks.* London: Routledge.

Tucker, J. A., Theocharis, Y., Roberts, M. E. and Barberá, P. (2017). From Liberation to Turmoil: Social Media and Democracy. *Journal of Democracy*, 28/4: 46-59.

Tufekci, Z. and Wilson, C. (2012). Social Media and the Decision to Participate in Political Protest: Observations from Tahrir Square. *Journal of Communication*, 62: 363-379.

Twitter Transparency (2020). *Kazakhstan*. Available at: https://transparency.twitter.com/en/reports/countries/kz.html (Accessed 5 October 2020).

Twitter Transparency (2020). *Ukraine*. Available at: https://transparency.twitter.com/en/reports/countries/ua.html (Accessed 5 October 2020).

Tworek, H. (2019). Information Warfare Is Here to Stay: States Have Always Fought for the Means of Communication. *Foreign Affairs*, 25 April. Available at: https://www.foreignaffairs.com/articles/germany/2019-04-25/information-warfare-here-stay (Accessed 24 May 2020).

Ukraine 112 (2017). Obyski v Redaktsii “Strana.ua”. [Raids in the Office of “Strana.ua”]. *Ukraine 112*, 23 June. Available at: https://112.ua/obshchestvo/obyski-v-redakcii-stranaua-guzhvu-dostavili-v-kievskiy-glavk-397379.html (Accessed 10 April 2020).

Ukrainskaya Pravda (2015). V Ministerstve Stetsya Otkazalis Obyasnit, Zachem Emu “Informatsionnye Voiska”. [The Ministry of Stets Refused to Explain Why He Needs “Information Troops”]. *Ukrainskaya Pravda*, 23 February. Available at: https://www.pravda.com.ua/rus/news/2015/02/23/7059512/ (Accessed 15 April 2020).

Valeriano, B. and Maness, R. C. (2015). *Cyber War Versus Cyber Realities: Cyber Conflict in the International System*. New York: Oxford University Press.

Vis, B. (2009). Governments and Unpopular Social Policy Reform: Biting The Bullet or Steering Clear?. *European Journal of Political Research*, 48: 31-57.

Veber, E. (2020). Zaderzhannyi Za Video s Kritikoi Nazarbaeva Karagandinets Arestovan na Dva Mesyatsa. [A Karaganda Citizen Detained for Video with the Criticism of Nazarbayev Was Arrested for Two Months]. *Radio Azattyq*, 20 April 2020. Available at: https://rus.azattyq.org/a/30565783.html Accessed 26 April 2020).

Vendil Pallin, C. (2017). Internet Control through Ownership: The Case of Russia. *Post-Soviet Affairs*, 33/1: 16-33.

Vesti (2017). “Maski-Shou” v Krupneishem Media-Holdinge Ukrainy. [“Mask-Show” in the Largest Media Holding of Ukraine]. *Vesti*, 14 July. Available at: https://vesti.ua/strana/247302-maski-shou-v-krupnejshem-media-kholdinhe-ukrainy (Accessed 10 April 2020).

VKontakte (2017). Poroshenko’s Official Profile. *Vk.com*. Available at: https://vk.com/poroshenko.petro (Accessed 7 April 2020).

Volkogonov, D. (1999). *The Rise and Fall of the Soviet Empire: Political Leaders from Lenin to Gorbachev*. London: HarperCollinsPublishers.

Volodzko, D. (2019). Is South Korea Sliding Toward Digital Dictatorship?. *Forbes*, 25 February 2019. Available at: https://www.forbes.com/sites/davidvolodzko/2019/02/25/is-south-korea-sliding-toward-digital-dictatorship/#57ab23dd648e (Accessed 08 October 2020).

Vorotilov, A. (2016). Velikii Kazahskii Firewall. [The Great Kazakh Firewall]. *Forbes Kazakhstan*, 53/1. Available at: https://forbes.kz/process/internet/velikiy_kazahskiy_firewall/ (Accessed 27 April 2020).

Walden, M. (2020). On World Press Freedom Day, Malaysia Investigates Journalist Over 'Provocation'. *ABC News*, 3 May. Available at: https://www.abc.net.au/news/2020-05-04/malaysia-investigates-journalist-world-press-freedom-day/12210552 (Accessed 1 July 2020).

Walker, S. and Rankin, J. (2020). Hungary Passes Law That Will Let Orbán Rule by Decree. *The Guardian*, 30 March. Available at: https://www.theguardian.com/world/2020/mar/30/hungary-jail-for-coronavirus-misinformation-viktor-orban (Accessed 30 June 2020).

Wagner, B. (2018). Understanding Internet Shutdowns: A Case Study from Pakistan. *International Journal of Communication*, 12: 3917-3938.

Watts, J. (2003). World's First Internet President Logs On. *The Guardian*, 24 February. Available at: https://www.theguardian.com/technology/2003/feb/24/newmedia.koreanews (Accessed 4 July 2020).

Webb, I. (2016). Social Media Sites Blocked in Kazakhstan on 25th Anniversary of Independence. *Global Voices*, 16 December. Available at: https://advox.globalvoices.org/2016/12/16/social-media-sites-blocked-in-kazakhstan-on-25th-anniversary-of-independence/ (Accessed 6 February 2017).

Webb, I. (2017). Ukraine Sanctions VKontakte, Other Russian Social Media Websites. *Global Voices,* 16 May. Available at: https://advox.globalvoices.org/2017/05/16/ukraine-sanctions-vkontakte-other-russian-social-media-websites/ (Accessed 7 April 2020).

Weidmann, N. B. and Rød E. G. (2019). *The Internet and Political Protest in Autocracies.* New York: Oxford University Press.

Weingast, B. R. (1998). Political Institutions: Rational Choice Perspectives. In: Goodin, R. E. and Klingemann, H-D. (ed), *A New Handbook of Political Science*. Oxford: Oxford University Press, 167-190.

Whalley, A. (2019). Protecting Chrome Users in Kazakhstan. *Google Security Blog*, 21 August. Available at: https://security.googleblog.com/2019/08/protecting-chrome-users-in-kazakhstan.html (Accessed 27 April 2020).

Wilson, A. (2015). *The Ukrainians: Unexpected Nation*. 4th ed. New Haven: Yale University Press.

World Bank (2018). *Worldwide Governance Indicators*. Worldbank.org. Available at: http://info.worldbank.org/governance/wgi/Home/Documents (Accessed 23 February 2019).

Wright, N. (2018). How Artificial Intelligence Will Reshape the Global Order: The Coming Competition between Digital Authoritarianism and Liberal Democracy. *Foreign Affairs*, 10 July. Available at: https://www.foreignaffairs.com/articles/world/2018-07-10/how-artificial-intelligence-will-reshape-global-order (Accessed 8 January 2020).

Wright, R. (2000). Gaining Freedom by Modem. *New York Times*, 28 January. Available at: https://www.nytimes.com/2000/01/28/opinion/gaining-freedom-by-modem.html (Accessed 7 January 2020).

Wriston, W. B. (1997). Bits, Bytes, and Diplomacy. *Foreign Affairs*, 76/5: 172-182.

Wu, W. and Weaver, D. (1996). On-Line Democracy or On-Line Demagoguery? Public Opinion “Polls” on the Internet. *Press/Politics*, 2/4: 71-86.

Yakubov, A. (2010). U Redaktsii “Respubliki” Est Tri Versii Prichin, Pochemu Blokiruyut Ee Saity. [The “Republic” Has Three Reasons Why its Sites Are Blocked]. *Radio Azattyq*, 30 April. Available at: https://rus.azattyq.org/a/respublika_newsspaper_website_closed/2028080.html (Accessed 25 April 2020).

Yastremskaya, T. (2017). V Ukraine Za Posty v Sotssetyah Vynesli 36 Prigovorov s 2014: Za Chto Mogut Osudit. [In Ukraine 36 Sentences Have Been Given for Posts on Social Media Since 2014: For What You Can Be Convicted]. *Ukrainskie Novosti*, 26 June. Available at: https://ukranews.com/news/504997-v-ukrayne-za-posty-v-socsetyakh-vynesly-36-prygovorov-s-2014-goda-za-chto-mogut-osudyt (Accessed 9 April 2020).

YouTube (n/d). *YouTube for Press.* Youtube.com. Available at: https://www.youtube.com/intl/en-GB/about/press/ (Accessed 15 September 2020).

Zakon (2009). Prezident Kazahstana Podpisal Zakon o Regulirovanii Interneta. [The President of Kazakhstan Signed a Law on Internet Regulation]. *Zakon*, 11 July. Available at: http://www.zakon.kz/143034-prezident-kazakhstana-podpisal-zakon-o.html (Accessed 6 February 2017).

Zakon (2017). Anonimnye Kommentarii na Saitah Zapretili v Kazahstane. [Anonymous Comments on Sites Are Banned in Kazakhstan]. *Zakon*, 28 December. Available at: https://www.zakon.kz/4896289-anonimnye-kommentarii-na-saytah.html (Accessed 22 December 2018).