ACCESS DENIED: CONTROL AND RESTRICTION STRATEGIES OF THE INTERNET IN HYBRID REGIMES

by
HATİCE BETÜL BAL

Submitted to the Graduate School of Social Sciences
in partial fulfilment of
the requirements for the degree of Master of Arts

Sabancı University
July 2023

ACCESS DENIED: CONTROL AND RESTRICTION STRATEGIES OF THE INTERNET IN HYBRID REGIMES

Approved by:

Assoc. Prof. Berk Esen .....
(Thesis Supervisor)

Asst. Prof. Mert Arslanalp .....

Asst. Prof. Oya Yeğen .....

Date of Approval: July 21, 2023

ABSTRACT

ACCESS DENIED: CONTROL AND RESTRICTION STRATEGIES OF THE INTERNET IN HYBRID REGIMES

HATICE BETÜL BAL

POLITICAL SCIENCE M.A. THESIS, JULY 2023

Thesis Supervisor: Assoc. Prof. Berk Esen

Keywords: hybrid regimes, digital authoritarianism, Internet, digital censorship, digital surveillance

This thesis aim to explain the control and restriction strategies used by authoritarian regimes, with a specific focus on hybrid regimes. The different techniques used by authoritarian regimes to cope with the Internet are analyzed into two groups; restrictive and proactive strategies. The repertoire of these two categories is explained with a case study of Turkey, and it is seen that regimes use both of these strategies when a due occasion occurs. In times of national crises, and critical political junctures like elections are the period where the restrictive strategies are used mostly, whereas the proactive strategies constitute the de facto stamce of the regime. Furthermore, the relationship between the elections and restrictive strategies is tested with both a cross country and a single country analysis. As a result, partial evidence is found supporting the main argument that regimes have a higher likelihood to use the restrictive strategies during pre-election period.

ÖZET

ERİŞİM ENGELİ: HİBRİT REJİMLERDE İNTERNET KULLANIMINA GETİRİLEN KONTROL VE KISITLAMA STRATEJİLERİ

HATİCE BETÜL BAL

SİYASET BİLİMİ YÜKSEK LİSANS TEZİ, TEMMUZ 2023

Tez Danışmanı: Doç. Dr. Berk Esen

Anahtar Kelimeler: hibrit rejimler, dijital otoriterleşme, Internet, dijital sansür, dijital gözetim

Bu tez, otoriter rejimler tarafından kullanılan kontrol ve kısıtlama stratejilerini, özellikle hibrit rejimlere odaklanarak, açıklamayı amaçlamaktadır. Tez boyunca otoriter rejimlerin internetle başa çıkmak için kullandıkları farklı teknikler iki grupta incelenmiştir; bu iki grup kısıtlayıcı ve proaktif stratejilerdir. Bu iki kategorinin içerdiği çeşitli teknikler, Türkiye örneği ile açıklanmıştır ve rejimlerin yeri geldiğinde her iki stratejiyi de kullandıkları görülmüştür. Ulusal kriz zamanları ve seçim gibi kritik siyasi dönemler, kısıtlayıcı stratejilerin en çok kullanıldığı dönem olurken, proaktif stratejiler ise rejimin fiili duruşunu oluşturmaktadır. Ayrıca, seçimler ve kısıtlayıcı stratejiler arasındaki ilişki hem ülkeler arası hem de tek ülke analizi ile test edilmiştir. Sonuç olarak, rejimlerin seçim öncesi dönemde kısıtlayıcı stratejileri kullanma olasılıklarının daha yüksek olduğu ana argümanını destekleyen kısmi kanıtlar bulunmuştur.

ACKNOWLEDGEMENTS

Firstly, I would like to express my gratitude to my thesis advisor, Assoc. Prof. Berk Esen, for his valuable advice, feedback, and support. Without his help, this work wouldn't have been possible. His guidance made this journey smoother and more insightful. His comments encouraged me in moments of stress to keep writing, improving, and completing my work.

I also want to thank Asst. Prof. Fatih Serkant Adıgüzel for his feedback. His insights on my thesis will not only benefit this project but also contribute to my academic journey and future work.

I want to acknowledge Asst. Prof. Mert Arslanalp for his role as a member of my Thesis Jury. His comments significantly enhanced my thesis and took it to a higher level.

A special thank you to Asst. Prof. Oya Yeğen for her help and comments.

I am grateful to my friends Merve, İrem, and Sena for their support. Throughout my master's studies, their companionship kept me motivated.

Lastly, I want to express my gratitude to my extended family for their continuous belief in me. I always feel their loving support, especially when I faced moments of doubt. A heartfelt thank you to my dear husband Mustafa for sharing my stress and easing my burdens. He supported me tirelessly. I am also deeply thankful to my mom, my sister, and brother for always being there for me. I must also mention my dad, whose guidance and work ethic have shaped me. I want to thank everyone else who I may not have mentioned here but who have always made me feel loved and supported.

To my mom
for being my best teacher
nothing would be possible without her love and dedication

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

1. INTRODUCTION

It was February the 6th 2023, when a devastating earthquake hit the eastern provinces of Turkey. That morning, everyone in the country tried to understand the scale of the damage and was shocked by its magnitude. Tens of thousands of buildings and major highways were destroyed or severely damaged, telecommunication lines were disrupted, thousands of people were trapped in the debris and many more died. Social media played a big role in search and rescue efforts after the earthquake because people communicated with each other via the Internet. The relatives of those under the debris used the Internet to get help, and there were times when even those under the wreckage used social media to reach the teams. Those who wanted to volunteer in the region organized through the Internet. People mobilized quickly to collect necessary supplies such as warm clothes, heaters, blankets, and hygiene products, thanks to social media. Two days after the earthquake destroyed the region, at the highest of all the efforts, Twitter has been restricted (NetBlocks 2023). The authorities declared that this was done to prevent the disinformation. Considering the scale of the crisis, it is surprising to see that the priority of the government is to prevent disinformation in the digital space. The restriction has been criticized harshly in social media by the ones who connected anyway through circumvention tools, and shortly after, Twitter access was restored.

This example illustrates how the Internet has changed society's communication styles massively. Thanks to the Internet, people can more easily organize, communicate with each other faster, and have a space to set their demands. The speed and accessibility of the Internet far surpass traditional communication systems. The connection between the people was greatly strengthened and became much more organic and unpredictable. Furthermore, in such times, people use the digital media to state their grievances and make demands. This is the reason why the Internet can be a source of fear for the ruling elite in terms of the durability of their regime. People have new avenues to discuss the problems they encounter in their lives and this can result in increasing anti-regime sentiment especially in authoritarian regimes. In the

given example, the same incident has happened. After the earthquake, people heavily criticized the government due to the policies allowing the construction of weak buildings. The responsibility of the regime in these destructions was seen as greater than the magnitude of the earthquake. The regime could not afford to allow the dissemination of increasing criticisms, therefore restricted the Internet, even though it serves the search and rescue efforts.

The revolutionary impact of the digital media on communication technologies brings out that fear, not only because it is a faster and easier way of communicating and getting news, but also because it provides a new platform for political debate and sharing concerns about the regime with other citizens. People do not use the Internet only as a source of communication and entertainment, but they use it as a news source and a place where they can make demands. Thus, the Internet can have the potential to be a more free alternative to traditional media, and this way can be a game changer, especially in regimes where traditional media sources are under the control of the government. The Internet can open the door to political liberalization in authoritarian countries.

This thesis focuses on the impact of the Internet, more specifically the liberalizing power of the Internet and the authoritarian response towards this new and revolutionary communication source. Starting with a discussion about whether the Internet has the power to democratize countries, this study focuses on the restriction and control patterns of non-democracies. The shift in the focus from democratization to restrictions is stemming from the journey of non-democracies concerning the Internet. Initially, the Internet attracted attention as having an effect to liberalize countries with authoritarian tendencies, and the example of Arab Spring supported this idea. However, as the years passed it was seen that authoritarian regimes have adapted their rule according to the digital age and learned new restriction and control strategies that will fit the nature of the Internet.

The main question of this thesis is what the different strategies of authoritarian regimes are to control and restrict the Internet. I gathered strategies of the authoritarian regimes employed to control the Internet into two main categories. Inspiring from the repression literature's categorization of different techniques to oppress society, I come up with two broad categories of digital repression strategies. These categories are restrictive strategies and proactive strategies. This categorization is an application of carrots versus sticks explanation. The different strategies employed by authoritarian regimes are discussed in the literature, the categorization I made in this thesis is collection of these strategies in a more comprehensive and organized way. Restrictive strategies include harsher measures to make the digital space free

from unwanted content via limitations such as censorship, Internet shutdowns, restrictions to access, and so on. In restrictive strategies, regime fights against the Internet. Restrictive strategies are the sticks in the given metaphor. The carrots are those strategies with a subtler operation mechanism which I called proactive strategies. The reason to name them as proactive is that, in these types of strategies, regime uses the means of the Internet to control the digital space. Regime uses various tools to control the digital discourse, to manipulate it and this way prevent the consequences caused by the digital activities harmful for its durability. One step further, through proactive strategies, the Internet even becomes an effective propaganda tool for the regime. Tools to make this transformation and control to happen, include troll armies, surveillance tools, and bot accounts. Restrictive and proactive strategies constitute the toolkit of the authoritarian regimes to control the digital space.

The main argument of this thesis is that regimes use a blend of these restrictive and proactive strategies to create their toolkit of digital repression. To understand the different weights of restrictive and proactive strategies in different regimes I focus on hybrid regimes. Hybrid regimes show the biggest variance and creativity when we compare them with democracies and closed autocracies. They do not have the capacity to impose broad restrictions openly as closed autocracies do therefore need proactive strategies in their toolkit. They also can not afford to give Internet a free space as democracies do therefore, they need restrictive strategies. This thesis focuses on the variance of digital repression n hybrid regimes and argues that as the regime gets more authoritarian, regime tendency to use restrictive strategies increase. I illustrate this argument with a detailed case study of Turkey.

Turkey is a country that is gong through democratic backsliding since 2007 onwards under the AKP government. 2007 general election is the beginning of the second term of AKP government, at the same time the centralization of power in the hands of incumbent started in this period with a set of underlying constitutional reforms. Since then, the regime maintains its rule with its electoral victories. As a competitive electoral regime, the Turkish government depends heavily on populism and media control. The population is relatively young and this makes the digital space a popular information and communication venue. High polarization within the population results in hot debates between the regime and opposition supporters, and social media serves as a platform for these debates. The regime is also aware of that, therefore, invests in Internet controls extensively. For these reasons, I made a detailed case study of Turkey, to examine the dynamics of the blend of restrictive and proactive strategies in hybrid regimes. Focusing on Turkey allow me to see how digital repression methods evolve through time, how a regime learns to cope with

the Internet and benefit from it, and how the level of authoritarianism effect the use of restrictive and proactive strategies.

Furthermore, this thesis argues that regimes have a higher tendency to use restrictive strategies during times of crises. Hence, I focus on the mechanisms behind the control and restriction strategies too and seeks to explain the factors that drive authoritarian regimes to pick restrictive or proactive strategies. After providing a discussion of possible reasons to choose either of the strategies, this thesis argues that elections are among the political junctures in which regimes have a higher likelihood to use restrictive strategies to control the Internet. Because election times are times of uncertainty for hybrid regimes, I assume that they tend to see the election times as a critical juncture point where they have a higher likelihood to resort to restrictive strategies. To test this argument, I make a cross-country, and a single-country analysis. In the cross-country analysis, I used most different systems design. The sample constitutes 32 hybrid regimes with varied populations, GDP per capita, and Internet penetration. I test the argument that hybrid regimes have a higher likelihood to use restrictive strategies to control the Internet during elections with a difference-in-differences model. As a result, I find partial evidence supporting the main argument. In the single-country analysis, I focus on Turkey 2023 elections to test the same argument as cross country analysis. Again I use the difference in differences model, but this time with a synthetic control unit, and the results support the main argument that the regime has a higher likelihood to use the restrictive strategies.

The analyses aim to contribute to the understudied parts of the literature. The literature focuses on the relationship between the Internet and the socio-political impacts of it in three main aspects. The first aspect is the impact of the Internet on social mobilization and democratization. The Arab Spring sparked hope about the democratization power of the Internet, however, the relationship between the Internet and democratization cannot be confirmed. The scholars agreed upon the impact of the Internet to facilitate social mobilization (Bailard 2012; Clarke and Kocak 2020; Ruijgrok 2021), however in terms of democracy, they concluded that whether this mobilization will turn into democratization does not depend solely to the Internet. The second aspect is related to the first one. The impact of the Internet on citizen attitudes is studied. The Internet does not only provide a new perspective on communication, but it shapes the citizens' attitudes and demands in favor of democracy and civil rights and against the institutions and wrongdoings of the regime (Nisbet et al. 2015; Ruijgrok 2021; Stoycheff and Nisbet 2014; You and Wang 2020). In the third aspect, the literature focuses on the response of authoritarian regimes to the Internet. The different strategies to cope with the

Internet are discussed (Deibert 2015; Gunitsky 2015; Rød and Weidmann 2015), and the effect of digital censorship is reviewed (Hassanpour 2014; Miller 2022; Pan and Siegel 2020; Roberts 2014). However, all of these studies are focusing the period after the controls and restrictions. The questions of how the regime chooses among the different strategies of restriction and control, or what are the factors that shape the regime's behavior in terms of Internet restrictions and controls are not answered in the literature. Hence, my main objective in the quantitative analyses is to contribute to this gap. In the following section I will talk about the methodology in detail before I move to the theoretical framework.

1.1 Methodology and Case Selection

In this thesis, mixed methods are used. There are two empirical chapters, one includes quantitative analyses of the relationship of restrictive strategies with elections, and the other includes a detailed case study that examines the use of restrictive and proactive strategies. In this section, I am going to explain the methodology of these chapters.

Mixed methods research facilitates quantitative and qualitative research methods together and aims to fill the weaknesses of one method with the strengths of the other. In this thesis, I have two hypotheses and I test them using different methodology. My strategy is to start from the general and move to the particular. Hence, the first analysis is a large N study with quantitative research design. Then, I focus on Turkish case by using both quantitative and qualitative methods. Mixed methods approach suits best for my two parted analyses.

I started with the quantitative analyses of the thesis. In these analyses, the main question is whether regimes increase to use of restrictive strategies during elections. The different strategies of authoritarian regimes are studied, and scholars mostly focus on the impacts of the different authoritarian control strategies. How the regime sentiment changes after a ban, how it is related to the social mobilization movements, and which strategies are used to repress the liberalizing power of the Internet are the questions that have been studied so far. However, the initial mechanism of the restrictive and proactive strategies is not studied enough. There are some ideas and clues about the factors which might drive the regimes to choose restrictive or proactive strategies but there is not much evidence showing the linkages. In the quantitative chapter, I aim to contribute to this gap in the literature. My main argument is that in pre-election times, as an important juncture for the regime, the

regime has a higher likelihood to employ restrictive strategies. I test this argument both with cross-country data with 32 hybrid regimes, including electoral autocracies and electoral democracies and in one specific case, Turkey.

There are several reasons to choose hybrid regimes for these analyses. Hybrid regimes are neither repressive at the scale of closed autocracies nor free at the scale of democracies. When we look in terms of control strategies of digital media, the constraints for its repressiveness bind them to employ harsh restrictions on the Internet. Also, the government that centralized power over the years does not want to hand on the incumbency, therefore they try to control the factors that might cause them to lose their legitimacy and popularity among people like the media. The elections, even though they lose the characteristics of being a free and fair election, are still important for hybrid regimes. Therefore, they do not want to lose legitimacy and popularity, as a result, the media was one of the institutions that is systematically restricted and manipulated in hybrid regimes. Robertson (2010, 170) highlights a similar point by saying that "hybrids are even more at risk from challenges in the streets because their regimes are both more open and have less repressive capacity than closed authoritarian regimes". For this reason, he argues that hybrid regimes have to put a lot of effort and creativity to fight with the uprisings. Digital repression is an important subcategory of these controls and restrictions. Therefore, to understand the variance in the mixture of restrictive and proactive strategies, this thesis focuses on hybrid regimes. Another reason why hybrid regimes give a better fit for this study than closed autocraciesis that in closed autocracies the elections either do not exist, or they are not competitive, in which only one party or one candidate participates and eventually receives 90 or more % of the votes. Therefore, hybrid regimes are the main focus group of this thesis.

In the first design of the quantitative chapter, I used a most different systems approach. I collected data from 32 different hybrid regimes. I picked those countries based on the data availability and the existence of elections between the 2020-2023 period. Since a difference in differences model is used to test the argument that the regime has a higher likelihood to use restrictive strategies during elections, there is a treatment group that constitutes the countries with elections, and there is a control group that constitutes the countries with no elections.

In the second analysis, I test the same argument based on a single case of Turkey. Turkey is a good example of hybrid regimes and their control and restriction strategies on the Internet for several reasons. Firstly, Turkey has been experiencing democratic backsliding since 2007. Diminishing media freedom is one of the effects of the authoritarianism that the country going through and the Internet restrictions and

controls are parts of this. Secondly, Turkey has a high ratio of young population, which makes the country's Internet use higher. Furthermore, the Turkish population is highly polarized and mobilized in terms of politics, especially during election times, hence digital platforms are highly used for political debates. The regime is aware of that too, paying special attention to the manipulation and restriction of digital platforms. Together with these, the very recent general elections held in May 2023 make Turkey a very suitable example for this analysis. A difference in differences model with a synthetic control unit is used to test the main argument. I created a synthetic Turkey based on the data come from 15 countries for the control group.

The qualitative analysis follows the quantitative analayses chapter. For the qualitative analysis, I make a detailed case study of Turkey to examine the categorization of restrictive and proactive controls. I want to focus on hybrid regimes for the analysis of restrictive and proactive strategies too because hybrid regimes are typically the ones that needed to employ restrictive and proactive strategies together, therefore, for the examination of restrictive and proactive controls, hybrid regimes are the best choice. I picked Turkey as a good example of competitive authoritarian rule. The said reasons in the quantitative analysis of Turkey are again influential for the case selection of the qualitative chapter. I review the evolution of Internet governance and the application of restrictive and proactive strategies in the Turkish case, as a part of the declining democracy through the years. This way, I aim to show a real-life example of the rich set of techniques used by hybrid regimes to tame and control the Internet and examine the special mixture of restrictive and proactive strategies of Turkish government.

In the following chapters, I will explain the theoretical framework, and the quantitative and qualitative analyses. Firstly, I will put forward theoretical framework with a literature review and categorization of restrictive and proactive strategies. Next, in Chapter 3, I will scruntinize the analyses of the relationship between the elections and restrictive strategies. In the fourth chapter, I wil discuss the detailed case study of the Turkish case of restrictive and proactive strategies. The fifth chapter will be the concluding chapter.

2. THEORETICAL FRAMEWORK

2.1 Existing Literature and Theoretical Framework of the Thesis

The Internet has become an essential part of our daily lives since around the 2000s. Today, it is the easiest and fastest way of reaching the most recent information and news. In this chapter, I am going to review and discuss the existing literature on the digital age in terms of its impacts on society, political mobilization, and authoritarian rule and I will connect this literature with competitive authoritarianism and repression. Afterward, I am going to introduce my conceptualization of Internet controls authoritarian regimes employ, and then discuss my main arguments once again.

The Internet created an online platform that binds way much bigger amounts of people across different geographies. The speed and the area that the information can reach is very groundbreaking, and it has a revolutionary power that comes from the interactive nature of digital platforms. Unlike traditional media, citizens now become part of the information-generating process via actively sharing, commenting, and even creating content. This way the Internet offers citizens a new virtual environment to communicate and discuss opinions. All of these contributions sparked hope about the potential of the Internet to liberalize societies as being an alternative way of communication, especially in regimes where traditional media is under total control of the regime. Scholars seek to answer whether the Internet could be the key to the path to liberation in autocracies. The early examples of Internet literature are named cyber-optimists by Gunitsky (2015). Following the examples about the effect of the Internet on democratization, cyber optimists argued that the Internet might have a liberalizing effect on authoritarian regimes. Because of its capacity to create a free ground in online platforms, it was expected to improve the communication between citizens and this way increase the discussion between them about political issues. Individuals can share their opinions and find the ones with

similar standpoints and build associations. This will help them to set agendas in line with their opinions and mobilize to demand, for instance, policy recommendations or even liberalization. This potential makes scholars research the relationship between democracy and the Internet. Digital media decreases the costs dramatically to spread information to big numbers of people and creates a new channel to raise awareness among society for a specific issue. This can make a big difference, especially for opposition groups living in authoritarian regimes where opposition is systematically excluded from the traditional media. As Ruijgrok (2017) shows in his article on the Internet's impact on citizens in authoritarian regimes, the Internet increases the anti-regime sentiment among citizens, and this way it contributes to the mobilization against the authoritarian regime.

Arab Spring is the most inspiring example of this literature. The first country where anti-regime protests begin is Tunisia, and the others like Egypt and Yemen followed the Tunisian example. Tunisian protests burst after the incident of Mohamed Bouazizi. Bouazizi was a street vendor in Tunisia, and he set himself on fire because of his frustration with the current economic and social hardships in Tunisia. His protest was shared by millions on social media platforms and became the starting point of country-wide demonstrations that lasted around one year and resulted in a change in the Tunisian government. The Tunisian protests set an example for the citizens living in different countries like Egypt and Yemen who have similar uneasiness with the current situation in their country. The effect of the Internet on mobilization exceeded domestic politics in the example of the Arab Spring. Stories spread via the Internet are dramatic and relatable among citizens, therefore it resulted in anti-regime sentiment and dissent in society. The contribution of the Internet in the example of Arab Spring is crucial because it shows how online dissent can turn into a public movement and eventually have some institutional returns. The Internet exemplifies the sorrows of fellow citizens more dramatically and more clearly compared to traditional media. People can see that there are lots of others who suffer from the same grievances, it is easier for them to come together, set an agenda, and protest. Even though it is hard to say that without the Internet no such protests would occur, the Internet definitely opened new ways of mobilization and strengthened the dynamism of the movement.

There are articles that show Arab Spring as evidence to show that Internet use increased the likelihood of anti-regime protests (Clarke and Kocak 2020; Ruijgrok 2017). There is more or less a consensus among them on the argument of the Internet increases protests (Bailard 2012; Clarke and Kocak 2020; Ruijgrok 2017).

Ruijgrok (2017) argues that despite the attempts of authoritarian regimes to control

and limit the Internet, it improved communication between citizens by decreasing the costs and risks for the opposition, changing the attitudes of the citizens against the government, and providing more complete and dramatic information. However, the benefits brought by the Internet help to build democracy could not be something that one can be sure of. The Internet facilitates means to mobilize among society, however, whether this mobilization achieves to establish democracy is a question mark.

Clarke and Kocak (2020), similarly inspired by the Arab Spring, seek to answer whether the use of Twitter and Facebook contributed to the Egyptian uprising. They concluded that social media plays the role of "first move" and help the masses to overcome the collective action problem. Despite the evidence supporting their argument, they added that this is a narrow account to claim big conclusions about the relationship between politics and the internet.

Bailard (2012) reaches the same conclusion as Clarke and Kocak (2020), by saying that the evidence showing the relationship between the Internet and protests is not falsifiable because of the lack of countercases. We could not know whether the protests that happened after the expansion of Internet use among societies would not erupt if there were no Internet, whether it is the Internet that makes them happen or not. However, Bailard (2012)'s findings too, like Ruijgrok (2017), and Clarke and Kocak (2020), show that the Internet definitely helps protests to spread across the masses by playing the role of "mirror holding" or "window opening". This means that the Internet shows people the sorrows of other members of the society in a clearer way and helps them to communicate and mobilize more easily.

The factors that constitute the democratizing potential of digital media can be summarized in three main points. First, the Internet creates a new venue for citizens to talk about their grievances and make demands. Unlike traditional media, digital media has the potential to open up space for citizens too, hence, it gives hope to be heard by a larger audience and get returns. Thanks to this contribution of the Internet, people not only share their grievances but also talk to others who have similar concerns. Hence, it acts like a virtual bridge that binds people together. Second, digital media decreases the costs for the opposition to come together and talk about an agenda. This factor's effect can be realized especially in an authoritarian context, where in traditional media, there is no room for opposition. Digital media is preferred as an alternative to traditional media which is heavily controlled by the regime. Lastly, the Internet provides access to a big source of information from around the world. It increases the awareness of people about democratic values, and institutions. This was because the demand for democracy is increasing in general.

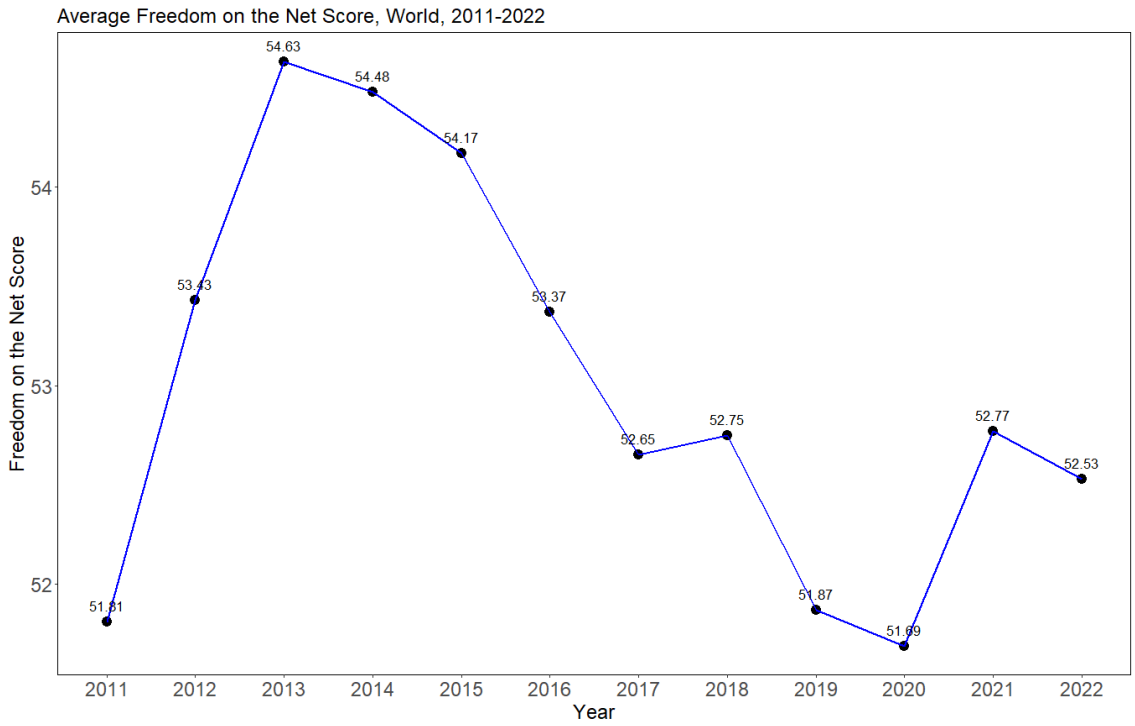
The combination of these three factors gives the Internet its democratizing power.

Nevertheless, this does not mean that the Internet bring liberalization on closed regimes because the liberalization depends as much on the regime's capacity to protect itself and to respond to the mobilizations, as it depends on the mobilization capacity of the society. The regime's part of the story might even have more impact than the mobilization capacity of the society because as Boas argues "Ultimately, the Internet is a tool, a medium of communication much like any other. It has no inherent political logic. As a tool, its political impacts will depend largely on who controls the medium and in what manner they seek to use it" (2004, 443). Similarly, Groshek (2009), argues that the Internet's impact on democratization depends on the existing level of democracy in the country, at least as much as it depends on the Internet penetration. Likewise, Nisbet, Stoycheff, and Pearce (2012) suggest that in order to understand the relationship between democracy and the Internet, the linkage between the Information and Communication Technologies (ICTs) and the level of democratic governance should be taken into serious account. This concludes the discussion about the relationship between the Internet and democratization, showing that it is not a direct relationship. It heavily depends on the regime's counter-movements and their success level. However, it is undeniable that the Internet contributes to social mobilization around a political agenda by enhancing citizens' communication tools.

One thing that is missing in the cyberoptimist literature is that they are not accounting the other factors that influence the democratization movement. For instance, the regime's institutional structure, its relations with the other power groups, i.e. economic and political elites, the popularity of the regime, the clientelist relationships with citizens, the capacity to control and manipulate the Internet, and so on. Also, authoritarian regimes do not stay the same through the years. The new tools to surveil the Internet, limit the information flow, and manipulate the narrative are employed by authoritarian regimes to regulate the untamed power of the Internet and harness it for their own durability. Another point that the literature does not capture is that the examples showing the positive contribution of the Internet on social movements do not have any counter-examples, therefore they are not falsifiable. In other words, even though the effect of the Internet is significant in these examples to facilitate the mobilization, we cannot know whether the cases would not erupt without the Internet, because there is not a case that we can compare to. Digital media could not be the factor that solely brings society to mobilize. Maybe, those cases would happen anyways regardless of the existence of an efficient communication tool.

Limitations towards Internet use become almost a general trend regardless of the regime type. In Figure 2.1, we can see the negative trend in the average Freedom on the Net Score's of the world. It is not a big change but still, it shows that Internet freedoms decreases through the years globally. According to the 2022 Freedom on the Net report, a big number of national governments take censorship measures and try to build walls around their national cyberspace, besides the limitations causing the declining Internet freedoms (FreedomHouse 2022).

Figure 2.1 Average freedom on the net score between 2011-2022, world



Source: Freeodom House (2023) - The average Freedom on the Net Score of the countries for each year were taken by the author

In closed autocracies like Iran, Syria, China, or Egypt, the Internet is highly controlled, and the government does not hesitate to use a wide range of censorships. Those regimes can enforce power and restrictions over society, and similarly, they can use harsh digital restrictions without worrying about the possible backlash. In democracies, however, we see a free flow of information. The limitations are within the boundaries of individual rights. The government's reach to individual information about Internet activity is restricted by laws and regulations, unlike closed autocracies where the government trespasses on the private information of digital activity. In closed autocracies and in regimes with authoritarian tendencies, the regime's interference with the Internet is protected by the rules and the laws. Hence, digital governance reflects the regime's respect for individual rights and freedoms in

general, which differ according to the regime's attitudes.

You and Wang (2020) give a regime-based account of the Internet's effect on the citizens' attitudes towards the regime and democracy. According to them, the effect of the Internet on citizen attitudes and preferences is not different from democracies and autocracies. Citizens become more knowledgeable about democratic values, and this creates an incentive to demand more democracy. Other than the democratic values, You and Wang (2020) claim that the Internet creates a sense of distrust towards the institutions. The difference between democracies and autocracies comes at this point in their way to answer the newly emerging demands. Democracies are more easily adapted to the Internet because they have mechanisms to refer to the demands of civil society. In regimes with authoritarian tendencies on the other hand, the Internet's impact on the citizen demands towards democracy and the distrust towards the existing institutions have a potential to pose a threat to the regime. Being a new communication tool between citizens might have the potential to increase dissent against the regime in authoritarian regimes because the Internet becomes an alternative to highly controlled traditional media outlets and this way open the channels between citizens.

Other than the effect of the Internet on democratization and governance, there is another group of studies that focuses on the impact of digital media on citizen attitudes. These studies focus on the effect of the Internet on citizens' perception of democracy and the performance of their government. Stoycheff and Nisbet (2014) argue that Internet use shapes people's perception of democracy. Thanks to the Internet, they become more aware of the qualities of democracy, and they demand the expansion of democracy in their country. Nisbet et al. (2012) study the relationship between the demand for democracy and Internet use, and they claim that individual Internet use has contributed to the increase in the demand for democratization, however, the country-level Internet penetration has not a significant impact on the demand for democracy. Ruijgrok (2021) focuses on anti-regime sentiment among people rather than the demand for democracy and expectations about the democratic government. He claims that Internet use in authoritarian regimes creates anti-regime sentiment. Similar to what Ruijgrok (2021) argues, as I mentioned previously, You and Wang (2020) find out that due to lower levels of representation of the public demands, the distrust of political institutions is directly associated with the authoritarian regime, and it ends up with a growing demand for regime opening among citizens. Hence, the impact of the Internet on the demand for democracy and more democratic institutions among citizens is a common contribution of the Internet across different regimes, however, the outcome is again dependent on the regime's decisions and durability.

The arguments about the demand for democracy and the anti-regime sentiments in authoritarian regimes are more interesting because arguing that in democracies Internet use increases the demand for democracy in society is like a tautology. Those who focus on authoritarian regimes should focus more on how anti-regime sentiment spread among the society. They should scrutinize the mechanism more deeply because it is very interesting to detect the increasing levels of anti-regime sentiment in a restricted cyber-space as Ruijgrok (2021) argue.

The effect of the Internet on the citizen attitudes towards the regime and democracy is in favor of democratization, the Internet definitely creates more demand for democracy and make citizens more cautious about the regime. These make Internet governance even more complicated for authoritarian regimes because direct attempts to restrict it have the potential to hurt their durability even deeper. Therefore, the strategies of authoritarian regimes attract scholarly attention too. Tang and Huhe (2014) give a detailed account of China's strategy to control the Internet. A set of repressive and more sophisticated strategies is used in China to control the Internet, according to them. They conclude that "the study of the Internet effect should aim to uncover the more specific mechanisms under authoritarian rule, instead of just focusing on political uprisings at the down of regime demise" (Tang and Huhe 2014, 572). According to them, what needs more attention is the authoritarian strategies to keep the Internet under control rather than seeking the role of the Internet in the cases that have been already coming to an end.

There are indeed such studies. The studies which focus on the different Internet control strategies mainly develop their arguments based on the assumption of the "authoritarian regime is in learning". That is to say, as years pass, the authoritarian regime has learned new ways of controlling digital space, and more interestingly, has become conscious of the potential of the Internet, and tries to benefit from it. Rød and Weidmann's argument gives a good account of this assumption; "Autocrats are likely aware of the tremendous potential this technology has for creating and maintaining a highly controlled sphere of public opinion" (Rød and Weidmann 2015, 341).

Rød and Weidmann (2015) argue that authoritarian regimes aim to control the Internet through different strategies. They do not want to allow it to turn into a threat to their power, therefore using the "repression technology" strategy, they censor the regime-critical content. However, they are aware of the potential too, therefore, they want to benefit from it by using the "liberation technology" to spread messages in favor of the regime. Rød and Weidmann (2015) also point out that the Internet becomes more and more fractionalized, in other words, "balkanized" because of the

controlling and monitoring attempts of authoritarian regimes; "Internet services are often provided by government agencies gives the regime even better information" (Rød and Weidmann 2015, 341). The authoritarian regime encourages the local Internet Service Provider (ISP) companies, and this way maintains its control of the Internet flow. They also force big, multinational social media companies to have local domains to store the information of their users locally. This enables the regime to have access to individual records whenever it deems necessary.

Similar to Rød and Weidmann (2015) account on the repressive and liberational technologies, Gunitsky (2015) also divides the authoritarian strategies into two; negative control strategies which include censorship and direct limitation on the one hand and positive proactive cooptation strategies on the other, which have a more subtle and cleverer way to keep the Internet under the limits of authoritarian rule while benefitting it in favor of the regime. Like the "balkanization" of Rød and Weidmann (2015), Gunitsky argues that "because of the increased territorialization of the Internet, and the diffusion of autocratic best practices, the web is increasingly becoming less of a public common good and more of a reflection of national borders" (Gunitsky 2015, 50). Boas (2004) also discusses two strategies of authoritarian regimes; the discussion is based on the questioning of the best option; to limit the expansion of the Internet or let it expand but control it by institutional and technological means. He concludes the discussion by pointing out that it is best to employ "multiple, overlapping layers of Internet control that have been effective at limiting the access of the majority of users" (Boas 2004, 442).

Deibert (2015) analyzes the different strategies too and divides them into three categories. He argues that authoritarian regimes are evolving to more sophisticated measures and explains the differences between the levels of sophistication between "first generation controls", "second generation controls" and "third generation controls". In the first generation, we see only repressive measures like censorship, filtering, and blocking certain websites (Deibert 2015, 65). In the second generation, we see more institutional measures like laws and regulations controlling cyberspace (Deibert 2015, 66). In the third generation, we see much more sophisticated measures necessitating technological infrastructures like surveillance, targeted cyberespionage, and cyber armies (Deibert 2015, 69).

Some studies show that the practices of authoritarian regimes to restrict the Internet can backfire and create even more dissent against the regime. Roberts (2014) focuses on the censorship practices in China and shows that the censored topic attracts more attention among users. Pan and Siegel (2020) look at the Saudi Arabian case and conclude that even though the repression of the online activities of opposition lead-

ers can create short-term returns to the regimes in the long run, it increases online dissent. Similarly, Hassanpour (2014) with his work about the Egyptian uprising in 2011, claims that the Internet shutdown resulted in street protests. Miller (2022) explains this backlash with reactance theory. According to reactance theory, temporary bans and shutdowns result in a higher level of negative conception towards the regime. In regions where Internet freedom and access to social media platforms are relatively open like it is in hybrid regimes, citizens actively resist and strive to regain their freedom when they face temporary bans. Thanks to the circumvention tools like VPN and DNS, social media and Internet use bans cannot fully prevent access to restricted content. There are still active users on the banned platforms who continue to post criticisms of the restrictions. This results in increasing anger towards the government and the regime.

Existing literature answers the questions concerning the relationship between democracy and the Internet, the relationship between the citizen attitudes about freedoms and democratization and the Internet, and the different strategies to control and restrict the Internet, however, it does not capture the decision-making mechanism of the regimes on Internet controls. How to govern such a new, groundbreaking, and potentially dangerous-for-some communication tool, how regime decide which strategies to employ, these questions are still waiting to be answered. In this thesis, the main objective is to contribute to this gap in the literature by focusing on Internet control and restriction strategies in non-democracies and trying to open the door to research the regime's decision-making mechanisms to choose between different strategies.

The literature about the Internet lacks a critical analysis based on different regimes. It mainly revolves around authoritarian regimes. The impact of the Internet on citizens' demand for democracy and the anti-regime sentiment is analyzed starting, on the basis of the democratizing power of the Internet over authoritarian regimes. The studies that focus on the regime's response to the Internet again put authoritarian regimes at the center. However, authoritarian regimes are considered as one homogenous entity. The variation between the different levels of authoritarian regimes is not differentiated in the literature. The strategies authoritarian regimes employ are examined, however, the analysis of authoritarian Internet controls remained limited to their effectiveness and impact on society. The variation between the authoritarian regimes and a detailed examination of their toolkit is understudied. The question of whether there is a variation between different types of authoritarian regimes is not studied enough. That is an interesting question to understand the relationship between the level of authoritarianism and the choice of digital control strategy of the regime. The most interesting story and the biggest variation exist in hybrid

regimes. They do not consolidate authoritarian rule as it is in closed autocracies, and they do not respect and protect democratic values and individual rights as it is in democracies. For this reason, they neither have the chance to deploy full-fledged Internet shutdowns and controls nor can afford to allow the free flow of the Internet completely. They are like in-between cases. that need more creativity in their set of repression (Robertson 2010). Digital control is a subcategory of overall repression practices of a regime and a reflection of it, hence their control strategies to control and restrict the Internet should be equally diverse, clever, and creative. Therefore, a set of different strategies to control the Internet and also benefit from it can best be observed in hybrid regimes. The censorship practices have a dark side as can trigger online dissent against the regime, and for hybrid regimes, a public movement can be more devastating compared to closed autocracies. Most hybrid regimes depend on popular support, therefore, censorship activities can hurt their legitimacy in the eyes of the supporting group. Furthermore, the Internet can be a good source of information about the public preferences of citizens, like the election results showing the opposition groups and the regime-supportive groups. In that sense, it can be very useful for the hybrid regime.

Hybrid regimes are like a new form of authoritarianism, 21st-century authoritarianism. They have some components to mimic democracies like holding regular elections, not using violent repression, appealing to public consent, implementing a market economy, and so on. Nevertheless, they do not have fully established democratic institutions that ensure the check and balances and prevent centralization of power, and not have a commitment to individual rights and liberties. They mostly emerged from collapsing autocracies after the cold war, when Western democracy became the international norm for governance and the pressure to establish democratic systems is very high (Levitsky and Way 2002). For this reason, they were named and treated as the transitioning cases from authoritarianism to democracy. However, passing years have shown that they are not transitioning (Merkel 2004), they have found a "middle ground between full-fledged democracy and outright dictatorship" (Carothers 2002, 18), that helps them to endure their regime. Different concepts were used to define these in between cases such as delegative democracy (O'Donell 1994), diminishing subtypes (Collier and Levitsky 1997; Merkel 2004), electoral autocracy (Diamond 2002), and competetive authoritarianism (Levitsky and Way 2002). The conceptualization of Levitsky and Way (2002), competitive authoritarianism, is the one that I mostly use in this thesis to refer to hybrid regimes.

Competitive authoritarian regimes have both democratic and autocratic elements, and they are neither democratic nor autocracy. Levitsky and Way (2002) explain characteristics of competitive authoritarian regimes as regimes that have certain

democratic institutions like elections, but, do not have checks and balances mechanisms. This way competitive authoritarian regimes play from the higher ground compared to opposition parties and change the rules of the game in their favor. This eclectic structure gives them durability in an electoral system and public support, however, at the same time, puts competitive authoritarian regimes at risk. This is because, the opposition still has some chance to win in the elections, even though it has not the equal opportunity with the incumbent. Schedler (2015) also points out the risk that hybrid regimes have to face, especially during elections by the "twin problem of uncertainty". Hybrid regimes are uncertain about their regime's 'security', and the electoral support of the opposition, as Schedler (2015) names it: 'opacity'. Together with elections, Levitsky and Way (2002) identify three contested areas in which the opposition may have a chance to win against incumbents in competitive authoritarian regimes. These are elective, legislative, judicial arenas, and the media. In these areas, competitive authoritarian regimes, unlike authoritarian regimes, do not completely prevent the opposition from being part of them because of the costs of mass protests and uprisings. However, these arenas are dominated by the incumbent, and the opposition has disadvantageous terms, this way prevented them from gaining control over any of these arenas. This way of securing the power through clandestine manipulation is a common trait of competitive authoritarianism and this is exactly what we see in digital media controls of competitive authoritarian regimes. Because these regimes cannot afford to give the expression of authoritarian repression due to their dependency on public support, they need to solve this problem with milder but complicated tools by controling the media, and digital media is not any different. The rich set of different strategies to control and restrict the Internet is mostly needed by hybrid regimes.

Competitive authoritarian regimes have a fragile mixed structure of democratic and autocratic origins, yet they establish quite durable regimes around the world. According to Gerschewski (2013), three important mechanisms make autocracies durable, and these hold for competitive authoritarian regimes too. These are legitimation, repression, and cooptation. Authoritarian regimes cannot survive if one of them is missing. Every authoritarian regime has a different mixture of these three factors depending on their power in terms of the cost of repression and toleration. In competitive authoritarian regimes, legitimation is even more influential because the channels to popular consent are not closed yet, therefore they are more bound to legitimation and this affects their balance of repression and cooptation. The digital space is a new place that authoritarian regime needs to control and establish its power, the rule of the digital space is very similar to traditional ways of repression. Digital media comes as a challenge for authoritarian regimes than

it is for democracies, just like public protest movements are more dangerous for authoritarian regimes than it is for democracies because of closed political opportunity structures (Earl 2011). Davenport (2007) and Earl (2011) conceptualize the repression practices of authoritarian regimes, and they differentiate between coercive responses such as harassment, bans, arrests, torture, and mass killings between different, softer techniques such as propaganda, persuasion, and material benefits. The digital repression strategies reflect the general repression patterns of authoritarian regimes. Especially for today's authoritarian regimes we see this wide range of different repression and cooptation strategies. As Earl (2022) argue too, digital repression is not totally different than typologies of general repression.

Repression and cooptation go hand in hand in competitive authoritarianism, however, the current strategy of autocracies is to implement cooptation more than repression. According to Guriev and Treisman (2019) the differentiating characteristics of today's authoritarian regimes from the former forms of authoritarianism is their retreat from harsh violent repression and leaning towards control through information manipulation under the façade of democracy. They argue that authoritarian regimes changed through time and their rule does not depend heavily on violent repression anymore, rather it depends on information manipulation and popularity. Levitsky and Way (2020) argue similarly. They questioned how countries with established democratic institutions and democratic cultures like Hungary, Venezuela, Turkey, and the Philippines have gone through authoritarianism. They conclude that these cases turn into more authoritarian regimes by skillful populists who gained public support and a legislative majority enough to make constitutional changes that circumvent checks and balances, together with individualistic repression and limitations on opposition via censorship. Popularity, rhetoric, manipulation, and targeted censorship are the new and effective tools of authoritarians. Controls and manipulations of digital space are the subcategories and effective tools for these practices of authoritarianism. Therefore, it is not surprising to see that the strategies of authoritarian regimes to control and restrict the Internet developed along these lines.

The change in authoritarian practices can be influenced by various reasons. Increasing identity politics around the world, international pressure for democratic values, and increasing importance and reporting of human rights, can be counted among these reasons. The role of the Internet is very influential too. Digitalization of almost all aspects of life changed the terms of communication and media. Hence, the changes and developments of authoritarian regimes can even be considered as actions to adapt to the digital age. Digital authoritarianism might be a good term to refer to the authoritarian regimes of today. Schlumberger et al. (2023) examine

authoritarian regimes of the digital age and say that the digitalization of dictatorship is an issue that should be studied and conceptualized more. They identify three main practices of digitalized authoritarian regimes in order to maintain themselves. Firstly, authoritarian regimes seek to gather information about potential threats, so they want to know about citizen preferences. Second, they seek to influence the behavior of their citizens via digital repression. Digital repression includes harsh responses from the regimes in the form of censorship, ban, and arrests. Third, regimes want to influence the belief of their citizens through digital cooptation such as manipulation. They emphasize these three strategies as the means of a digital authoritarian regime's maintenance. Boo and Slater (2021) and Tufekci (2014) discuss the liberalizing power of the Internet. These two studies' common conclusion is that the Internet has come with benefits for both citizens and the regime, however, the regime's hand strengthens more than the citizens'. Tufekci (2014) named new means of digital authoritarianism under six categories and name these as computational politics. Big data, various surveillance tools, and the use of behavioral science enable governments to make algorithmic governance. This could be the future of digital authoritarianism.

One of the main contributions of this thesis is to collect all of the strategies discussed in the literature, which are employed by authoritarian regimes to control the digital space. Most studies divide authoritarian control strategies into two, one category that has censorship at the center and the other category that has manipulations at the center. The modalities of authoritarian repression emerges in the control and restriction strategies of digital space too. However, the categorization of Internet controls is scattered and not clear. In this thesis, I summarize all of the techniques employed by authoritarian regimes to control and restrict the Internet into two main categories, namely restrictive and proactive strategies. This categorization sets off the roadmap of this thesis to understand the authoritarian regime's attitude towards the Internet.

As one of the main contributions of this thesis, I argue that the controls and restrictions of the Internet can be studied under two subcategories. The first set of strategies includes harsher strategies like censorship. They are directed toward the elimination of unwanted content immediately. Therefore, it would be suitable for this category to be named as restrictive strategies. The unwanted content is deemed as so by the regime. It can be criticism of the regime or arguments about the corruption or unlawful conduct of high-ranking politicians. The aim of the restrictive strategies is to prevent the flow of unwanted content in digital space and this way protect the regime from any subsequent threats. Restrictive strategies can be classified as a) broadband internet shutdowns and slowdowns, b) bans on specific domain

names, c) bans on specific content, and c) punishments based on anti-regime content sharing. These four categories are all complementary to each other and intertwined, the regime uses these techniques based on the tradeoff between the reaction of the society and the level of threat. These measures are simpler and do not necessitate sophisticated surveillance tools. The direct nature of restrictive strategies makes them handier in critical times for the regime. Therefore, regimes use restrictive strategies as an emergency valve, they have a higher likelihood of resorting to restrictive strategies in times when the stakes are high and taking risks is dangerous for the durability of the regime, like elections.

The proactive cooperational strategies require more sophisticated tools, even special institutions, and platforms to create controlled cyberspace. Proactive control strategies can be classified as a) a set of control, cooptation, and manipulation via the spread of messages favoring the regime, b) surveillance of the content containing regime criticism to reveal the sources of anti-regime sentiment, and c) fractionalization of the cyber-space to create a nationalized digital media away from the interventions of foreign trends. These strategies aim to cleverly mold the Internet in favor of the regime and turn it into a surveillance and propaganda tool. Proactive control strategies, different from restrictive strategies, do not aim to limit the Internet flow, instead, it is a way of actively involving the regime in the Internet to make its own propaganda, to fight back the criticisms through disinformation and naming-shaming. Gunitsky (2015) compares the Internet with the elections held in hybrid regimes and argues that the Internet activities of the citizens provide information to the regime about their preferences and stance against the regime like the election results give the map of opposition and regime voters to the regime. Thus, the detection of the sources of criticism is another goal of the regime to benefit from the Internet. It would not be wrong to say that proactive control strategies are a result of authoritarian regimes learning to benefit from the Internet. The regime first establishes an institutional base for Internet controls, then influence the digital discourse through various activities like disinformation, lynching, demonization of the opposition, and hacking. Furthermore, the regime uses the Internet as a source of information by surveilling the online activity of the users to pinpoint the oppositional trends in society and punish the ones with anti-regime opinions. These activities are done by intermediaries, both funded and voluntary, and this helps the regime to benefit from the Internet without getting attention on itself.

The most important difference of proactive strategies compared to restrictive ones is that the former is much more subtle. The proactive strategies mold the Internet to the regime's advantage. The Internet is drifted apart from being an arena of free speech and information flow and become a space with limits that are set by the

regime. The regime finds a way to reflect the strategies to control the traditional media in digital media too, and this way dominate the digital discourse by giving the patterns of acceptable, nationalistic, and patriotic citizen, and the opposite of it, which is nearly associated with being a traitor to the nation and terrorism. Thus, the proactive control strategies use the populist discourse and mobilize the regime supporters with this narrative. This eventually ends up with deepening online polarization and hate speeches.

The regimes which mainly adopt the first set of strategies, the restrictive ones, aim to limit the internet, and this way they keep it under control. However, the regimes which adopt the second, the proactive ones, with more sophisticated tools, do not intend to keep the Internet limited. On the contrary, to use the proactive strategies, the regime would want to expand the Internet. Nevertheless, the Internet expanded in such an environment would be highly controlled and in some cases government-provided. This is because the Internet has the potential to be a source of information about individuals in terms of their political tendencies and attitudes towards the regime, much more fine-grained information compared to traditional sources. Hence, the use of the Internet could benefit the authoritarian regime to consolidate its power even more with proactive strategies. Furthermore, restrictive strategies have a higher likelihood to trigger anti-regime dissent in society due to their direct and harsh nature, while proactive strategies offer a more subtle way to keep the Internet under control. The assumption about the restrictive strategies being a rather first-generation strategy is partially true, but the regime does not abstain from using restrictive measures as the new generation strategies emerge. The restrictive strategies always will be the "stick" of the regime, the final solution. The regime tries to expand the space for itself to use censorship more freely by preparing a suitable ground for censorship practices via the institutions, laws, and regulations, as well as the legitimization discourse for all of these; in order to implement censorship on necessary domains, accounts, and content in necessary times. Hence, the main question that should be answered is what drives the regime to choose between these strategies. The literature does not answer this question. The mechanism behind the authoritarian control strategies needs more attention. Several reasons could be counted as effective in the regime's decision to choose among strategies.

One factor could be budget constraints. The proactive strategies necessitate more sophisticated tools, institutions, and also people to employ in these institutions. China, as it is almost the inventor of proactive strategies, is the country that employs proactive strategies most widely and effectively. There is an Internet Propaganda Office in Zhanggong dedicated to creating 50c party posts to make government propaganda and eliminate the anti-regime posts in cyberspace, according to King,

Pan, and Roberts (2017). They say that "we estimate and reveal the size of what turns out to be a massive government operation that writes approximately 448 million 50c posts a year", which necessitates the employment of a huge number of people (King, Pan, and Roberts 2017, 485). A country with limited resources cannot afford to build such an infrastructure, therefore one of the reasons behind the decision to use this strategy would be related to economic strength.

Another reason could be related to the tactical preference of the regime. For instance, Gohdes (2020) argues that government limits the Internet where the social cleavages and political opposition groups are known and allows the free flow of the Internet in regions where it wants to gather information. He looked at the variation within the country and finds out that the regime wants the Internet use to expand on the territories where the regime cannot be sure about the social cleavages. Hence, not using restrictive measures for a while might be because of the regime's surveillance and information-gathering purposes.

Another one could be related to the capacity of the regime. Since the Internet provides an interactive platform with users' ability to make immediate reactions to posts, using proactive strategies such as manipulation of the narrative through propaganda and dissemination of wrong information is a risky business. Gunitsky argues that in order for the cooptation strategies to be successful, the regime has to have "clientelist networks or social groups whose members are willing to support the regime" (Gunitsky 2015, 49).

The structural limitations are another factor that binds the restrictive strategy use. If the regime does not have the power to confront the reactions after censorship or ban, it is better not to use restrictive strategies as the first solution. This might be the case when the regime gets more authoritarian, it became more reckless to use restrictive strategies instead of proactive strategies. Therefore, the regime's capacity, its penetration into the society, and the strength of its hand in terms of repression-consolidation power in terms of civil society and economic, political, and military elites are important determinants too to decide on the Internet control strategy.

In this thesis, I argue that the most important factor determining the strategy a regime chooses is the times of national crises and political junctures. In other words, I argue that, in times of crisis, all the other factors would lose their importance, and the regime resort to restrictive strategies. Portraying the proactive strategies as the everyday strategy of the regime and the restrictive strategies as the emergency policy of the regime would not be wrong. This is because of the fact that restrictive strategies give more immediate returns by limiting access to harmful content whereas proactive strategies necessitate a project-based penetration and manipulation of the

digital space. Therefore, the points of critical political junctures and national crises are the times when regimes are most probably use restrictive measures (Freedom-House 2022; Freyburg and Garbe 2018; Miller 2022). National crisis times can be stemming from a natural disaster, a military dispute, or a big accident that leads to hundreds of deaths. Among the political junctures, we can count the elections and coups. In both times of crises, and during political junctures regimes feel themselves at the highest vulnerability. These times are very suitable for the opposition to unite and criticize the government too. Therefore, the critical points are also the times when the regime is most likely to restrict the Internet, using censorship and bans.

In this thesis, I specifically focus on elections as one of the most important political junctures. In terms of the effects of the Internet control strategies of the regime, elections are the most frequent one among all others such as coups or wars, therefore we can say that it has the biggest impact. The relationship between the elections and restrictive strategies is discussed in the literature too. Crete-Nishihata, Deibert, and Senft (2013, 4) argue that elections are among the periods when the information is disrupted through subtle, and temporary Internet slowdowns. Gohdes (2015, 353) gives a supporting example to that argument by pointing out the Internet throttling done by the Iranian government in the immediate aftermath of the 2009 elections. Similarly, Maréchal (2017, 31) argues that Internet shutdowns whether it is in the form of total cut out of access or based on specific domains, are mostly imposed around sensitive events like elections and protests. The reason behind the regime's increasing tendency to use restrictive strategies is explained by Roberts as well, she says that "Facing elections or political opponents, governments purport to represent their constituents and rely on public opinion for the maintenance of their own power, and therefore have strong incentives to manipulate the spread of information" (Roberts 2018, 40), and besides the manipulation they need to prevent the unwanted content that has a potential to harm their legitimacy and popularity, via censorship. Again, Gohdes (Gohdes 2020, 4) emphasizes the regime's attempt to prevent the content including regime criticism, with the examples of limitation on Internet access during the 2009 elections in Iran, and social media blocks during mass protests in Turkey and China. Miller agrees with these arguments too by arguing that regimes try to manipulate the information and to repress the opposition "especially during critical political junctures such as elections, imposing temporary bans on social media platforms is one-way regimes attempt this manipulation in the digital era" (Miller 2022, 805). He analyzes the circumvention activity and anti-regime sentiment after the temporary Twitter ban imposed right before the 2014 general elections in Turkey.

The impact of elections on the use of restrictive strategies is examined in hy-

brid regimes in this thesis because these arguments are especially valid for hybrid regimes. Hybrid regimes have two distinctive characteristics which separate them from democracies and closed autocracies. Their dependence on popular support differentiates them from closed autocracies. Hybrid regimes do not consolidate their power in society as much as closed autocracies, therefore popular support is still important for them to stay in power. The source of this public support is the elections. Therefore, the elections are not completely façade in hybrid regimes, unlike closed autocracies. Hence, even though they are not completely free and fair, elections are competitive and this makes election times a critical juncture point for the hybrid regimes. The second characteristic is that hybrid regimes have authoritarian tendencies and eroded non-independent institutions and this way they differentiate from the democracies. The elections are competitive, however, the regime resorts to unlawful techniques to secure the elections and the incumbency. Therefore, Internet shutdowns and censorship can be one of those techniques, a new way to limit the free media and flow of information during critical times. Hence, I argue that the relationship between the elections and the restrictive strategies is best studied in hybrid regimes.

In this chapter, I discussed the existing literature about the effect of the Internet on democratization, public movements, and authoritarian repression and connect this literature with competitive authoritarianism and digital authoritarianism. Then I discussed the categorization of restrictive and proactive strategies in detail in order to define the authoritarian strategies to control and restrict the digital space. In the following sections, I am going to move my empirical research to test my arguments. First, I am going to look at the relationship between restrictive strategies and elections with two quantitative analyses. Second, I am going to make a detailed case study to examine the use of restrictive and proactive strategies in a competitive authoritarian regime.

3. PREELECTION PERIOD AS A TRIGGER FOR RESTRICTIVE STRATEGIES

In this chapter, I am going to discuss one of the factors which arguably triggers the use of restrictive strategies, namely the elections. My main argument in this chapter is that election period is an important determining factor of the Internet control strategy of a regime. Election period is a turning point especially for competetive authoritarian regimes because regimes' legitimacy depends on elections and the stakes are very high in case of electoral defeat. Therefore, elections are critical periods for hybrid regimes. Not only the election day, but the periods preceding and following the elections are important too. The period following the elections are especially ciritical in cases of opposition victories, whereas the period preceding the elections is always critical because of the uncertainty. It is an important period for opposition and incumbent to reach the voters, therefore the role of the media in general has a great importance. In hybrid regimes, media is systematically controlled and manipulated to serve the durability of the regime. The main argument of this chapter built on this logic. Hence, I argue that during preelection period, the regime has a higher likelihood to use restrictions.

In the literature, the arguments supporting the relationship between the elections and restrictive strategies are mostly based on anectodal evidence. Therefore, a detailed analysis and statistical evidence of the relationship between elections and restrictive strategies are missing. Therefore the arguments remain in need of supporting studies. The main goal of the analyses in this chapter is to contribute to that gap in the literature.

Here, I examine the restrictive strategies as the censorship on the websites, and use the number of political criticism websites restricted from access as the measurement. The reason to choose censorship on the websites to represent the restrictive strategies is that it better signifies the subtle and temporary nature of the restrictions imposed by hybrid regimes than broadband Internet shutdowns and slowdowns, and it is easier to keep track of than the content-based restrictions and bans. The restriction

practices during the elections cannot be broadband because this would severely damage the reputation of the regime during such a critical period. Therefore, there should be a more specific, strategical restrictions to repress the oppositon without getting too much attention. There are subtler techniques of restrictive strategies such as bans on specific content, however, there is no data source that report the cases of single content bans. Therefore, the data on specific content bans is not availiable.

Hence, the main dependent variable in the two analyses is the count of restricted websites. Only the websites that are dedicated to political criticism are included. There are other censorship cases related to pornography, gambling, or alcohol&drugs, however they are excluded due to their irrelevance with the study. The data come from Online Observatory of Network Inference (OONI) which is a platform offering open data about the internet censorships since 2012 from more than 200 countries. I will explain the rest of the research designs and also the findings in the following sections of each analysis.

3.1 The effect of preelection period on the use of restrictive strategies: cross-country analysis

3.1.1 Research Design

In this analysis, I work with cross-sectional data with 32 hybrid regimes and I employ a difference in differences (DiD) model to test the main hypothesis. The countries are selected firstly based on their score on the V-Dem (V-Dem 2023) regime classification. I include both types of hybrid regimes, namely electoral autocracies and electoral democracies in the sample. The next selection parameter is the data availability in OONI Explorer (OONI 2023). I look for two years long weekly data for each country, however, the data of most countries have lots of missing weeks. This would create a big problem therefore I simply exclude the countries with missing data from my sample. To increase the chances of data availability, I focus on the most recent elections for the countries in the treatment group. Hence, the treatment goup consists of the countries that have elections in 2022 or 2023. The main hypothesis is that:

Hypothesis: The number of restricted political criticism websites increases during the period one year before the elections.

The treatment period is set as one year before the election date, thus the treatment is entering into the election year. I picked the period one year before the elections in order to capture the restriction activities of hybrid regimes during a period of approaching the elections. Setting the election date as the treatment would not allow me to focus on the critical election propaganda period in which regime feels the biggest vulnerability. Another time period might be picked as well, for instance the day that the election date is officially announced, or the day that official period of election campaigns begins. However, I choose one year before the elections, to capture the variation between the election regulations of different countries, and also not to miss the activities of the incumbent party that unofficially begin before the campaign period.

To test the hypothesis, I employed a DiD model with two-way fixed effects (TWFE). Beacuse of the most diffferent system design, there is a big variation of country specific characteristics in the sample. The time periods, altough there is only one year at most between the election dates of the countries, is varied too. Therefore I choose to make a TWFE estimation to include the country and time specific trends. The theoretical expectation is that the regime tends to increase its control on the Internet because of the sense of threat coming from the approaching elections.

As the main dependent variable, I collected the count of restricted political criticism websites from OONI on a weekly basis for each of the 32 countries in the sample. So, the sample consists of a collection of 32 countries' data between the years 2020 and 2023. I picked the most recent time period because the earlier periods do not have available data. I collected a two year long data for each country. One year for the treatment period, and the other year is for the control period. The data of the treatment group is collected two years before the election date, and therefore for the countries that have elections on 2022 the date range goes back to 2020. For the control group the data was collected between the years 2021-2023. Because, there is not elections in those years in control group countries, I simply collected the most recent data. Both treatment group and control group include 16 countries and contain electoral democracies and electoral autocracies. Table 3.1 shows the distribution of the countries across regime type and treatment or control group.

Because of the sample size and the diversity of the country-specific characteristics, a set of additional variables was also included. I borrowed the control variables of Miller (2022). He works with the temporary censorships before the elections and introduced the controls which most probably affect the countries' Internet penetration, citizens' Internet usage, and regimes' tendency to employ censorship. For the country-specific distinctions, GDP per capita and regime type; for Internet penetra-

Table 3.1 Countries in the sample by regime type and control group

Regime Type	Control Group	Treatment Group
Electoral Autocracies	Algeria, Belarus, Egypt, India, Iraq, Russia, Singapore, Ukraine, Venezuela	Bangladesh, Hungary, Kazakhstan, Malaysia, Philippines, Serbia, Tunisia, Turkey
Electoral Democracies	Argentina, Chile, Indonesia, Mexico, Poland, Romania, South Africa	Austria, Brazil, Colombia, Czechia, Greece, Kenya, Moldova, Portugal

tion of the country, mobile cellular subscription rate, and broadband subscription rate; for citizen's Internet use, again mobile cellular subscription rate and labor participation ages 15-24 are included in the data. Labor participation of ages 15-24 is included in order to capture the youth population which is assumed to be the group of people with the highest Internet usage. All of the control variables come from World Development Indicators of World Bank (WorldBank 2023), except the regime type which comes from V-Dem (V-Dem 2023). The control variables are included in the model through country-fixed effects.

The limitations of TWFE design stem from my data. There is heterogenity in the time period I use, therefore TWFE give biased results. Together with TWFE estimation, I employed Callaway Sant'Anna (2021) estimator too, because of the limitations of the TWFE model to capture country and time trends in cross-sectional time-series data. The main variable is count data, for this reason too the Quasipoisson regression would be more appropriate to use instead of OLS. Other than that, the main variable is distributed heavily right-skewed because of the high density of weeks with no restrictions and the rare occurrence of weeks with very high restrictions. I report the density curve and histogram of the dependent variable in Appendix A. Hence, Quasipoisson regression in the TWFE estimation would be better than OLS to fix the skewness too. Quasipoisson is a type of Poisson regression that fixes the falsely calculated standard errors caused by overdispersion of the data. In Callaway Sant' Anna Estimation, I take the log of the dependent variable to fix the skewness. For descriptive statistics, please see Table 3.2.

Table 3.2 Descriptive statistics - cross country analysis

	N	Mean	SD	Min	Median	Max
Restricted Websites	3360	201.23	606.58	0.00	10.00	6857.00
GDP per Capita	3360	12849.09	14714.11	2081.80	8368.67	72794.00
Mobile Subscription	3360	121.52	22.55	60.32	123.25	168.98
Broadband Subscription	3360	19.39	11.33	1.49	19.27	42.46
Labor Force 15-24	3360	32.76	10.67	13.84	31.37	56.39
Regime Type	3360	1.47	0.50	1.00	1.00	2.00

3.1.2 Findings

3.1.2.1 TWFE estimation

TWFE estimation results are shown in Table 3.3. Country and year-fixed effects are not included in the table. The unit of analysis is week-country and there is 105 observations for each country. The DiD estimate has a statistically significant effect, this implies that entering into the election year has a significant impact on the number of restricted political criticism websites. The coefficient of the interaction of election year and election country is 1.5 and it is statistically significant. This means that In countries that have elections during treatment period, weekly 1.5 more websites is restricted. The mean of the depndent variable is weekly 201 websites. Substansive significance of the estimate is approximately 0.06, hence we can conclude that substansively, the estimate much significant. Nevertheless, this estimation supports the theoretical expectations of the hypothesis. Regimes have a higher likelihood to restrict access to political criticism websites, when an election will be held within a year.

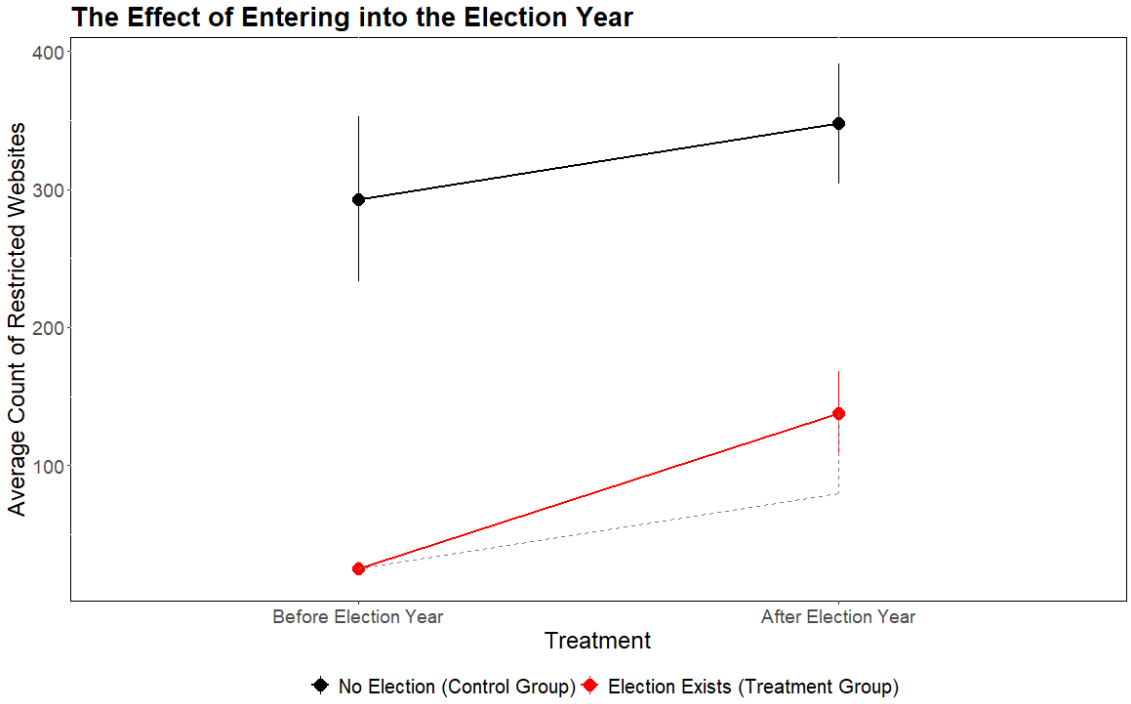
Table 3.3 TWFE estimation results

	TWFE DiD Estimation with Quasipoisson Regression
Election Year	0.696**
	(0.226)
Election Country	1.648***
	(0.204)
Election Year x Election Country	1.540***
	(0.070)
Num.Obs.	3360

Note: p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001
Note: Standard Errors in the parantheses
Note: Country and year fixed effects are included in the model.

The change in the average count of restricted websites in the treatment group in the periods before and after the election year is higher than those in the control group, as seen in Figure 3.1. This shows the effect of entering into the election year on the count of restricted political criticism websites. The change in the control group is smaller han the treatment group.

Figure 3.1 The visualization of possible DiD effect - TWFE estimation



3.1.2.2 Callaway-sant'anna estimation

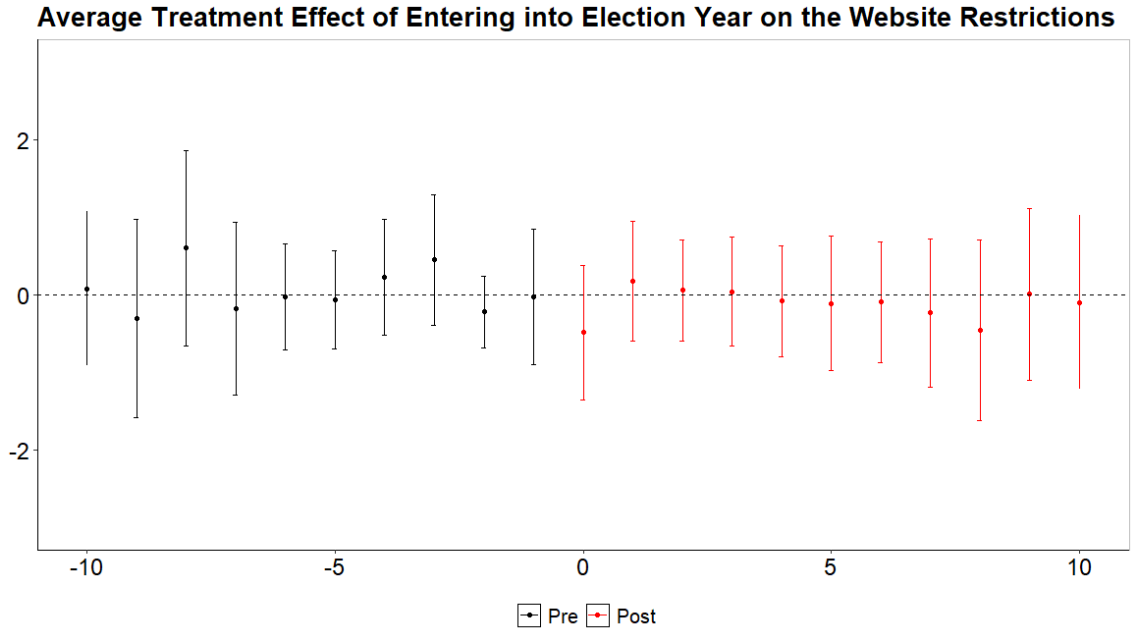
Even though the results of the TWFE DiD estimation are significant and confirm the hypothesis, the Callaway-Sant'Anna estimation does not support it. The average treatment effect is negative, as can be seen in Table 3.4. However, it is not a significant effect.

Table 3.4 Average treatment effect of callaway sant'anna estimation

ATT Score	Std. Error	95% Confidence Intervals
-0.68	0.45	-1.566 - 0.2051

As can be also seen in Figure 3.2, entering into the election year has no effect on the number of restrictions imposed on political criticism websites, according to the Callaway-Sant'Anna' estimation.

Figure 3.2 Callaway sant' anna estimation results



Based on the TWFE estimation, the null hypothesis is rejected, and the model stands as evidence to the relationship between the elections and the use of restrictive strategies. However, based on the Callaway Sant'Anna estimation, the null hypothesis cannot be rejected, and the theoretical expectations are not fulfilled. Based on these results, we can say that the generalizability of this model is low. A different estimation model would fit this hypothesis better. To test the hypothesis once again in a single case, I am going to focus on Turkey in the next section.

3.2 The Effect of Preelection Period on the Use of Restrictive Strategies: Turkish Case

3.2.1 Research Design

Turkey has been experiencing democratic backsliding for about 15-20 years under the AKP government. For the Turkish regime, the elections have at most importance because their popularity and legitimacy come from populist discourse and election victories. The elections maintain uncertainty because there is no fraud or stealing of the elections however the same thing does not hold for free and fairness. The regime secures the election results via the domination of the media sources mainly. It manipulates the media, openly degrades the opposition leaders and associates them with terrorism, and cuts down their access to media sources. For these reasons I

choose Turkey as my case study for the analysis of the digital media controls during elections.

The research design is almost the same as the cross-country analysis. The hypothesis is again:

Hypothesis: The number of restricted political criticism websites increases during the period one year before the elections.

To test the hypothesis, I made a DiD design with the synthetic control unit. The main dependent variable is the same as the cross-country analysis. One difference is that the count of restricted political criticism websites is collected on a daily basis. The data come from OONI again. The focus is on the 2023 general elections; therefore, I gathered the count of restricted websites between May 2021 and May 2023. The period between May 2021 and May 2022 constitutes the period before treatment, and the period between May 2022 and May 2023 constitutes the period after the treatment.

I used synthetic control unit as the control group. This method is borrowed from Miller (2022). Following his operations, I constitute a synthetic Turkey that has no elections during 2021-2023 but is the same in other aspects. To create the synthetic unit, first I gathered data with five covariates from every country in the World Developments Indicators series of World Bank (2023). The covariates are the same variables as the controls in the first analysis, except for the regime type. GDP per capita, mobile subscription rate, broadband subscription rate, labor force participation ages 15-24, and lastly Freedom on the Net Score (FOTN) coming from Freedom House (2023) instead of regime type. Based on these five covariates, I calculated the Mahalanobis distance of each country relative to Turkey, and 15 countries with the lowest Mahalanobis distance constituted the donor pool. As a result, I created a synthetic Turkey based on the weighted data of these 15 countries. In Table 3.5, the donor countries are listed.

Table 3.5 Countries constituting the donor pool

Donor Countries
Argentina, Brazil, Belarus, Germany, Hungary, India, Iran, Iraq, Mexico, Russia, Saudi Arabia, Pakistan, Serbia, Thailand, Egypt

I created synthetic Turkey in R. I gathered the data, picked the donor pool, and employ the synthetic control operations in R. As a result, I reached the synthetic Turkey which I will be using as the control country in DiD estimation. The comparison of the scores of synthetic and actual Turkey can be seen in Table 3.6. They

are more or less the same except for the difference in the FOTN score.

Table 3.6 Balance table

Covariates	Treated	Synthetic	Sample Mean
GDP per capita (current US$)	9661.24	9665.34	11561.80
Labor Participation ages 15-24	53.13	53.12	45.09
Mobile cellular Subscription	101.78	107.91	118.92
Broadband Subscription	21.39	21.39	20.75
Freedom on the Net Score	34.00	40.69	46.20

The dependent variable is right skewed as can be seen in the density curve and the histogram in Appendix A. For the descriptive statistics, please see Table 3.6. Because the dependent variable is count data and because it is skewed to the right, the Poisson regression is used instead of OLS in the DiD estimation, like in the cross-country analysis.

Table 3.7 Descriptive statistics - Turkish case

	N	Mean	SD	Min	Median	Max
Restricted Websites	11936	185.03	514.04	0.00	19.00	7273.00
GDP per capita	11936	11443.01	11663.82	1505.01	8368.67	51203.55
Mobile Subscription	11936	117.85	26.96	81.55	114.85	168.98
Broadband Subscription	11936	20.79	11.23	1.27	20.41	44.22
Labor Force 15-24	11936	45.60	9.32	34.61	43.15	64.66
FOTN Score	11936	45.44	20.02	16.00	38.50	79.00

3.2.2 Findings

Entering into the election year seems to influence the use of restrictive strategies in the Turkish case, as can be inferred from Figure 3.3. The top chart in Figure 3.3 is the line chart of the log count of the restricted websites, in the bottom chart the fitted line is reported for the effect to be seen clearer. The number of restricted websites increased more in actual Turkey than it is in synthetic Turkey, due to the elections. The effect of the DiD estimation can be seen in Table 3.7. The DiD estimate gives statistically significant results, this means that entering into the election year increases the number of restricted websites by 0.25 websites in a day. Substantive significance is approximately 0.001 which means even though statistical significance is high substantively results are not striking.

With this analysis, the theoretical expectation of the main hypothesis is fulfilled. Restrictions on political criticism websites are higher in the period approaching

Table 3.8 The results of the DiD estimation - actual Turkey vs synthetic Turkey

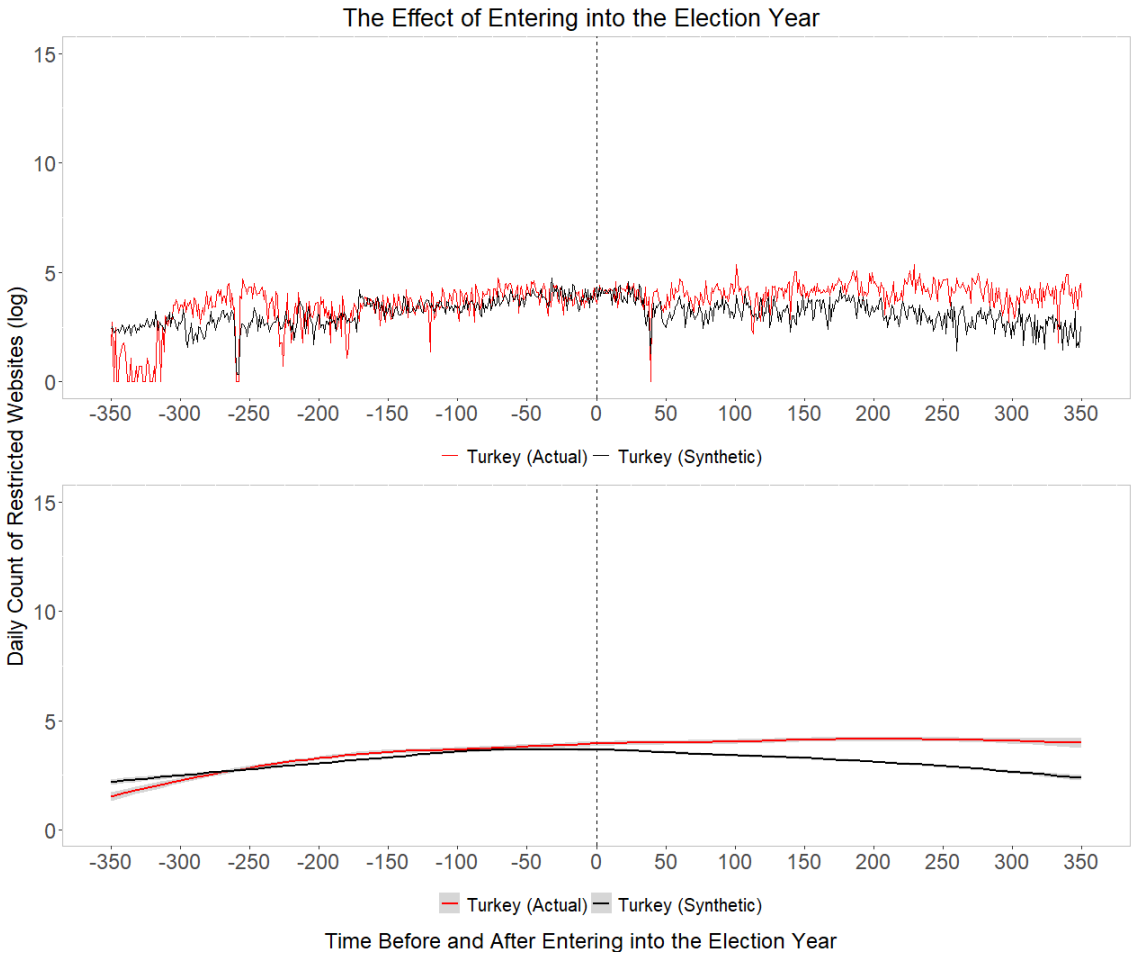
	DiD Estimation with Poisson Regression
Election Year	0.0257
	(0.0187)
Having Elections	0.0138
	(0.0187)
Election Year x Having Elections	0.2531***
	(0.0257)
Num.Obs.	1492

Note: p < 0.1, * p < 0.05, ** p < 0.01, *** p < 0.001
Note: Standard Errrors are in the parantheses.

elections in Turkey. However, the generalizability of the analysis is limited. The hypothesis is tested only in one country and only in one case in this country. Previous elections in 2014 and 2018 can be included to see whether the effect is still significant in these too. The 2023 elections are general and presidential elections. Another thing that can be checked is that whether the effect still holds in local elections. The regime might have different strategies in local, parliamentary, and presidential elections. This analysis only considers the first round of the elections, expanding the time period to capture the second round would give more interesting results. Focusing only on the period between the two rounds of the election might be another idea, considering that this time period is highly crucial for the regime.

During elections, the regime would not want to trigger anti-regime sentiment by imposing open and broad restrictions, on the contrary, it would try to appear as democratic as possible. Therefore, the restrictions cannot be broadband if it is not absolutely necessary on the regime's part. Proactive strategies are also used complementarily during elections. Together with the subtle censorship of opposition and criticisms, the propaganda of the regime is made in social media through various manipulation methods. To put it another way, restrictive and proactive strategies are used in combination in critical times. As a complementary to these analyses, in the future, regimes' activity with proactive strategies can be studied to understand the regime's behavior more comprehensively during the elections. Furthermore, it would be interesting to see how the regime manages the level of challenge that the election poses to its durability and also the level of risk and fragility increasing as election day approaches. Seeing the variation between different elections might be more explanatory on this account. Also, designs that can capture the increasing importance of the passing days until election day would show us a different point of view. These are the ideas that can be pursued in the future.

Figure 3.3 The visualization of the possible DiD effect - actual Turkey vs synthetic Turkey



In this chapter, I analyzed the relationship between elections and the use of restrictive strategies. The results of cross-country analysis give partial evidence for the argument of regimes have a higher likelihood to restrict the websites including political criticism during the pre-election period. The analysis focuses on the 2023 Turkey elections to support the argument. However, these studies show only a small part of the issue. Nevertheless, the relationship between Internet control strategies with elections cannot be denied. These studies can be considered as preliminary analyses of election-Internet control strategies which might open the way for new research mentioned in the previous paragraph. Especially, the combination of restrictive and proactive control strategies needs more attention. In the following chapter, I will examine this in the example of Turkey. My argument here is that we can better capture the combination of restrictive and proactive controls with a case study because it greatly depends on the regime's special structure to endure the regime in general. For this reason in the following chapter, I will also provide a brief revision of the authoritarianisation story of Turkey together with a short discussion of regime-media relationships.

4. RESTRICTIVE AND PROACTIVE STRATEGIES IN PRACTICE: THE CASE OF TURKEY

In this chapter, real-life examples of restrictive and proactive strategies will be analyzed based on the Turkish case. The main aim is to see the distinct combination of the restrictive and proactive strategies with a detailed case study while examining the real-life application of the categorization provided in this thesis. As a hybrid regime, Turkey has both democratic and autocratic characteristics. On the one hand, the authoritarian tendency of the regime is growing day by day, this increases the expectations to observe the radical ends of both strategies implemented in Turkey such as broad Internet shutdowns, or completely nationalized cyberspace. However, on the other hand, the regime still takes its power from regular elections, and keeps its durability through populism, therefore it depends on popular support and legitimacy. In order to keep the support intact, it requires to keep its legitimacy and a façade of respect for the elections and democratic values. Therefore, cleverer, and subtler ways of Internet control are expected to be observed too.

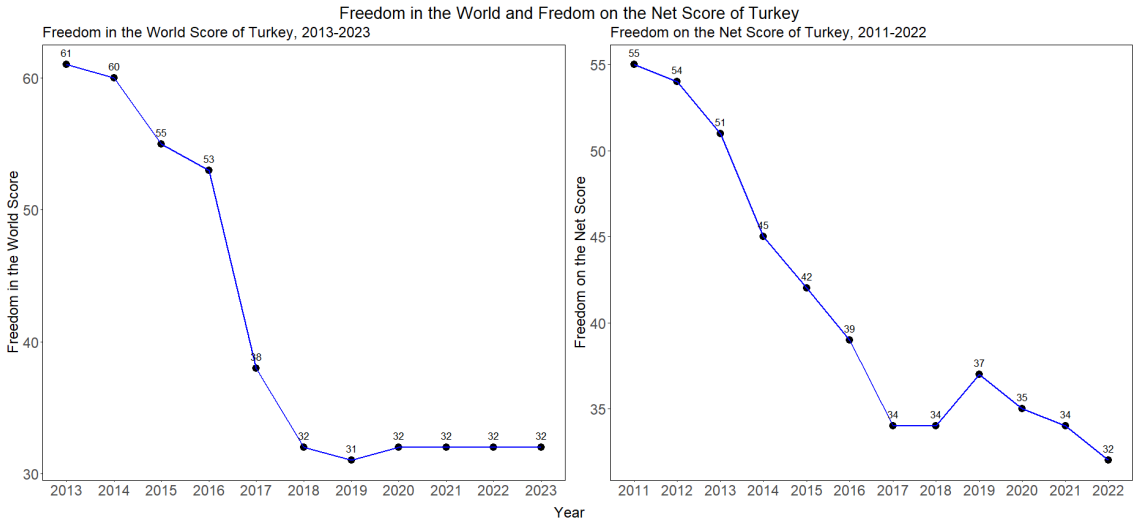
The chapter consists of three main sections. In the first section, the story of gradual democratic backsliding in Turkey, and in line with this, the history of authoritarianisation of digital governance will be analyzed. In the second section, the usage of restrictive strategies, and in the third section the usage of proactive strategies in Turkey will be the focus of the discussion.

4.1 Turkey's Authoritarianisation Story

The authoritarianisation trend that captures countries like Hungary, and India affected Turkey as well, most probably in a much more severe way. Approximately for 10 to 15 years, Turkey is going through a gradual democratic backsliding. Twenty years of AKP rule strengthen its durability via the erosion of democratic institutions,

control over the media, centralization of power, and marginalization of opposition. Turkey, once a tutelary democracy, is today accepted as a competitive authoritarian regime (Esen and Gumuscu 2016). AKP has won parliamentary majority in five consecutive elections between 2002-2018, and three victories in local elections between 2004 and 2014 (Demiralp and Balta 2021). Besides this big achievement in the ballot boxes, however, civil liberties have deteriorated through the years and the creation of controlled digital media is a part of this process (see Figure 4.1).

Figure 4.1 Freedom in the world and freedom on the net score of Turkey



Source: Freedom House

AKP government's policies are reflected in its Internet governance too. In this section, the gradual erosion of Turkish democracy will be reviewed and then the reflection of this process in digital media will be discussed.

4.1.1 Democratic Backsliding

In 2002, when the AKP came to power, it was away from the current authoritarian intentions. For the first years of its rule, it was even accepted as a showcase of the successful democratization in a predominantly Muslim country, looking at its trajectories to build an inclusive democracy based on the values of "liberalism, human rights, and, the market economy" (Kubicek 2020, 245). Turkey was a tutelary democracy at the beginning of the 2000s, a democracy which is under the political pressure of the military and judiciary (Esen and Gumuscu 2016). Those two institutions were keeping the tutelary power over the civilian government and through their ability to veto the parliamentary decisions. AKP's main aim was to reform

the state institutions to build a more inclusive structure for Turkish democracy, and this was especially appealing to the excluded groups from the conservative and Islamic parts of the society, and from Kurdish background. Hence, in the first years of its rule, the AKP government gained popularity among the central-right and religious voters, and also the Kurdish minority, while being accepted as the government that brings Turkey democratic consolidation by the international community and secular-liberals within the country (Esen and Gumuscu 2016; Kubicek 2020).

Unexpectedly, the AKP rule did not continue with the same path that it began, left the liberal democratic, inclusive approach, and took a more dominant and exclusive stance, over the passing years. Reformed the institutions to maintain their durability with the help of populist discourse. Demiralp and Balta illustrate the current state of the AKP regime as populist competitive authoritarianism and add that "these regimes build an election-winning machine that is sustained by three key strategies: a tightly controlled media, a punishment system relying on a coopted judiciary, a giant patronage system that redistributes state revenues" (Demiralp and Balta 2021, 4). Thus, media control, subordinate judiciary and criminalization of the opposition through it, and clientelist relationships are the three pillars of populist authoritarianism that is built by the AKP government during their 20 yearlong rule.

The gradual transformation of Turkey from tutelary democracy to competitive authoritarianism happen step by step, through incremental reforms. With every step, the checks and balance mechanism of the country was hurt, the institutions that are supposed to keep the executive limited were eroded and the power is centralized in the hands of Erdoğan. Esen and Gümüşçü (2016) portray the Turkish case of competitive authoritarianism based on three characteristics. These three characteristics are the result of the slow erosion of democracy, and what ensures the authoritarian rule's durability today. According to them, in competitive authoritarianism in Turkey, elections are regular but "unfair", parties compete on an "uneven playing field", and civil liberties are violated by the government. The reason for the elections being unfair is not systemic manipulation or fraud during the elections. The incumbent does not steal the elections; however, it secures the elections, through the election laws in favor of the incumbent and is disadvantageous for the opposition. For instance, campaign limitations limit the official election campaigns to a short time period, however, the incumbent starts to make election campaigns unofficially during public events. The limited access of the opposition to the media and the resources on top of it creates a big gap between the incumbent and the opposition, obliging the opposition to compete with the incumbent on an uneven playing field. This is the mechanism of the "election winning machine" and it is very hard to break the chain of populism-electoral victory-further centralization of power. The regime

uses the victories of the unfair elections to bolster its popularity among voters and reform the check and balance institutions in a more centralized way at the expense of civil liberties.

To put authortarianisation story of Turkey in chronological order, we can state a few turning points. Starting with the 2002 elections when they first came to power, until 2011 their popularity increased among people, and they won election victories. While their revisionist trajectory and economic success were contributing to their credit, the underlying constitutional reforms started to weaken the institutions of checks and balances, civil society, and free media. From 2013 onwards, the centralization of power became more apparent with the harsh response of the government toward the Gezi protestors. Together with the Gezi protests, 17-25 December Corruption and Bribery Investigations is another challenge for the regime, and these challenges resulted in an increase in repression. Opposition was marginalized, degraded, and criminalized; traditional media became almost completely under the regime's control. These limitations increased the popularity of digital media as an alternative platform to discuss opinions and make demands. However, the regime's response to this was not late, digital censorship increased heavily, and social media was portrayed as big trouble for society. In 2015, AKP lost the majority in parliament, following this ended its policies to maintain the peace with the Kurdish minority in eastern provinces. As a result, the violence increased and AKP regained the parliamentary majority in an early election held after four months. In 2016, after the failed coup attempt, the regime's authoritarian tendencies peaked, the country was governed by decree laws; the media was censored heavily; many journalists, and opposition leaders were arrested. In 2017, with the constitutional referendum, the executive power is collected in the hands of the president with no veto power of the legislative (Esen and Gümüşçü 2017). With the victories in the 2019 and 2023 general elections, AKP continued to monopolize the power and along with this continue to increase the repressions.

Control over media is a very important part of this system. The manipulations are made through the media, and the opposition's chance to reach the voters is limited through the media. Digital communication technologies enter this space as a challenge because of their revolutionary structure, speed, and interaction. However, the Turkish government finds ways to tame the Internet as well. Let's have a look at the story of the authoritarianisation of the media in general and then focus on the history of controls over digital media in the following section.

4.1.2 Authoritarianisation of Traditional and Digital Media

The strategy to control the media is based on ownership of the media in Turkey. Yeşil (2014) argues that the media in Turkey has never been free. The subordination of the media to the government is set by the constitution itself. However, under the AKP rule, press-party parallelism has increased and politically motivated activities is increased. AKP monopolized the press ownership by buying the big media conglomerates one by one or building clientelist relationships with other enterprises of these conglomerates (Yanatma 2021) and used it as tools for regime propaganda. In 2004, Star and Star TV was confiscated and sold to Doğan Group which was eventually acquired by AKP. A similar case happened in 2007 when the media holdings of Ciner Group were taken over and then sold to a company owned by Berat Albayrak. In 2011, Doğan Media had to sell firstly Milliyet and Vatan, and then Hürriyet and Doğan Haber Ajansı to Demirören Group, in order to pay the extremely high fine sentenced in 2009 (Yıldırım, Baruh, and Çarkoğlu 2021). Besides the media ownership, the Turkish government has the power to impose punishments on journalists and censor the news based on Press Law, Penal Code, and Anti-Terror Law (Yesil 2014). The authoritarianisation of the AKP government increased the use of these powers. Turkey ranked 157th out of 180 countries in the 2019 World Press Freedom Index by Reporters without borders (Yıldırım, Baruh, and Çarkoğlu 2021). Thus, the control over the media is done by ownership and also penalizations, and its parallel with the democratic backsliding of the regime.

The Internet has first perceived as a threat from 2007 onwards. The cases of online sites including content about child pornography unsettled society and created a fear towards the Internet. Starting with that, until 2013 the Internet interferences of the government were based on moral issues, hence the restrictions were directed towards websites including sexuality, pornography, drug use, and video games (Yesil, Sözeri, and Khazraee 2017). However, moral issues are not the only concern of Internet restrictions. A series of penal code reforms were made to "criminalize the speech that insults the Turkish nation, government agencies, or the military" (Yesil, Sözeri, and Khazraee 2017, 5). The criminalization of certain digital content was established by newly introduced laws and regulations like anti-terror law, and intellectual property law. Telecom and Communication Presidency (TIB) attempted to categorize the harmful content and introduced the "Internet Law". Mandatory Internet filtering was an additional project of TIB based on the categorization made by them. It would have put an initial filter to the Internet usage and automatically restrict the access to the URLs that are labeled as harmful by TIB if it was implemented, however strong criticisms prevent it to be enacted. So, the first phase of Internet

government was based on the moral issues and protection of family values with subtle attempts to institutionalize the rules of the Internet.

The regime's stance towards the Internet started to change from 2013 onwards together with the Gezi protests. It was right after the Arab Spring and the expectation from the Internet to liberalize the closed regimes was dominant. Gezi protests in Turkey were associated with the Arab Spring protests, partly because of its timing, and mostly because of the effective usage of social media accounts by the protesters to mobilize. This was the first time in Turkey, that social media facilitated a social movement against the regime. The government met this event with a strong negative reaction and demonized the Internet altogether. Social media activity started to be associated with terrorism, and disobedience. The Prime Minister of the time, Erdoğan, even dubbed social media as the biggest calamity of societies. Afterward, the Internet restrictions were taken for the ultimate goal of protecting public safety. Surveillance activities conducted by National Intelligence Service (MIT) and through the ISPs; strong restrictions to prevent criticisms about "corruption scandals, foreign policy failures, the Kurdish issue and/or security crises"; and content removals are started to be implemented (Yesil, Sözeri, and Khazraee 2017, 8). Failed coup attempt in 2016 resulted in stricter controls over the Internet. The Information Technologies and Communication Authority (BTK) was granted full access to the individual online activity with decree laws (Yesil and Sozeri 2017). The restrictions over the Internet and tight control strategies are increasing since then. Today, Internet controls are highly institutionalized and this institutionalization prepares the ground for both restrictive and proactive strategies. Before moving to the restrictive and proactive strategies of the Turkish government, I will first review the institutionalization of the controls on digital media, and discuss how this facilitates the implementation of both strategies.

4.1.3 Establishment of Internet Governance and Surveillance Institutions

Internet governance in Turkey started as part of the institutions that existed to control the media, and through the years it expanded into national security institutions too. Today, the Internet governance structure is constituted by several special institutions and several departments of the existing institutions.

Sarı (2019) lists the institutions dedicated to the Internet. Cyber Security Council of the Ministry of Maritime Affairs and Communications, The National Cybercrime Intervention Center (USOM), The Information Technologies and Communi-

cation Authority (BTK), the National Research Institute of Electronics and Cryptology (UEKAE), and Cyber Emergency Response Team (CERT) under the roof of TUBITAK are the institutions dedicated to Internet controls. Cybercrime investigations and defense against cyber-attacks are the foundational goals of these institutions. However, the reason that makes the Internet government authoritarian is the range of power of these institutions that can violate individual rights and freedoms and the ability of these institutions to take arbitrary decisions in line with the regime's goals.

Information and Communication Technologies Authority, BTK with its Turkish abbreviation, is the most important Internet governance institution. Currently, the vast majority of censorship decisions and individualistic bans are done through BTK. It is an institution operated under the Ministry of Transport and Infrastructure, but it is an autonomous authority dedicated to govern especially digital media.In 2000, the Information and Communication Technologies Authority was established under the name of Telecommunications Authority. The actions of BTK and the autonomy of it are based on Electronic Communication Law enacted in 2008. However, it was given almost limitless authority over individual digital activity when the regime deems it necessary as we see in the case of the failed coup attempt in 2016. Its foundational goals were regulating Internet activity, preventing the dissemination and promotion of criminal websites, and protecting children and family values. Starting with its foundation, protection is a word that is used as a shield of the BTK. Firstly, it was established to protect family values, today its goal is to protect induvial rights. The legitimization rhetoric is an inherent characteristic of these institutions.

In 2008, Telecommunications Authority turned into Information and Communication Technologies Authority with Electronic Communication Law. This period is also the period when Turkish digital space started to be censored by the regime. BTK determined harmful and illegal content on the Internet, and authorities offered to establish a national filter to pre-censor the digital space through BTK. In 2016, after the failed coup attempt, BTK has been granted to rule by decree laws and unlimited access to individual records of digital activity. As the regime gets more authoritarian, BTK has turned into a censorship and digital policing tool rather than a digital regulation and governance tool.

The most recent development regarding this institution is the Disinformation Bill enacted on October 13th, 2022. With the new bill, BTK is aiming to "prevent the spread of false, untrue, baseless, and dales information, designed to create a specific perspective, and ensure that anonymous accounts can be associated with real persons" (Rojas Navarro 2023, 2). This bill was criticized because of its reach to the

individual accounts directly. BTK does not need to consult any journalists before it decides one content is a case of disinformation. For this reason, many believe that the Disinformation Bill will allow BTK to make digital censorship on a scale that has not been seen before (Rojas Navarro 2023). Rojas Navarro (2023) argues that BTK seems to aim at the prevention of disinformation and fascism in digital space, however, it actually targets free speech. In fact, according to Medyascope (2022) article, BTK now collecting the records of individual digital activity and personal data. BTK can collect un-anonymous data on individual activity by the vague language of its regulation. This way regime's capacity to censor the digital media and make individualistic repressions is increased and with BTK it becomes more systematic and legitimized.

Institutionalization and legitimization of digital repression is a common goal of these digital governance institutions. The legitimization of the cyber operations is made by those institutions and possible criticism against the regime's control over the Internet is prevented with this. Yeşil and Sözeri (2017, 544) explain how the regime in Turkey "instrumentalize the populist rhetoric that valorizes the good, responsible, and patriotic citizens, (...), and labeled dissidents and critics as sources of threat". The opposition is criminalized, and the activities to prevent the dissemination of unwanted content are legitimized through populist rhetoric. The arrests, investigations of private accounts, and surveillance are necessary because they are all a case of national security. The Cybercrime Department of the General Directorate of Security has a section for the laws and regulations that the arrests are based on in their website:

> "Articles 135-138 of the Criminal Procedure Law dated 04.12.2004 and numbered 5271, Electronic Communications Law dated 05.11.2008 and numbered 5809, Regulation on the Procedures and Principles Regarding the Detection, Listening, Evaluation, and Recording of Signal Information and the Establishment, Duties, and Authorities of the Telecommunication Communication Presidency (Prime Ministry Regulation), Regulation on the Supervision of Communication via Telecommunication, and the Implementation of Monitoring Measures by Confidential Investigators and Technical Means, as stipulated in the Criminal Procedure Law, published in the Official Gazette dated 14.02.2007 and numbered 26434 (Regulation of the Ministry of Justice)" (EGM 2023).

Hence, institutionalization is the first step for restrictive and proactive strategies, it enables the regime to lawfully censor the Internet and clean it from any harmful content. This way, the ground will be prepared for the other techniques of restrictive and proactive controls to be effective. In the following sections, the two types of

strategies will be reviewed and the current state of Internet controls and restrictions in Turkey will be discussed

4.2 The use of Restrictive Strategies

Censorship practices in Turkey date way back to the spread of the Internet among the population. The media has always been under strict control in Turkey. The Internet's penetration into daily usage has become step by step and under the cautious eyes of the government. Today, with the increasing authoritarian tendencies of the AKP government, we are witnessing a highly controlled cyberspace. The restrictive strategies are heavily used by the government and in this chapter, the examples of these strategies will be reviewed. The aim of this section to show the parallelism of the Turkish case with the authoritarian style of Internet controls and make a descriptive analysis of the authoritarian strategies with a specific focus on Turkey.

The restrictive strategies are going to be studied in four categories here. These are broadband shutdowns and slowdowns on the Internet service providers level, censorship on specific websites, bans on unwanted content, and punishments on users who engage in unwanted content. In the following sections, all of these categories will be analyzed one by one.

4.2.1 Internet Shutdowns and Slowdowns

This type of restriction is the broadest one among the four techniques. In Turkey, we encountered broadband shutdowns mostly on social media and communication channels like Twitter, Facebook, Instagram, YouTube, Telegram, and WhatsApp. The shutdowns are implemented at the Internet service provider (ISP) level. The biggest ISP in Turkey is TTNet, and it belongs to the state-owned telecommunication company Türk Telekom. There are several independent ISP's too, mostly for mobile subscriptions such as Turkcell and Vodafone. The shutdowns or slowdowns are enacted on social media platforms especially in times of crises by using ISPs. The most recent one is implemented after the big earthquake catastrophe in the eastern provinces in early 2023 (NetBlocks 2023). According to the NetBlocks and TurkeyBlocks reports Turkey has experienced five temporary shutdowns since 2016 and all of them were implemented following a national crisis. In addition to the southeastern earthquake; the Idlib crisis, the shutdown of the Russian ambassador

in December 2016, the release of the video about the ISIS propaganda again in December 2016, and the deadly blast that happened in Taksim Square in November 2022 were followed by shutdowns of Twitter, YouTube, Facebook, and Whats-app (NetBlocks 2020, 2022; TurkeyBlocks 2016*a*,*b*). These shutdowns are taking only hours. The longest one was enacted after the escalation of the Idlib crisis in February 2020, and it lasted for 16 hours (NetBlocks 2020).

The authorities, the Supreme Board of Radio and Television (RTUK) and the Information and Communication Technologies Authority (BTK) made declarations that the shutdowns are necessary to prevent the dissemination of disinformation and fragile content, however thinking the last shutdown following the earthquake shows that there are higher concerns than the social wellbeing. The shutdown on Twitter hindered the information flow at a very crucial time. Twitter was the main communication channel in the provinces with destroyed infrastructures and the shutdown caused disruptions in the rescue efforts. The shutdown ended up after a half day as a result of huge criticism and reactions within the society.

Hence, shutdowns and slowdowns are temporary solutions, and they have a high potential to cause online dissent. They are enacted as the first reflex of the authorities when they face a crisis. Even though the authorities defend these measures as necessary precautions against the dissemination of harmful content to society, the shutdowns are curtailing press freedom during critical times.

4.2.2 Censorship on Websites

Censorship has a longstanding history of controlling and filtering media content. The definition of "unwanted" and "should-be-censored" content has evolved based on the political agenda and the priorities of the governments. For instance, in the 1980s and 1990s, the unacceptable content was mainly those which include denigration of Atatürk, Turkishness, and territorial integrity of the Turkish State, then under the AKP rule, criticism of the religion and the President became the redline of the media, and subsequently, it changed once again after the failed coup attempt in 2016. Combating terrorism became the primary focus of the censorship practices (Akdeniz and Altıparmak 2018). Currently, complaints about the violation of individual rights coming mostly from high-ranking politicians and their families and/or business associates can be considered the most frequent reason to be unwanted content. The violation of individual rights could be the basis for the indictments by the Criminal Judgeship for Peace, leading to the banning of websites. BTK has a desk for this specific reason and the applications to enact a restriction on a website can

be made via the digital platform of the government, e-Government Gateway. The violation of the individual rights indictments is made mostly for the charges of the violation of the rights of the President, his close relatives, and some high-ranking pro-government business people (Akdeniz and Altıparmak 2018; EngelliWeb 2021). These cases get immediate returns and acceptance in the Constitutional Court. Unlike them, countercases aimed at removing the restrictions have to face significant delays.

The strict controls on the Internet started in 2007 onwards with the realization of the authorities the insufficiency of the traditional ways of controlling the media including penal procedures and press code and the existing institutions like RTUK to keep the Internet within the state limitations (Ververis, Marguel, and Fabian 2020). This way new institutions are channeled to this area and the structure of the Internet regulations was started to be formed around 2007 onwards. Today, the restrictions on the Internet are lawful and backed by multiple institutions.

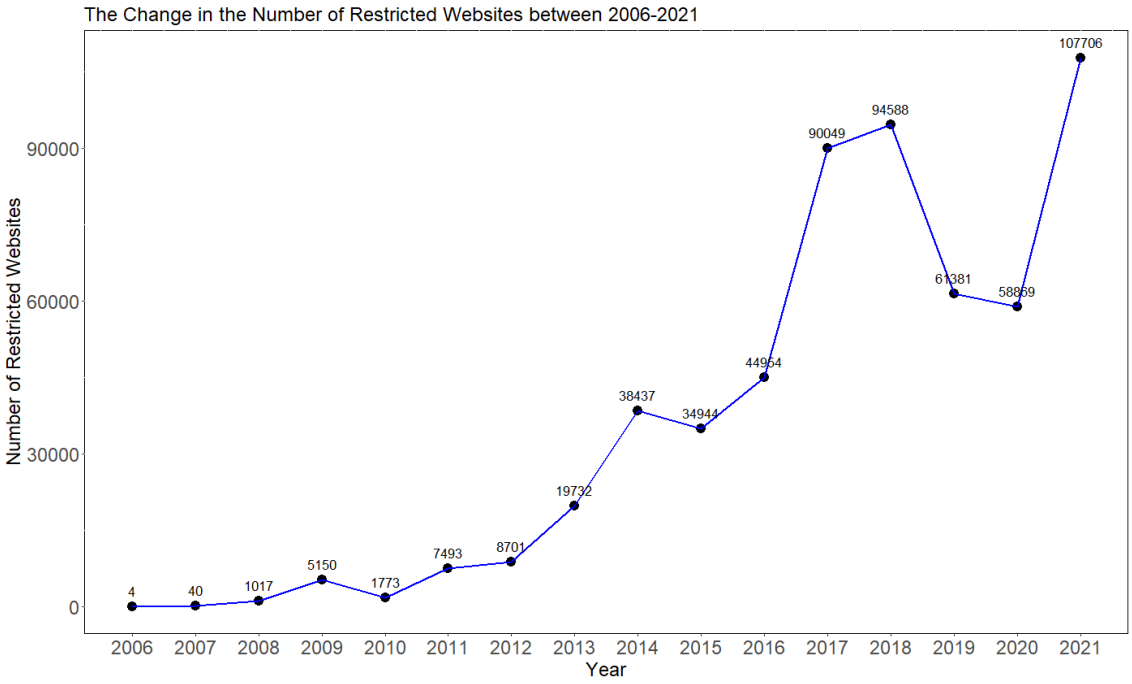
Eldem argues the government defines Internet controls as "a matter of national security" and says that "in military-strategic terms, cyberspace is accepted now as a domain equal to land, air, sea, and space" (Eldem 2020, 2). The authorities legitimize the laws, regulations, and institutions dedicated to controlling and restricting the Internet by reasoning them with the protection of individual rights, protection of family and children values (Ververis, Marguel, and Fabian 2020), and to create a "clean" Internet (Akgül and Kırlıdoğ 2015). Apparently, those arguments provide the legitimate ground for the censorship practices especially among the more religious and conservative group of the society, as shown in survey results of Çarkoğlu and Andı (2021). Hence the censorship practices of the regime are not only supported by the institutional setup, but also, they are legitimized in the eyes of the citizens, or at least on one part of it, with the discourse of nationalism, and social structure.

One clear indication that censorship is not solely driven by the innocent motive of protecting social values, but rather by the government's political interests, is its increasing implementation during times of political crises. Similar to the sudden increase in Internet slowdowns and shutdowns, the volume of the censorship practices increases at times of political crisis such as the occupy Gezi movement or the 2016 failed coup attempt, and during important political junctures like elections (Ververis, Marguel, and Fabian 2020; İlhan 2015). However, censorship is a strategy that is used more frequently than shutdowns. It is like regular filtering of cyberspace. According to the most recent report of the Engelli Web, until 2021, 2604 websites, 3221 Twitter accounts, 618 Facebook accounts, and 1895 YouTube accounts were re-

stricted in Turkey (EngelliWeb 2021, 23). Restrictions, both temporary and permanent, target especially and repeatedly to the Kurdish and opposition websites. Some of the examples are Etkin Haber, Mezopotamya Ajansı Yeni Demokrasi Gazetesi, JinNews, and sedatpeker.com.

In Figure 4.2, you can see the change in the number of websites from 2006 to 2021. The data come from the 2021 report of Engelli Web (2021). The restrictions increased almost every year, especially after 2012 the restrictions increased very rapidly. Looking at the increasing trend in restricted websites we can understand the tightening of the Internet controls through time.

Figure 4.2 The number of restricted websites through the years



Source: Engelli Web 2021 Report

4.2.3 Bans on "Unwanted" Content

The censorship of specific content is very close to the bans on websites. The difference between the censorship of specific content and the bans on websites is that in the former the ban has been put on one particular content which is deemed as unwanted or critical on the part of the regime, whereas in the latter, the whole domain name of a website has been restricted from the access. Content banning can be in the form of complete deletion of the content from the website that it is published, or if the authorities cannot do it because of the policies of social media platforms about

the protection of individual accounts, the access has been restricted in ISP level. As mentioned in the previous category, like censorship the whole domain is based on individual applications to restrict, a URL, a post or a video, or a tweet can be banned based on citizen complaints. This way people are encouraged to look for any harmful posts on social media and a culture of self-surveilling-users and an "online snitching" environment is created (Topak 2019). In a highly polarized society such as Turkey, these policies are likely to deepen the existing polarization, further eroding the already little trust among citizens and marginalizing the opposition groups resulting in social lynching.

The applications based on the violation of individual rights target one specific content. Not the whole domain but only the content that is deemed harmful is banned, such as the URL of a news article about a critical issue. For instance, in 2021, the bans are highly based on the judicial cases opened to protect President's individual rights. According to Engelli Web 2021 report, the articles including unlawful tender bits of Bilal Erdoğan and his businessman friend were banned. Similarly, the Paradise Island activities of Berat Albayrak and Serhat Albayrak were banned from multiple newspaper websites such as Diken, Duvar, Sözcü, and Cumhuriyet on the basis of protection of individual rights, and the violation of honor and integrity. Not only the article URLs but tweets including the same information were also restricted from access to (EngelliWeb 2021). Because of the high frequency of such cases and bans, Engelli Web named the 2021 report "The Year of Damaged Reputation, Honor, and Dignity of High Ranking Public Figures".

Government institutions and decisions are protected by the bans too. For instance, URLs about police brutality and arbitrariness, and institutional corruption are systematically filtered from news websites and social media. The controversial decision of the rector appointment to the Boğaziçi University was also backed by censorship. Any URL or social media content including opposing arguments about this decision was banned or deleted.

According to the Engelli Web report, there are 28.474 URLs that are restricted from access, and 22.941 URLs that are deleted. The newspaper website that is the most URLs are banned from is Hürriyet, it is followed sequentially by Sabah, Cumhuriyet, Sözcü, and T24. It is surprising to see Sabah which is known as being a pro-government newspaper at the high ranks of restricted newspapers. The reason for this could be that the newspapers that are known as opposition friendly are already making self-censorship. Content filtering enables the regime to make strategic censorship. This is a way to escape from the potential backlash and online dissent created by broadband shutdowns or censorship. People who do not come across op-

position articles, often do not realize that there is significant filtering happening in the digital media. Therefore, content-based filtering offers a subtler way to restrict unwanted content.

The backlash created in the digital media after a ban is named as Streisand Effect by Akgül and Kırlıdoğ (2015). Akgül and Kırlıdoğ (2015) focus on broadband domain shutdowns imposed on social media applications like Twitter, and they argue that Streisand Effect happening through the use of circumvention tools. Even though a ban is imposed on Twitter, the users keep going to tweet with the help of circumvention tools, and they criticize the shutdown and the authorities that impose that restriction, and this way the broadband shutdown causes online dissent. Content banning is a way to escape from the Streisand Effect.

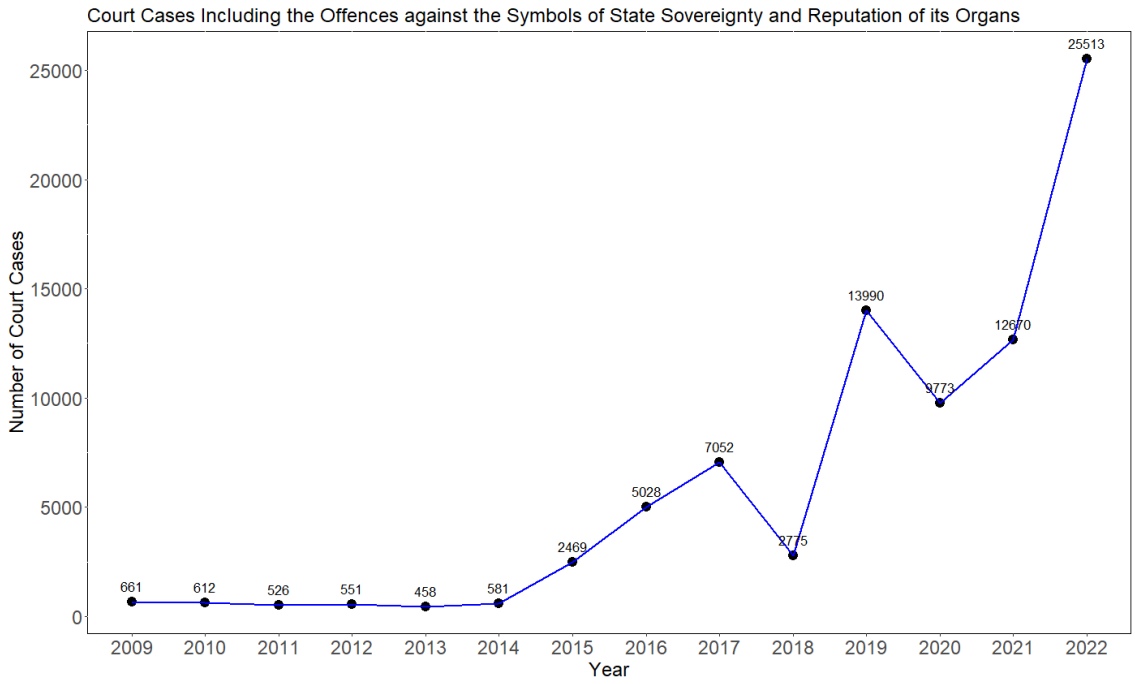
It is hard to realize the censorship because the URLs reporting the bans on certain content are also banned (EngelliWeb 2021). The regime frames censorship as necessary measures to protect national security, social harmony, and family values and this way, legitimizes the content and domain censorships.

4.2.4 Punishments on the Users who Engage in Critical Content

The punishments based on cybercrimes are made mostly by the General Directorate of Security, Cybercrime Department. Among the reasons for arrests done by the Cybercrime Department, the most important one is the violation of the individual rights of the public authorities, or the criticism of the government.

Figure 4.3 shows the number of court cases about the offences against the symbols of state sovereignty and the reputation of its organs. The offences include insulting the president; degrading the symbols of state sovereignty; and degrading the Turkish Nation, the state of the Turkish Republic, and the organs and institutions of the state. The data come from the General Directorate of Criminal Records and Statistics (2023). The court cases show an increasing trend since 2015, and in 2022 there is a big jump. The General Directorate stopped publishing the distribution of the court cases between the three offences under the category of Symbols of State Sovereignty and Reputation of its Organs in 2022, but in 2021, 11.211 out of 12.670 cases were for the charge of insulting the president, and in 2020, 8769 ones of 9773 cases were about insulting the president. Hence, it can be said that Figure 3 is illustrating the trend of the number of cases opened for the offence of insulting the president. The cases are increased nearly ten times since 2015.

Figure 4.3 Number of court cases about offences including insulting the president



Source: General Directorate of Criminal Records and Statistics

Like the other categories of restrictive strategies, the periods of political or national crisis are when the punishments are increasing in terms of sequence. For instance, 3861 individuals were detained and 1734 of them were arrested in the following period of the 2016 failed coup attempt (Topak 2019, 464). A more recent example, during Boğaziçi University protests confronting the rector appointment decision of the government, two students were arrested based on their social media posts (Cumhuriyet 2021; DW 2021). More strikingly, during the days following the Gaziantep-Maraş Earthquakes in 2023, 78 individuals were detained and 20 of them were arrested with the charge of spreading provocative message (Euronews 2023). As I mentioned detailly in the previous section, Cybercrime Department gives a list of articles to point out the legal grounds of the arrestments. This constitutes a clear example of the institutionalization of the restrictive strategies and how the regime built a secure legal field for itself to marginalize the opposition and to protect itself from online criticism and dissemination of anti-regime discourse.

4.3 The Use of Proactive Strategies

In this section, the use of proactive strategies in Turkey will be reviewed based on three categories. The categories are the control, cooptation and manipulation of cyberspace via spreading content in favor of the regime; surveillance to detect the sources of the regime criticism, and fractionalization to create a nationalized cyberspace. In the following sections, I will analyze all of the categories' applications in Turkey.

The most influential technique of proactive strategies is the manipulation of the digital discourse by various tools. The regime's populist discourse enables it to successfully implement manipulation in digital media. Already polarized and mobilized society gives manipulation techniques a prepared ground. The most important characteristic of the Turkish model of proactive control strategies is its subtleness. Although the government benefits from manipulation and digital propaganda, there is not an apparent relationship between the regime and digital media manipulation operations. Unlike restrictive strategies, the government does not fully establish proactive control strategies yet. Therefore, for proactive strategies, there are not as many examples as restrictive strategies but the intentions of the regime towards establishing these strategies are clear. Let's have a look at these strategies one by one.

4.3.1 Control, Cooptation and Manipulation of the Cyber Space

This technique is at the heart of proactive controls. It includes a set of different activities to manipulate digital media and turn it into a propaganda tool. It is hard to achieve for a regime to successfully manipulate the digital discourse because of the importance of organic interactions in digital media. The manipulations are made by using the means of social media, therefore, require base followers which helps the content to reach out a wider audience by sharing and commenting. However, once a regime-friendly discourse becomes one of the trends in social media, it has the potential to become an even more effective propaganda strategy, than those made in the traditional media, especially among young people.

China and Russia are the countries that most openly use manipulation techniques. China has a state department, the Internet Propaganda Office which posts 50 party posts in digital platforms to create a regime-friendly discourse. Russia has a state-funded troll army to achieve a similar goal to China. However, in Turkey, the

manipulation structure is much more subtle. The existence of a regime-friendly troll army, also known as AkTrolls, is among the rumors, but there is no clear evidence proving a funded relationship between the government and AkTrolls. However, there is a campaigned pro-regime discourse in social media that follows a distinctive set of strategies to fight against the regime opposition and portray the success of the regime. Yeşil, Sözeri, and Khazraee point out the change in the online policy after the failed coup attempt in 2016 and add that "coordinated online harassment campaigns by pro-government users against alleged coup planners, Kurdish activists, and government critics in general" as a new trend (Yesil, Sözeri, and Khazraee 2017, 4). Beginning from those years, the pro-government users are actively making regime propaganda.

Bulut and Yörük (2017) make a deep analysis of social media trolls. They emphasize that the aim of the trolls is to "energize the society" and "push users to political debate" through the usage of populist discourse. As a result, digital media is deeply polarized, and energized users are forced to take a stance on the political agenda set by Twitter bots. However, it is hard to remain in the opposition because of the trolls' lynch operations toward the oppositional figures.

Saka (2018) lists the set of strategies used by the trolls. Social lynching, refashioning popular social media trends to spread their content, usage of automated bots to counter anti-AKP discourse, hacking opposition accounts and making them post pro-regime content, and even apologizing for being in the opposition are the strategies used by trolls. In a way, trolls are combatting social media to contribute to the reputation of the regime.

The organizational structure of the troll accounts is very complicated. Saka explains the structure as "AkTrolls function in a decentralized networking pattern, with different nodes finding their own ways to participate in the government's struggle with opponents", and this makes the government harness the results of the troll activities while keeping itself clean and away from the accusations (Saka 2018, 164). The AKP's voluntary organizations can be one of the structures that organize the campaigns. Bulut and Yörük (2017) referred to an article published in Taraf newspaper explaining the organizational structure of the AkTrolls, by Hüseyin Özay, which is restricted from access right now. According to them, Özay is explaining that AkTrolls are recruiting individuals from AKP's youth organization, AKP Gençlik Kolları, and they are paid a minimum of 1000 Turkish liras for their service. Saka (2018) argues that the groups are organized by high-ranking party affiliates and governors, and there are unorganized activities too, willing to contribute to the regime's durability. Loyalty to the regime is a big motivation behind troll activity in Turkey.

The trolls can be used for within-party rivalries too, like the case of purging Ahmet Davutoğlu who is a former prime minister of the AKP government, from AKP, as Saka (2018) explains. Yeşil, Sözeri, and Khazraee point out the same crisis between Erdoğan and Davutoğlu, the case of Pelican Files, where a number of files criticizing Davutoğlu were released by a group of users, who are loyal specifically to Erdoğan, also known as Bosphorus Global. They operated like "fact checking services" against the critical coverage of the AKP government in international media (Yesil, Sözeri, and Khazraee 2017, 23). As mentioned in the previous chapters, Gunitsky (2015) argues that for a successful proactive strategy application, the regime requires a social group that is willing to support the regime. The Turkish case is a good example of the effective use of manipulation, and the loyal supporters of the regime play a crucial role in this success.

4.3.2 Detection of the Sources of Regime Criticism Via Surveillance

The surveillance of the opposition users and the anti-regime sentiment among society is another technique of proactive control strategies. The regime does this via state institutions like National Intelligence Agency (MIT), or in an indirect way using the ISP companies like TTNet. In addition to MIT, General Directorate of Security is also surveilling digital activity and make arrestments based on the social media posts, as discussed in the previous section. The problematic part of the government surveillance is that the boundaries of the institutions are very blurry like they are limitless, they can surveil the accounts anytime without getting a legal permission. For instance, after the failed coup attempt in 2016, the decree law gives permission to BTK to investigate all private accounts of the users.

Several spyware tools make the surveillance possible for the institutions. Phorm, Package Shaper, Remote Control System, Deep Package Inspection system are among the tools that is used to spy on the individual accounts (Yesil, Sözeri, and Khazraee 2017). Not only the departments of security and intelligence but also ISP companies like TürkTelekom use these tools. With these multifaceted surveillance structure, government not only get information about the digital activities, but also establish norms for permissible speech and this way contributes to the expansion of regime's authority by giving the message of "big brother is watching you".

4.3.3 Fractionalization to Create a Nationalized Cyber Space

The last technique of proactive controls is the fractionalization. The fractionalization of the Internet is the result of multiple countries' attempts to create nationalized cyberspaces. The global network is becoming divided into boundaries. The initiator countries of fractionalization are again China and Russia. The Great Firewall of China and Roskommdzor of Russia draws the boundaries of the countries cyberspace by censoring numerous websites. They are so dedicated to keep the national cyberspace free from the unwanted websites that China even launched a DDoS attack to the servers of GitHub and GreatFire.org because they provide circumvention tools to get through the censorship applied by the Chinese government (Sari 2019, 135). Russia is forcing the social media sites to abide by the Russian data storage law. The law enables Russian government to control the Internet traffic of those social media sites (Sari 2019, 136). Similar to those of China and Russa, Sari (2019) offers a national cyber security wall project to protect the cyberspace from foreign attacks, and names it as Seddülbahir. However, following the examples of China and Russia signals that this wall might hurt the Internet freedom of Turkey.

The intentions of Turkish government are in line with the creation of a closed Turkish cyberspace, as the declarations of high-ranking politicians reveal. For instance, İlhan gives an example of such declarations; "in April 2014, newly appointed Minister of Transport, Maritime Affairs, and Communications Lütfi Elvan suggested setting up a national Internet using "ttt" domain instead of the "www", so as to protect Turkey's national security interests" (İlhan 2015, 49). Similarly, Topak claims that the regime wants from social media sites like Twitter, Facebook, and Youtube to establish "local data centers that would fully comply with national laws" (Topak 2019, 464). Yeşil, Sözeri and Khazraee (2017) agree to Topak (2019)'s argument on that and point out the official statements about the need for domestic data collection which would ensure the inspection of those domestic data by the national authorities. All in all, the nationalization of the Turkish cyberspace is not fully established yet, however, there is a high probability that this could be among the future projects of the regime about the Internet controls.

In this chapter, I focused on the examination of restrictive and proactive strategies based on the Turkish example. As a result, found out that the strategies employed by the government has a strong parallelism with the phases of authoritarianisation. As the regime become more powerful by the centralization of the state authority and elimination of the check and balance institutions, it became more institutionalized in the digital space control strategies and consequently increases the repression over digital media. The most important characteristic of the Turkish government in terms

of digital controls is its caution to not to decrease the legitimacy of its rule. Therefore, it prioritizes the institutionalization before censorship and subtleness before manipulation. The combination of the Turkish regime of restrictive and proactive strategies is very intertwined. The space that opened up via restrictive strategies is filled with proactive controls and this way the digital propaganda contributes to the regime durability. The Turkish case of restrictive and proactive control strategies can be summarized by these characteristics.

5. CONCLUSION

The Internet is a powerful new source of information, communication, and media. For regimes with authoritarian tendencies, the Internet has come with its perils and challenges. Being a new platform of engagement among people, the Internet enhanced people's views about democracy and led them to question the existing institutions. This way, the Internet poses a threat to the domination of authoritarian regimes over the media sources, and eventually to their durability. The examples of Arab Spring showed that the Internet can facilitate political mobilization, therefore, gave hope for a democratic future for authoritarian regimes. Nevertheless, authoritarian regimes learned how to control and restrict the Internet, therefore the cyberoptimist expectations were not fulfilled. In this thesis, I focused on the response of the authoritarian regimes to this new means of communication and media. I examined different strategies of digital authoritarianism to control and restrict the Internet. The authoritarian toolkit of Internet controls was examined under two main categories in this thesis, restrictive and proactive strategies. In chapter 2, I reviewed the literature and put forward the theoretical framework. I argued that there is not a clear divide between different regimes as those who use restrictive controls, and those who use proactive controls exclusively, rather regimes use these strategies complementarily and create their own blend of restrictive and proactive strategies. The regimes that have more economic resources and more capacity to use power over their population, either by the penetration into society via clientelism or ideology, are more advantageous to implement proactive strategies. Russia and China can be given as examples of successful implementation of proactive strategies and effective manipulation of digital space. I argued that in order to understand the mixture of the restrictive and proactive strategies better, I focused specifically to hybrid regimes and ask the question of what drives regimes to build their blend of restrictive and proactive strategies. In the theoretical framework chapter, I discussed these main arguments and main questions of the thesis together with a discussion of the existing literature.

In chapter 3, I tested my second argument that in times of crises, regimes have a higher likelihood to employ restrictive strategies. This argument attempts to contribute to the gap in the literature about the decision-making mechanism of authoritarian regimes to choose between different digital repression strategies. Specifically, I focused on the impact of preelection period on the use of restrictive strategies. I moved from general to particular, made two analyses, those of a cross country analysis, and those of a single case analysis. This chapter constitutes the quantitative part of my mixed method thesis.

In chapter 4, I made a detailed case study of Turkey to examine the use of restrictive and proactive strategies. This chapter provides the qualitative part of the thesis. The main aim of the chapter 4 was to understand the current application of restrictive and proactive strategies of AKP regime to control and restrict the Internet. Along with this, I traced the authoritarianisation process of the Turkey in general and made a short review of chronological evolution of digital governance and repression of Turkish government.

Turkey can be counted among the countries that use proactive controls efficiently. Since 2007, Turkey is experiencing authoritarianisation under AKP rule. The populist discourse and clientelist relationships of the AKP government with its supporting group, enable the regime to manipulate the digital discourse with little effort. However, the manipulation of the digital space via proactive strategies is a relatively new approach to controlling the Internet. Digital censorship started around 2007 with a concern for moral values. Since then, the institutional structure has been built to limit cyberspace systematically. The Internet governance infrastructure was built in a way that the regime intervenes in the digital space to protect its durability whenever it deems necessary. Today, in Turkey restrictive and proactive strategies are used complementarily. With restrictive strategies, the regime represses opposition voices, cleans the digital space of any critical content, and prepares the ground for manipulation. With proactive strategies, it surveils the citizen preferences and opposition tendencies, set the digital discourse via trend topics, energizes the society, and then channels the debates towards populist rhetoric. This way, it uses digital media as an effective propaganda tool.

The Internet can enable authoritarian rule to penetrate into society in a deeper way than at any other time and this way makes it stronger, or it can open the way to liberalization by facilitating social mobilization. The realization of either of these two possibilities depends on the regime's ability to control the Internet. In this thesis, I analyzed how authoritarian regimes contain the democratizing power of the Internet, and how they learn new ways of turning it into a new tool for their

durability. I also explored varied strategies authoritarian regimes employ to prevent opposition actors from using the Internet to undermine the regime. I provided a new categorization of control and restriction strategies of authoritarian regimes and examine it on hybrid regimes. Hybrid regimes are at the center of the spectrum of democracies and autocracies, therefore, their strategies to cope with the Internet include a more diverse set of strategies. This stems from the level of power that they can apply to society. They cannot afford to employ full-fledged Internet shutdowns or implement fully controlled, national substitutes of cyberspace, unlike closed autocracies, because of the threat of a possible backlash grow after such measures. On the other side, cyberspace free from censorship and restrictions is not a realistic option either, because of the positive impact of the Internet on citizens' demand for democracy. Therefore, the adaptation of hybrid regimes to the new digital age is a more challenging and interesting story than those of democracies and autocracies.

Literature shows that the regime's attitude towards the Internet plays a decisive role in the discussion of whether it initiates a democratization movement or not. Today, most of the regimes which have strict policies to keep the media under control, are learning how to establish control over digital media. The restrictive and proactive strategies provided in this thesis aim to categorize the new way of Internet controls. Considering the different approaches of these categories, this thesis claims that there are different times and occasions for both restrictive and proactive strategies, and regimes use both of these strategies when they are necessary. Restrictive ones are more directed towards the elimination of unwanted content immediately, therefore they are used as swift solutions in times of crisis. Proactive strategies require more time but aim to establish a sanitized digital environment through manipulation and nationalization. They are like long-term investments to tame the Internet, therefore used by the regime as a project that is implemented step by step. This increasing diversification is an indication of how cyberspace too is getting more and more authoritarian, as the regimes learn new ways of establishing their power over it.

The contribution of this thesis is threefold. Firstly, it introduces a new categorization of the strategies to control and restrict the Internet. The strategies to control and restrict the Internet are grouped as restrictive and proactive strategies in this study. The former includes the techniques with the aim of preventing unwanted information immediately, and the latter includes the ones with the aim of manipulation of cyberspace and benefitting it. The restrictive strategies are more straightforward, they are like the first solution that can come to mind. To remove any regime-critical activity from cyberspace, restrictive strategies offer a set of strategies including shutting down the Internet flow, cutting access to social media sites, banning the URLs of critical sites, or deleting harmful posts. The thought behind the restrictive strate-

gies is to prevent unwanted content's dissemination via limitations on access. In the proactive strategies, on the other hand, the Internet is tamed so that it no longer poses a threat to the regime, instead it is turned into a new channel for propaganda. The techniques in proactive strategies adopt the rules of the digital age, therefore, they aim to manipulate the digital discourse in a way that favors the regime while using the Internet as a source of information about citizen preferences and oppositional tendencies. In this thesis, the different measures to control and restrict the Internet are presented under the roofs of restrictive and proactive strategies.

As the second contribution, this thesis refers to the gap in the literature concerning the initial mechanism behind the control and restriction strategies. After presenting the possible factors that can be influential to determine the behavior of authoritarian regimes to control the Internet, the relationship between the elections and restrictive strategies is tested. The election period is marked as the time span when harsher measures are more likely to be used by the regime (Crete-Nishihata, Deibert, and Senft 2013; Freyburg and Garbe 2018; Gohdes 2020; Maréchal 2017; Miller 2022; Roberts 2018). Based on this argument, this thesis makes two analyses. One of the analyses has a cross-country design and the other has a single-country design. The samples are picked from the hybrid regimes in both analyses because hybrid regimes show the biggest variation due to the limitations coming from not being a completely closed autocracy and a total democracy. In both analyses, the question of whether elections have an impact on the frequency of restrictive strategies is studied. The results support the main argument that the regimes have a higher likelihood of implementing restrictions on the digital space during the pre-election period. The pre-election period is chosen as the period under study because of the assumption that this is the period when the regime feels the most pressure about its future, therefore has the highest probability to employ restrictions. However, the analyses have some limitations. In both analyses, the measure for the restrictive strategies is the restrictions on political criticism websites. The other techniques of restrictive strategies were not controlled. The generalizability of the cross-country analysis is questionable because, in the Callaway Sant'Anna estimation, the results are not significant. In the Turkey analysis, only one election was taken into account, whether the hypothesis would hold for the 2018 elections is a question mark for instance. However, taking the limitations aside, we can say that elections are among the fragile periods for the regime, therefore it has an impact on the regime's behavior towards the Internet. Looking at the usage of proactive strategies during elections in future research might be complementary to this study.

The third contribution of this study is that it offers a detailed case study of Turkey, in terms of the history and current state of Internet governance. Turkey's Internet

governance and restrictions were analyzed based on the categorization of restrictive and proactive strategies. Hence, a descriptive analysis of electoral authoritarianism is the third contribution of this thesis. Turkey is a country that is experiencing democratic backsliding under a populist government. The elections are still competitive, even though they are held in unequal conditions for the opposition and incumbent party. The popularity of the government in the eyes of the supporting voter is very high. One of the determining factors of the strategy selection of the regime to cope with the Internet is the regime's reputation as being the protector of the nation, protector of national values, and social cohesion. To maintain this reputation, the Turkish government built a big infrastructure of Internet governance institutions which help them to legitimize the digital censorship practices, prosecutions due to social media activity, and attempts to create a closed Internet. Among the most frequent excuses for those control and restrictions, the protection of society from disinformation and harmful activities like gambling, pornography, or drug use; protection of individual rights and dignity; and protection of the Turkish state and its symbols can be counted. However, the practices of Internet restrictions signal that those steps are taken first and foremost to contribute to the regime's durability. Other than the measures which are taken openly and legitimately, there are a set of clandestine strategies. The most important one is the manipulation of the digital discourse using troll armies. The connection of these troll accounts with the regime is nothing more than a loyal support and fondness to the incumbent, and unorganized guidance of the party elite. If there is a funded relationship between the trolls and the regime, it is extremely subtle and secret, it is not revealed yet. Based on these findings, this thesis argues that the Turkish style of the Internet has been built on three main pillars. Firstly, there is a high level of institutionalization in Internet controls. Second, these controls are supported and legitimized by populist discourse. Lastly, the controls include a concern not to damage the popularity and legitimacy of the regime therefore they are made very subtly and indirectly.

This is a growing area of research focusing on rapidly changing and adapting strategies. Future research might study the variation among authoritarian regimes in their special mixture of restrictive and proactive strategies. New case studies of these said categories would help to further understand authoritarian regimes' steps to control the digital space. Moreover, the analysis of Internet controls during the elections should be expanded. How regimes employ proactive and restrictive strategies complementarily in times of crisis is another interesting question that can be studied in the future. The activities of bot accounts and usage of artificial intelligence to manipulate the digital discourse would be another interesting issue for further research too.

BIBLIOGRAPHY

Akdeniz, Yaman, and Kerem Altıparmak. 2018. *Turkey: Freedom of expression in jeopardy.* Violations of the Rights of Authors, Publishers and Academics Under the State of Emergency.

Akgül, Mustafa, and Melih Kırlıdoğ. 2015. "Internet censorship in Turkey." *Internet Policy Review* 4(June).

Bailard, Catie Snow. 2012. "Testing the Internet's Effect on Democratic Satisfaction: A Multi-Methodological, Cross-National Approach." *Journal of Information Technology & Politics* 9(April): 185–204.

Boas, Taylor C. 2004. "Weaving the Authoritarian Web." *Current History* 103(December): 438–443.

Boo, Jeremy, and Dan Slater. 2021. "The Digitization Of Dictatorship: Early Lessons From A Growing Literature.".

Bulut, Ergin, and E. Yörük. 2017. "Mediatized Populisms| Digital Populism: Trolls and Political Polarization of Twitter in Turkey." *International Journal of Communication* (October).

Callaway, Brantly, and Pedro H. C. Sant'Anna. 2021. "Difference-in-Differences with multiple time periods." *Journal of Econometrics* 225(December): 200–230.

Carothers, Thomas. 2002. "The End of the Transition Paradigm." *Journal of Democracy* 13(January): 5–21.

Clarke, Killian, and Korhan Kocak. 2020. "Launching Revolution: Social Media and the Egyptian Uprising's First Movers." *British Journal of Political Science* 50(July): 1025–1045.

Collier, David, and Steven Levitsky. 1997. "Democracy with Adjectives: Conceptual Innovation in Comparative Research." *World Politics* 49(April): 430–451.

Crete-Nishihata, Masashi, Ronald J. Deibert, and Adam Senft. 2013. "Not by Technical Means Alone: The Multidisciplinary Challenge of Studying Information Controls.".

Cumhuriyet. 2021. "Boğaziçi Üniversitesi öğrencilerinin tutuklanması için suç vasfı değiştirildi.".

Davenport, Christian. 2007. "State Repression and Political Order." *Annual Review of Political Science* 10(1): 1–23.

Deibert, Ron. 2015. "Cyberspace Under Siege." *Journal of Democracy* 26(July): 64–78.

Demiralp, Seda, and Evren Balta. 2021. "Defeating Populists: The Case of 2019 Istanbul Elections." *South European Society and Politics* 26(January): 1–26.

Diamond, Larry. 2002. "Elections Without Democracy: Thinking About Hybrid Regimes." *Journal of Democracy* 13(2): 21–35.

DW. 2021. "Boğaziçi eylemlerinde sosyal medya tutuklamaları.".

Earl, Jennifer. 2011. "Political Repression: Iron Fists, Velvet Gloves, and Diffuse Control." *Annual Review of Sociology* 37(1): 261–284.

Earl, Jennifer. 2022. "Repression and Social Movements." In *The Wiley-Blackwell Encyclopedia of Social and Political Movements*. John Wiley & Sons, Ltd pp. 1–7.

EGM, Siber Suçlarla Mücadele Daire Başkanlığı. 2023. "Sıkça Sorulan Sorular.".

Eldem, Tuba. 2020. "The Governance of Turkey's Cyberspace: Between Cyber Security and Information Security." *International Journal of Public Administration* 43(April): 452–465.

EngelliWeb. 2021. EngelliWeb 2021: Üst Düzey Kamu Şahsiyetlerinin İncinen İtibar, Onur ve Haysiyet Yılı. Technical report İfade Özgürlüğü Derneği.

Esen, Berk, and Sebnem Gumuscu. 2016. "Rising competitive authoritarianism in Turkey." *Third World Quarterly* 37(September): 1581–1606.

Esen, Berk, and Şebnem Gümüşçü. 2017. "A Small Yes for Presidentialism: The Turkish Constitutional Referendum of April 2017." *South European Society and Politics* 22(July): 303–326.

Euronews. 2023. "Sosyal medyada deprem paylaşımlarına 78 gözaltı 20 tutuklama.".

FreedomHouse. 2022. "Freedom on the Net Report 2022: Countering an Authoritarian Overhaul of the Internet.".

FreedomHouse. 2023. "Freedom on the Net All Data: 2011-2022.".

Freyburg, Tina, and Lisa Garbe. 2018. "Authoritarian Practices in the Digital Age| Blocking the Bottleneck: Internet Shutdowns and Ownership at Election Times in Sub-Saharan Africa." *International Journal of Communication* 12(September): 21.

Gerschewski, Johannes. 2013. "The three pillars of stability: legitimation, repression, and co-optation in autocratic regimes." *Democratization* 20(January): 13–38.

Gohdes, Anita R. 2015. "Pulling the plug: Network disruptions and violence in civil conflict." *Journal of Peace Research* 52(May): 352–367.

Gohdes, Anita R. 2020. "Repression Technology: Internet Accessibility and State Violence." *American Journal of Political Science* 64(3): 488–503.

Groshek, Jacob. 2009. "The Democratic Effects of the Internet, 1994—2003: A Cross-National Inquiry of 152 Countries." *International Communication Gazette* 71(April): 115–136.

Gunitsky, Seva. 2015. "Corrupting the Cyber-Commons: Social Media as a Tool of Autocratic Stability." *Perspectives on Politics* 13(March): 42–54.

Guriev, Sergei, and Daniel Treisman. 2019. "Informational Autocrats." *Journal of Economic Perspectives* 33(November): 100–127.

Hassanpour, Navid. 2014. "Media Disruption and Revolutionary Unrest: Evidence From Mubarak's Quasi-Experiment." *Political Communication* 31(January): 1–24.

King, Gary, Jennifer Pan, and Margaret E. Roberts. 2017. "How the Chinese Government Fabricates Social Media Posts for Strategic Distraction, not Engaged Argument." *American Political Science Review* 111(3): 484–501.

Kubicek, Paul. 2020. "Faulty Assumptions about Democratization in Turkey." *Middle East Critique* 29(July): 245–257.

Levitsky, Steven, and Lucan Way. 2002. "Elections Without Democracy: The Rise of Competitive Authoritarianism." *Journal of Democracy* 13(April): 51–65.

Levitsky, Steven, and Lucan Way. 2020. "The New Competitive Authoritarianism." *Journal of Democracy* 31(January): 51–65.

Maréchal, Nathalie. 2017. "Networked Authoritarianism and the Geopolitics of Information: Understanding Russian Internet Policy." *Media and Communication* 5(March): 29–41.

Medyascope, Turkey. 2022. "BTK-gate: Internet activity, identity, and personal data of all users in Turkey has been collected by BTK for the past year and a half.".

Merkel, Wolfgang. 2004. "Embedded and defective democracies." *Democratization* 11(January): 33–58.

Miller, Andrew Cesare. 2022. "#DictatorErdogan: How Social Media Bans Trigger Backlash." *Political Communication* 39(November): 801–825.

NetBlocks. 2020. "Social media blocked in Turkey as Idlib military crisis escalates.".

NetBlocks. 2022. "Social media restricted in Turkey after blast in Taksim, Istanbul.".

NetBlocks. 2023. "Twitter restricted in Turkey in aftermath of earthquake.".

Nisbet, Erik, Aysenur Dal, Golnoosh Behrouzian, and Ali Çarkoglu. 2015. "Benchmarking Demand: Turkey's Contested Internet." *Internet Policy Observatory* (October).

Nisbet, Erik C., Elizabeth Stoycheff, and Katy E. Pearce. 2012. "Internet Use and Democratic Demands: A Multinational, Multilevel Model of Internet Use and Citizen Attitudes About Democracy." *Journal of Communication* 62(2): 249–265.

O'Donell, Guillermo A. 1994. "Delegative Democracy." *Journal of Democracy* 5(1): 55–69.

OONI. 2023. "Open Observatory of Network Interference.".

Pan, Jennifer, and Alexandra A. Siegel. 2020. "How Saudi Crackdowns Fail to Silence Online Dissent." *American Political Science Review* 114(February): 109–125.

Roberts, Margaret E. 2014. Fear or Friction ? How Censorship Slows the Spread of Information in the Digital Age.

Roberts, Margaret E. 2018. *Censored: Distraction and Diversion Inside China's Great Firewall*. Illustrated edition ed. Princeton, New Jersey: Princeton University Press.

Robertson, Graeme B. 2010. *The Politics of Protest in Hybrid Regimes: Managing Dissent in Post-Communist Russia*. Illustrated edition ed. New York: Cambridge University Press.

Rojas Navarro, Zaira. 2023. "Free Speech: A Right in Crisis as Turkish Parliament Passes New "Disinformation" Bill." *CICLR Online* (January).

Ruijgrok, Kris. 2017. "From the web to the streets: internet and protests under authoritarian regimes." *Democratization* 24(April): 498–520.

Ruijgrok, Kris. 2021. "Illusion of control: how internet use generates anti-regime sentiment in authoritarian regimes." *Contemporary Politics* 27(May): 247–270.

Rød, Espen Geelmuyden, and Nils B Weidmann. 2015. "Empowering activists or autocrats? The Internet in authoritarian regimes." *Journal of Peace Research* 52(May): 338–351.

Saka, Erkan. 2018. "Social Media in Turkey as a Space for Political Battles: AK-Trolls and other Politically motivated trolling." *Middle East Critique* 27(April): 161–177.

Sari, Arif. 2019. "Turkish national cyber-firewall to mitigate countrywide cyber-attacks." *Computers & Electrical Engineering* 73(January): 128–144.

Schedler, Andreas. 2015. *The Politics of Uncertainty: Sustaining and Subverting Electoral Authoritarianism*. First edition ed. Oxford: Oxford University Press.

Schlumberger, Oliver, Mirjam Edel, Ahmed Maati, and Koray Saglam. 2023. "How Authoritarianism Transforms: A Framework for the Study of Digital Dictatorship." *Government and Opposition* (July): 1–23.

Stoycheff, Elizabeth, and Erik C. Nisbet. 2014. "What's the Bandwidth for Democracy? Deconstructing Internet Penetration and Citizen Attitudes About Governance." *Political Communication* 31(October): 628–646.

Tang, Min, and Narisong Huhe. 2014. "Alternative framing: The effect of the Internet on political support in authoritarian China." *International Political Science Review* 35(November): 559–576.

Topak, Özgün. 2019. "The authoritarian surveillant assemblage: Authoritarian state surveillance in Turkey." *Security Dialogue* 50(October): 454–472.

Tufekci, Zeynep. 2014. "Engineering the public: Big data, surveillance and computational politics." *First Monday* (July).

TurkeyBlocks. 2016*a*. "Social media shutdowns in Turkey after ISIS releases soldier video.".

TurkeyBlocks. 2016*b*. "Social media slowdown detected in Turkey after assassination of Russian ambassador.".

V-Dem. 2023. "V-Dem V13 Full + Others.".

ve İstatistik Genel Müdürlüğü, Adli Sicil. 2023. "Adalet İstatistikleri 2009-2022.".

Ververis, Vasilis, Sophia Marguel, and Benjamin Fabian. 2020. "Cross-Country Comparison of Internet Censorship: A Literature Review." *Policy & Internet* 12(December): 450–473.

WorldBank. 2023. "World Development Indicators.".

Yanatma, Servet. 2021. "Advertising and Media Capture in Turkey: How Does the State Emerge as the Largest Advertiser with the Rise of Competitive Authoritarianism?" *The International Journal of Press/Politics* 26(October): 797–821.

Yesil, Bilge. 2014. "Press Censorship in Turkey: Networks of State Power, Commercial Pressures, and Self-Censorship." *Communication, Culture and Critique* 7(June): 154–173.

Yesil, Bilge, and Efe Sozeri. 2017. "Online Surveillance in Turkey: Legislation, Technology and Citizen Involvement." *Surveillance & Society* 15(August): 543–549.

Yesil, Bilge, Efe Sözeri, and Emad Khazraee. 2017. "Turkey's Internet Policy After the Coup Attempt: The Emergence of a Distributed Network of Online Suppression and Surveillance." (February).

You, Yu, and Zhengxu Wang. 2020. "The Internet, political trust, and regime types: a cross-national and multilevel analysis." *Japanese Journal of Political Science* 21(June): 68–89.

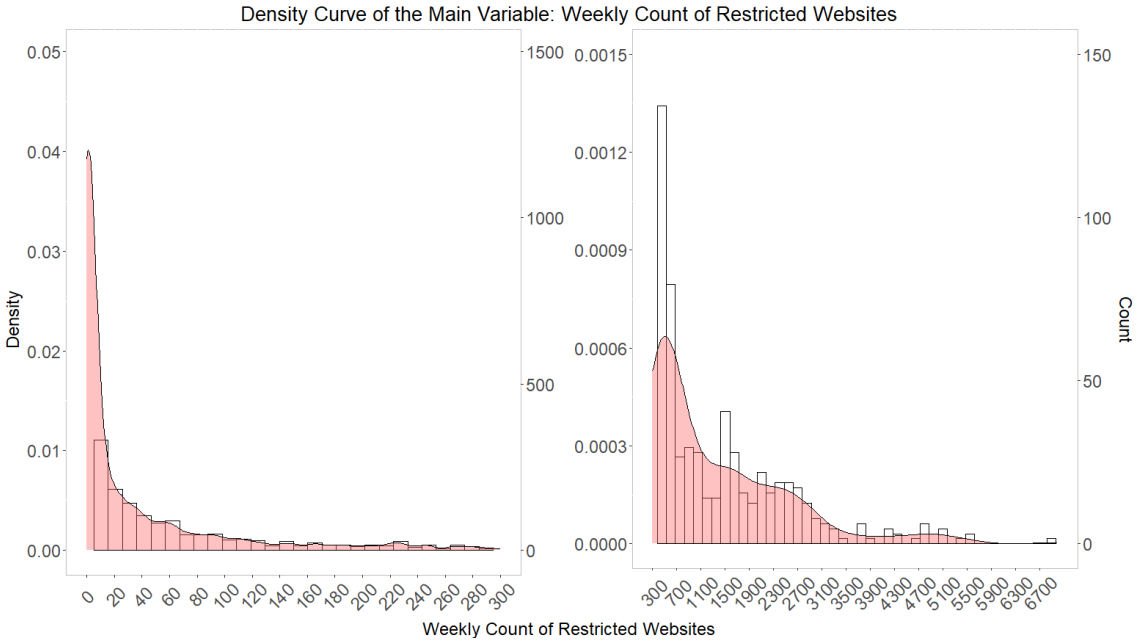
Yıldırım, Kerem, Lemi Baruh, and Ali Çarkoğlu. 2021. "Dynamics of Campaign Reporting and Press-Party Parallelism: Rise of Competitive Authoritarianism and the Media System in Turkey." *Political Communication* 38(May): 326–349.

Çarkoğlu, Ali, and Simge Andı. 2021. "Support for Censorship of Online and Offline Media: The Partisan Divide in Turkey." *The International Journal of Press/Politics* 26(July): 568–586.

İlhan, Ebru. 2015. "Plugged Out? Turkey's Internet Politics and Business." *Turkish Policy Quarterly Winter* 2015: 47–59.

APPENDIX A

Density Curve and Histogram of the Main Dependent Variable in Cross Country Analysis



Density Curve and Histogram of the Main Dependent Variable in Turkey Case Study