UNIVERSITY OF TARTU
Faculty of Social Sciences
Johan Skytte Institute of Political Studies

Mariia Maksimova

CIVIL SOCIETY AGAINST STATELY CYBERCONTROL: THE CASE OF RUSSIA

MA thesis

Supervisor: Andrey Makarychev, PhD
Co-supervisor: Catarina Fróis, PhD

Tartu 2022

AUTHOR'S DECLARATION

I have written this Master's thesis independently. All viewpoints of other authors, literary sources and data from elsewhere used for writing this paper have been referenced.

.....

/signature of author/

The defence will take place on ..... /date/

at ..... /time/..... /address/

in auditorium number ...../number/

Opponent ..... /name / (..... /academic degree/), ... /position/

Word count: 25,566

ACKNOWLEDGEMENTS

First and foremost, I am incredibly grateful to my supervisor Andrey Makarychev for his support and feedback. I am also thankful to my co-supervisor, Catarina Fróis, for her meaningful contribution throughout the writing process. As I started writing this thesis in Estonia, continued in Portugal and finished in Estonia, their backing helped me progress with the study while enriching my thesis with the perspective gained in each country.

Further, I want to express my gratitude to all people who partook in this investigation. Since Spring 2021, I have interviewed ten people who found time in their busy schedules to talk with me. I am thankful for their contributions, which became the basis for this thesis. I am deeply indebted to the interviewees who helped me find participants for focus groups. Thank you for your trust!

I am grateful to the focus group participants. From January to February 2022, I have led focus groups with 52 activists and volunteers. Despite all the risks, they have agreed to share their experiences with me. I cannot emphasise how thankful I am for their contribution. This thesis would not be possible without your enormous help!

I would also like to thank the University of Tartu (Estonia) and ISCTE – University Institute of Lisbon (Portugal), which provided materials for this project through courses I took or their extensive libraries. Mainly, I want to thank Thomas Linsenmaier, Stefano Braghiroli, Clara Carvalho, and Louis Wierenga for their courses that have helped me shape this study. Also, an additional thank you to Louis Wierenga for finding time to advise me on my thesis outside of the classroom.

Moreover, my appreciation is to OVD-Info, one of the organizations I focused on and a starting point for my empirical research. I am grateful to coordinators who not only helped me with recruiting but also shared writing tips on how to formulate the call for volunteers. My special thanks are to Artem, who supported me throughout the year by finding interviewees and focus group participants!

Finally, I am thankful to everyone who supported me during this research: my mother, my friends – and, notably, Anna, who was one of the first people to read the text and give me feedback.

Thank you! Спасибо! Obrigada! Aitäh! Danke!

ABSTRACT

This thesis investigates the Russian liberal civil society – a part of the Russian civil society that strives for a domestic socio-political change, democratization and liberalization of the current order – in cyberspace, where it must battle growing pressure from the state, seeking to control all dissent. I hypothesize that in its reaction to the stately cybercontrol, the liberal civil society develops cybersecurity practices that make it more potent and allow for a counteraction against the state. Hence, I use in-depth expert interviews and focus groups with representatives of the liberal civil society to collect the data for qualitative content analysis to analyze the research question. As a result, the thesis discovers a wide range of societal cybersecurity practices beyond defensive actions to include resistant components. Hence, I conclude that the Russian liberal civil society, although experiencing significant pressure that hinders its efficiency, can fight off the state's attacks on it and continues to develop itself. The results of this study could be of value for viewing Russia not as a singular actor but as a context in which liberal powers are struggling against the authoritarian regime.

Keywords: Russia, civil society, cybersecurity, cybercontrol

TABLE OF CONTENTS

INTRODUCTION

In today's world, technology and the Internet have long become vital parts of the socio-political life of the international community and nation-states. Moreover, states and their citizens depend on the cybersphere in their daily lives (Bruno, 2012, p. 343). Naturally, cybersecurity is crucial for them to protect their data and infrastructure. An increasingly growing body of research on the topic, mainly focusing on the state's cybersecurity (Shackelford et al., 2017), proves this point. Nevertheless, the cybersecurity for other actors is significantly understudied. It is especially true for society, often viewed as indistinguishable from the nation-state with national cybersecurity protecting its interests. However, the security of society is crucial precisely because the goals of the state might go contrary to the people's interests. Most importantly, the security of the society might suffer from the state to which it belongs.

Most notably, the limitation of the body of literature is considerable for the countries in which the state is a threat to its people (here and further, the country encompasses the state and the society as actors). Whereas Western researchers address cybersecurity from corporations (Zuboff, 2019) that "harvest data" (Finnemore, 2018, p. 458) for revenues more often, they overlook the non-Western countries with illiberal regimes. Nevertheless, with the latter's governments almost entirely controlling the offline world, cyberspace is what remains for the societies to organize their resistance. In other words, social movements and NGOs use the Internet to avoid governmental superintendence. For instance, Russia is a country where a liberal civil society, consisting of NGOs and social movements aiming for regime change, is under constant online and offline pressure. The state uses an 'anti-extremist' and 'foreign agents' legislature to shut down their websites and social media accounts (Daucé, 2020). For instance, on December 25, 2021, the Russian government blocked the website of the independent human rights media project OVD-Info. However, there is little academic research done on the topic.

Consequently, this thesis focuses on the cybersecurity of liberal civil society, utilizing the case of Russia. With the state increasing pressure and shifting to a totalitarian regime, it is crucial to investigate how the surviving liberal civil society deals with it while having significantly less power and resources than the state. I attempt to provide a better understanding of the situation inside Russia. With existing research primarily focused on cybersecurity *from* Russia or for Russia *as a state*, I want to look deeper into

under-researched societal cybersecurity, with only a handful of academic articles considering the issue (Burton and Lain, 2020, p. 452). This perspective allows for a deeper understanding of the Russian domestic context, which affects Russia from the inside and the country's international policies. I believe that despite the Russian liberal civil society often being considered weak and overpowered by the state, it continues to exist and resist, making it an exciting topic for research. Most importantly, unlike other illiberal and non-democratic states, e.g., China, the Russian state struggles to control cyberspace entirely, leading to it being a territory of relative freedom for the liberal civil society. As a result, societal cybersecurity in Russia is an academically valuable case.

This study aims to understand how Russian liberal civil society responds to the pressure from the state in cyberspace. I seek to realize whether it translates into cybersecurity practices strengthening the community and helping it resist the state, or society becomes even weaker and unable to resist it, fighting only for survival or 'escape' from the state. However, due to possible biases, including my political position – which corresponds with the liberal position held by the study participants – the thesis aims for exploration rather than proof of a specific standpoint to avoid favouring a particular view. Further, although the thesis intends to explore the responses of the Russian liberal civil society to governmental pressure in cyberspace, it does not seek to resolve the insecurities suffered by the former.

Due to the complexity of Russian civil society, which consists of various actors with distinct aims, it is crucial to limit the scope of the study to a more narrow area. Hence, I intend to focus on a small portion of the Russian civil society – liberal civil society. It represents the society but consists of entities active in the socio-political sphere, suffering most pressure from the state due to the latter monopolizing the rights of political participation in Russia. Further, a liberal civil society adopts liberalism from adherence to procedural liberalism rather than a political stance. Consequently, the scope encompasses liberal actors, i.e., NGOs, and social movements, aiming for the democratization of Russia. As a result, the civil society in this thesis scaled down to its liberal subgroup – liberal civil society.

At the same time, when considering liberalism in the context of the illiberal country, the question arises of whether, in such conditions, liberal civil society might exist. I acknowledge that in a country like Russia, the survival and promotion of the socio-

politically active groups are hindered by the state's counteraction. However, the liberal civil society fights against the order, which negates its existence. Its struggle for survival might come before fighting for a socio-political change. Nevertheless, liberalism makes the former necessary but insufficient for liberal civil society, with the latter being crucial for long-term existence and development. Moreover, practices of survival that result in 'escape' cannot be entirely liberal as they do not lead to more freedom, e.g., using cyberspace for 'virtual politics' without a significant impact on real politics. On the contrary, I view the liberal component as a driver for change. As a result, I seek to highlight practices beyond mere survival and 'escape' from stately control, which allow liberal civil society to fight back.

The study considers the offline and online effects of cyberspace as "an evolving, loosely bounded and interconnected information environment" (Ormrod and Turnbull, 2016, 283). In other words, although this thesis focuses on cybersecurity, it also accounts for issues outside virtual reality as cyberspace includes physical elements. Furthermore, I consider only threats from the state, disregarding other potential actors being dangerous to liberal civil society, e.g., technological corporations. As a result, the study's scope includes liberal civil society actors active in cyberspace with the state as the source of insecurity. Hence, the research question of the current thesis is:

How does the Russian liberal civil society react to stately cybercontrol?

The research question focuses on liberal civil society and its practices rather than the state. Even though the thesis includes an overview of the state policies, I primarily concentrate on the societal response. Furthermore, the study's main argument is that this reaction is non-linear, meaning that the pressure from the state leads to an evolution of societal cybersecurity practices. In other words, while cybercontrol works against society (e.g., shutting down websites of societal organizations stops them from functioning efficiently and hinders access to them, especially for new users), it also leads to the development of new instruments and tools of resistance. As a result, the primary hypothesis of the study is:

H1: The more cybercontrol the state exerts, the less cybersecure the liberal civil society becomes, but the more societal cybersecurity practices the liberal civil society develops, enhancing itself.

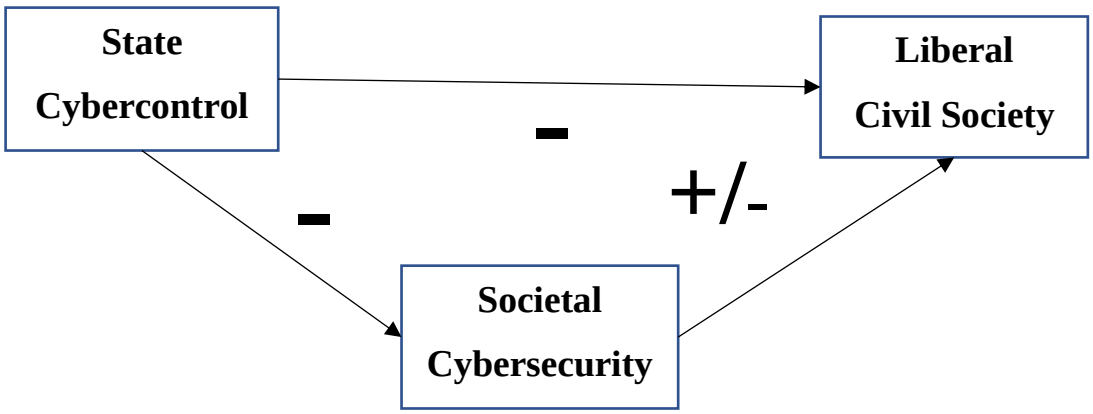

Figure 1. Arrow diagram for the research hypothesis

By the hypothesis, the independent variable (cybercontrol) impacts the liberal civil society in two ways: directly with adverse effects and indirectly through the practices of societal cybersecurity with mixed – but potentially resistant – outcomes (see Figure 1). I expect the latter to be through technological (e.g., VPN) or non-technological (e.g., trust networks, self-censorship) means. In other words, societal cybersecurity might still lead to non-resistance and compliance, which I consider a negative outcome. For instance, self-censorship helps avoid repercussions from the state but hinders freedom of speech. However, this study expects societal cybersecurity to enhance the resistance of liberal civil society, which I consider a positive outcome. As a result, the thesis hypothesises that cybercontrol triggers improvement of the societal cybersecurity practices, making the liberal civil society more resistant.

In this thesis, I empirically analyze the Russian case and compile the results to prove the study's primary hypothesis. First, I conducted a literature review on the research topic to provide a theoretical background. Second, I studied the existing research about Russia on the state actions in cyberspace and the societal landscape. The third task was to outline the research methodology following the study's theoretical framework. Hence, I determined the specific methods and planned for their application. Specifically, I used in-depth interviews and focus groups for the empirical part of the study. To do so, I compiled a list of liberal civil society organizations and their representatives, highlighting NGOs with a network of volunteers to conduct the focus groups.

The fifth step of the research included fieldwork, interviewing the study participants selected at the previous stage. This step also consisted of recruiting interview and focus group participants; second, contacting them and arranging meetings; third,

conducting the interview or focus group; and fourth, arranging transcripts. This stage was allocated the most time to account for possible issues with respondents' availability. Next, I analyzed the data acquired at the preceding stage and compiled the research findings to answer the research question and address the primary hypothesis. Finally, I provide a textual description of all the steps in this thesis. All in all, these research tasks outline all the necessary steps done to accomplish this thesis.

Furthermore, the thesis utilized a qualitative interpretive methodology. I have conducted in-depth expert interviews with the representatives of the major socio-political NGOs and social movements belonging to the Russian liberal civil society. Further, I did focus groups with non-experts in liberal civil society – volunteers who represent the latter but might not possess professional expertise and significant political pressure experience. The data obtained from these sources then were analyzed using qualitative content analysis (QCA) with a code system based on the developed theoretical framework. The study's methodology is addressed more in-depth in the third chapter of the current thesis.

As a result, reflecting the research tasks, the thesis is arranged as follows: first, I provide an overview of the conceptual framework for the research problem by discussing where (cyberspace), what (cybercontrol) and against whom (liberal civil society) of the research question based on the existing body of the literature. The second chapter focuses on the Russian context by giving an account of the situation with cybercontrol in the country and, second, overviewing the specifics of the Russian liberal civil society. The third chapter focuses on the study's methodology by discussing the case, research design and methods of data collection and analysis. Chapter 4 presents the empirical findings of the thesis. Finally, the study concludes with a discussion of the results and possible future directions of the research and its practical application.

1. CYBERCONTROL AND CIVIL SOCIETY

In this chapter, I establish a theoretical framework for the research problem. I start with locating the issue in a specific space – cyberspace – and proceed with actors: the state and the civil society. I define cybercontrol, civil society and societal cybersecurity before proceeding with the Russian context in Chapter 2.

1.1. Cyberspace as a Panopticon

First, I want to establish what 'cyber' is and how it is distinct from 'digital' and 'online'. According to the Merriam-Webster dictionary, 'digital'[1] relates to "devices constructed or working by the methods or principles of electronics" and data. At the same time, 'cyber'[2] involves "computers or computer networks (such as the Internet)". Hence, my preference for the latter term lies in its communication capabilities, as 'digital' includes any electronics without underlying connectivity. Further, 'cyber' also encompasses 'online' and 'offline' as it deals with data, virtual networks, physical hardware and people. As a result, this thesis employs 'cyber' over 'digital' as it includes both offline and online worlds in their capacity for communication networks.

Hence, cyberspace exists physically and non-physically. In other words, it includes hardware, software, data, and users (Ormrod and Turnbull, 2016, pp. 280-3). Notably, software and data are virtual, having no physical manifestation, whereas hardware and users are a part of physical reality. Furthermore, cyberspace is a global environment that includes the Internet, communication networks, and embedded systems (Deibert, 2018, p. 532), deeply interconnected with the 'real' world. As a result, cyberspace goes beyond the Internet by being intrinsically linked to the socio-political reality, including technological networks like surveillance cameras (Weller, 2012, p. 59), enhanced by facial recognition online and offline (Lyon, 2018, pp. 87-8).

Nevertheless, cyberspace does not mirror the borders of the natural world, albeit to a degree. It is loosely bounded (Ormrod and Turnbull, 2016, pp. 280-1), transcending the borders of the nation-states and simultaneously depending on them (Schou and Hjelholt, 2019, p. 441): domestic laws and policies impact hardware and users. At the same time, cyberspace's borders are not strictly defined, which hinders the laws' application. Although some boundaries enclosing it exist (Bogard, 2012, p. 31), they

[1] Retrieved March 28, 2022, from https://www.merriam-webster.com/dictionary/digital
[2] Retrieved March 28, 2022, from https://www.merriam-webster.com/dictionary/cyber

overlap (Lambach, 2020, p. 489) and constantly shift (Schou and Hjelholt, 2019, p. 451). For instance, borders can be defined by linguistic rather than geographic proximity, e.g., the Donbas sector of the Internet has shifted towards Russian rather than Ukrainian cyberspace since 2014 (Limonier et al., 2021). Hence, cyberspace is not a sum of separate national spaces (Balzacq and Dunn Cavelty, 2016, p. 177) but a fragmented and interconnected single space (Lambach, 2020, p. 483) with 'blurred' geography (Carrapico and Barrinha, 2017, p. 1255) and "unstable spatiality" (Lambach, 2020, p. 489). Consequently, as virtual and physical simultaneously and beyond stately territorial jurisdiction, cyberspace significantly affects domestic and international domains (Whyte, 2018, p. 520) and challenges the state.

Notwithstanding, this study defines cyberspace as a panopticon in a Foucauldian sense, adding the surveillance ubiquity and multitude of actors involved. Initially, Bentham (Elmer, 2012, p. 21-3) used the term 'panopticon' to describe a space in which the 'prisoners' are automatically watched by the 'inspector' isolated in a 'tower'. Hence, he asserts the centrality of the 'inspector' over the 'prisoners'. Further, Foucault updated the concept by inverting the panopticon towards the focus on the 'prisoners' (Elmer, 2012, p. 24). This thesis prefers the Foucauldian perspective over Benthamian as the former considers an 'inspector' being watched. Hence, cyberspace is a panopticon, with the users as surveyed 'prisoners' and the state as the 'inspector' observing them. Although the 'inspector' might include several actors who also watch over each other, this study views them as a single actor for simplicity, disregarding internal surveillance. Notably, this panopticon is a prison with a significant degree of freedom given to the 'prisoners', watched nonetheless.

Furthermore, the 'prisoners' ability to enact surveillance allows for the reversal of power relations (Kohn, 2010, p. 580), manifesting in the *sousveillance* (Bogard, 2012, p. 30): the 'prisoners' gain the ability to watch over the 'inspector'. Hence, civil society can watch over the state. Furthermore, Weller (2012, p. 62) notes that the surveillance enacted by citizens against other citizens is common in authoritarian regimes. Hence, the 'prisoners' watch over each other, taking into account the "goals of the authority" (Kohn, 2010, p. 580). Consequently, the modern panopticon is characterized by the "increased ability to watch" (Manokha, 2018, p. 220) by many actors through ubiquitous means – e.g., surveillance cameras, increasing visibility, albeit with questionable effectiveness in

combating crime (Marx, 2005). As a result, cyberspace is a panopticon where the ‘inspector’ watches over ‘prisoners’ surveying the ‘inspector’ and each other.

Moreover, cyberspace as a panopticon represents a challenging space. First, it is not a ‘building’ but a constantly changing space without fixed borders. Consequently, from Bentham's perspective, a single ‘tower’ cannot exist in such a digital space. As per the Foucauldian view, the panopticon does not separate ‘inspectors’ and ‘prisoners’, hindering watching but allowing for decentralization. However, the initial aims of “[establishing] the potential political effects” of the panoptical surveillance proposed by Foucault (Elmer, 2012, p. 24) still holds. Although the panopticon model is often viewed as outdated, I argue that it is relevant to the case of a non-democratic illiberal country like Russia that, as per Bauman and Lyon (2013, p. 60), is not in a “majority in the global north”. Hence, cyberspace is a panopticon informed by the Foucauldian logic but enhanced by sousveilling capabilities and ‘prisoners’ watching each other.

Finally, the state seeks to establish its control over cyberspace via various means but cannot fully achieve this goal. Although military and academic communities created cyberspace, their aims were significantly distinct, with the latter making an apolitical space without controlling authority (Jayawardane et al., 2016, p. 66). However, the military and, consequently, the state were long interested in reshaping it (Deibert, 2015, p. 64). Many nation-states in cyberspace aim to nationalize it to achieve total control (Fliegauf, 2016, p. 79). At the same time, some states go for the disruption of cyberspace (Fasana, 2018, p. 169) when they cannot rule over it the way they control the physical world on their territory. Thus, the state seeking to control cyberspace is not a new issue but a significant factor in its development over its existence. As a result, it is a concern for the users, especially in illiberal countries where cyberspace becomes the only space availably for resistance.

1.2. Cybercontrol

In this study, I employ the concept of cybercontrol, which represents control enacted in cyberspace. Notably, this concept is not widely used in academia. Biennier and Favrel (2005) employ ‘cyber-control’ as relying on the technological networks, whereas Batko (2016) uses the term ‘cybercontrol’ as a human-oriented concept in Management science. Hence, the concept shifts from strictly focusing on the IT systems to looking at the users as the main impact points. In this thesis, I support the latter perception by

concentrating on the users rather than hardware, software, or data, which I see as secondary to the persons impacted by the cybercontrol.

1.2.1. Control and Discipline

The concept of cybercontrol builds up upon the Foucauldian "control and discipline" inside the panopticon (Elmer, 2012, p. 21). In other words, cybercontrol encompasses the panoptic surveillance (Foucault, 1975) enacted in cyberspace as it comprises control, discipline and – highlighted as the location – panopticon. At the same time, control can be defined as "being able to make and enforce rules for some actor(s) or space(s)" physically or non-physically (Lambach, 2020, p. 485-6), relying on the territory (Luger, 2020, p. 88). Further, I restrict the scope of cybercontrol to the state as an actor as it is the most capable of exerting cyber-power (Dunn Cavelty, 2018, p. 307). Hence, this thesis defines cybercontrol as control and discipline in cyberspace using the stately resources of cyber-power.

This study views control as watching over the users to prevent unwanted behaviours. Ceyhan (2012, p. 41) argues that the stately actions evolve "from care to control", with it seeking to exert it for crime preventing purposes resulting in a deepening of the control (Bebber, 2017, p. 434) and the construction of the surveillance and disciplining networks to accommodate the state's needs (Weller, 2012, p. 57). Control is surveillance that expands to cover more users' lives, including automation (Elmer, 2012, p. 28), to prevent deviation from the rules (Schou and Hjelholt, 2019, p. 442). As a result, it initiates the act of surveillance and proceeds to discipline the 'prisoners'.

Further, discipline signifies "modifying one's behaviour in the face of the panopticon" (Elmer, 2012, p. 22). Its primary aim is to construct a "disciplined society" (Weller, 2012, p. 58), in which the 'prisoners' are bound to the rules. At the same time, the "permanent visibility" of the Foucauldian panopticon leads to self-discipline (Manokha, 2018, p. 234). In other words, the 'prisoners' themselves modify their behaviour without an 'inspector' acting or "social supervision" (Weller, 2012, p. 57-9). Moreover, self-discipline is the consequence of ubiquitous control, which, however, can be selective when the disciplining becomes internalized. One instance of self-disciplining is self-censorship, e.g., users not posting provoking content. As a result, cybercontrol includes both control and discipline to achieve a "disciplined society".

1.2.2. Surveillance

For the notion of cybercontrol, there is a need to outline the concept of surveillance better. The Foucauldian panopticon emphasizes surveillance (Elmer, 2012, p. 23), making discipline possible. Hence, surveillance is central to cybercontrol as it is an act of watching and modifying the subjects' behaviours through self-discipline. Through surveillance, illiberal states reinforce hierarchy by making "the government unaccountable and the citizens – docile" (Kohn, 2010, p. 585) and deepen it by adopting laws allowing for acting without court orders (Yatsyk, 2019, p. 463) – "surveillance creep" (Broeders, 2007, p. 87). In other words, surveillance – and cyber-surveillance – is a tool to manage society into a "disciplined society".

Furthermore, surveillance studies build upon Foucauldian panoptical vision but go beyond it by adding more complexity. This thesis also sees surveillance as multifaceted and more than just a process of watching. Therefore, with modern surveillance being "more organized, formal and centralized" than its previous forms (Weller, 2012, p. 57), new information technologies make surveillance in cyberspace relatively cheap, allowing monitoring on a large scale (Ball et al., 2012, p. 2). Hence, surveillance policies are enacted globally and on a growing scale (Garrido, 2015, p. 155). However, surveillance is a product of modernity and not a result of technological advancement (Lyon and Zureik, 1996, p. 3). As technology surveillance does not always produce only adverse outcomes, it also has benefits, e.g., cyber-surveillance allows to combat cybercrimes. Hence, although surveillance does not belong to totalitarianism and authoritarianism, it has significant risks and dangers especially relevant to such contexts.

In other words, surveillance produces many risks and dangers which are especially imminent to the civil societies in illiberal states. First, there are infringements on human rights with data protection rights and "the right of the state to depart from the rule of law in the name of national security" (Bigo et al., 2013, p. 29) contradicting each other. Nevertheless, such issues are also relevant to the more liberal contexts, e.g., the case of internal surveillance in the EU against illegal immigration (Broeders, 2007, p. 87) shows that even liberal democracies use technology for control purposes. Another example is the COVID-19 pandemic: due to the world's increasing reliance on the cybersphere during lockdowns (Švedkauskas and Maati, 2001, p. 106) and the need for public health and order (Greitens, 2020), the states were able to increase their control drastically. Even

in the liberal context, they could justify the surveillance creep (Švedkauskas and Maati, 2001, p. 106), reutilizing the tactics used by more illiberal states. Moreover, the pandemic propagated "peer-to-peer" surveillance (Bigo et al., 2021, p. 2), corresponding with social supervision.

All in all, surveillance and cyber-surveillance are constantly evolving in the contemporary world. Although it is an issue for both liberal and illiberal states, the civil societies in the former are resisting surveillance technology. In contrast, the illiberal states have successfully increased their surveillance diffusion (Greitens, 2020). Furthermore, with the spread of surveillance normalizing it (Švedkauskas and Maati, 2001, p. 113), the future use of such technologies is made easier. Thus, surveillance is a widespread and a vital component of cybercontrol in illiberal states, enabling not only watching but also disciplining and correcting the users' behaviours.

1.2.3. Cybercontrol Practices

Technology is central to the contemporary "control, govern and discipline" outlook (Schou and Hjelholt, 2019, p. 451). Hence, the Internet is not purely a "liberation instrument" because the authoritarian regimes "possess more resources and power to control and oppress" than the society (Rudnik, 2020, p. 13), even if there is a "hunger for genuine democratization and freedom" on the part of the users themselves (Kurowska, 2020, p. 99). Despite initial freedom, cyberspace is now increasingly under the state's cybercontrol (Deibert, 2015, p. 65) as it increases its technological capabilities (Bruno, 2012, p. 343). As a result, societies become highly controlled by their respective governments in cyberspace.

Cybercontrol tools include technological and non-technological means, i.e., laws, policies, and regulations. There are instruments, such as shutdowns and blocks on access, where the "kill switch" is the ultimate form of control (Lambach, 2020, p. 495). However, according to Deibert (2015, p. 65-6), modern cybercontrol combines technological and non-technological means, with the latter growing in impact, e.g., "targeted malware attacks and campaigns to coopt social media". Hence, the third generation of such instruments includes "surveillance, targeted espionage, and other types of covert disruption" (Deibert, 2015, p. 68) and is employed today by the Russian state. Authoritarian states have become more assertive on the international level (Glen, 2014, p. 646), where countries like China and Russia promote state-centric perspectives on

cyberspace (Zeng et al., 2017, p. 440) with other states exporting the technology from them (Ramesh et al., 2020, p. 13). Hence, cybercontrol is growing worldwide and has become more ubiquitous.

At the same time, cybercontrol might have different goals, among which this thesis focuses on the state seeking to increase its power over all spheres of the lives of its citizens. Nevertheless, there are also more "acceptable" aims as upholding law and order. For instance, preventing and reducing cyber-related crimes is typical for the liberal states, e.g., the Cybersecurity Strategy of the European Union (CSSEU) (Christou, 2018, p. 356). Nevertheless, the states predominantly use cybercontrol to maintain power: peaceful protest recordings are typical for liberal and illiberal states (Abu-Laban, 2012, p. 423). Similarly, access to 'threatening' information is blocked by the state. According to Marx (2001), "it involves a determination of what can, and [cannot], […] be expressed to a broader audience in light of given political, religious, cultural, and artistic standards." This practice is more common in illiberal states (Hansen and Nissenbaum, 2009, p. 1156) but exists in liberal democracies in the form of censorship (Ramesh et al., 2020, p. 3). At the same time, non-technological means of control (Deibert, 2015, p. 65) include arrests of the users involved in cyber activities (Luger, 2020, p. 88). Therefore, illiberal, authoritarian, and non-democratic states are more prone to using cybercontrol to maintain themselves.

All in all, cybercontrol refers to the control in cyberspace and, in a panoptical sense, comprises surveillance, control and discipline. This thesis limits the concept to stately actions as the state possesses the most power and biopower (Ceyhan, 2012, p. 38). Hence, other actors with the same capacity for cybercontrol are excluded from consideration, e.g., technological corporations, which can produce comparable results but with goals of revenue rather than power (Finnemore, 2018, p. 458). However, cybercontrol cannot be entirely ubiquitous and complete (Glen, 2014, p. 637) due to the resistance of the users belonging to civil society.

1.3. Civil Society and Societal Cybersecurity

This thesis focuses on civil society representing a broader society active in the socio-political sphere. Notably, it does not look at the Russian society as a whole – as a "national, ethnic, or religious [community]" (Bilgin, 2003, p. 211) – but at a specific subgroup of the liberal civil society. The following subsection provides the definitions of

civil society and societal cybersecurity before diving into the context of Russian liberal civil society in Chapter 2.

1.3.1. Civil Society

According to Lewis et al. (2020, p. 64), civil society is a "space in which there exists a set of organizational actors which are not a part of the household, the state, or the market". This definition already presupposes some degree of organization between the actors in this space. Nevertheless, civil society also includes less institutionalized actors, such as social movements (Fominaya, 2014, pp. 6-8). Although they might represent a significant portion of the civil society, the institutionalization – i.e. creation of structured and formalized norms and institutions within the social system– allows for stability. In this thesis, I focus on NGOs and social movements with at least some degree of organization, considering civil society not "a collection of organizations […], but a 'context'" in which these organizations and movements interact and organize themselves (Lewis, 2020, p. 128). Such a perspective reflects the Tocquevillian model, prioritising more formal connections over informal ones (Ljubownikow et al., 2013, p. 154). As a result, I focus on civil society as a space where non-state actors communicate and organize themselves to protect their interests.

More specifically, NGOs could be defined as "privately constituted organizations – be they companies, professional, trade and voluntary organizations, or charities – that may or may not make a profit" (Lewis, 2020, p. 10). Notably, 'privately' here could also be replaced with 'publicly' as such organizations are independent of the state and dependent on society and the public, consisting of private individuals. Despite this broad definition, this study delineates NGO as a non-governmental organization with the goal of "the promotion of social, political or economic change" while acting as "implementers, catalysts and partners" (Lewis, 2020, p. 11-2). Despite having similar goals and "some degree of organization" (Fominaya, 2014, p. 8), social movements are different from NGOs as they do not share the same level of organizational structure and represent an informal network of public representation (Fominaya, 2014, p. 8-9). As a result, NGOs are more stable entities with visible structure and representation, making them an easier target for stately cybercontrol, whereas social movements are more flexible and harder to control on the part of the state.

Furthermore, NGOs play a significant role inside countries and internationally as non-state actors. Lewis (2020, pp. 21-2) notes that they represent alternatives to governmental organizations by providing development and socio-political change while remaining flexible and cost-effective in solving social, political, and economic issues domestically and internationally. Importantly, NGOs often act as advocacy or watchdogs when monitoring state policies (Baur and Schmitz, 2012, p. 11). Nevertheless, there are multiple critics of NGOs as being unaccountable to both the state and civil society (Sternberg, 2010) or not representative of society (Piotrowski, 2020, p. 211). Further, the NGOs might not have the same importance and role locally, especially in non-democratic countries. In an authoritarian context, the state might hinder the activities of NGOs when they go against its power. However, NGOs are valuable for society despite possible drawbacks and the state's counteraction. With a low level of accountability of the state and a non-existent feedback loop in an authoritarian context, only NGOs support society in the areas it needs, including at the international level. As a result, the NGOs are significant and valuable actors even in the authoritarian context.

Further, civil society is a vital force for social representation and resistance to governmental powers. Historically, the Westphalian view prioritized the nation-states as the only actors, seeing civil society as secondary (Maréchal, 2017, p. 35). However, the need for the "change 'from below'" (Fominaya, 2014, p. 21) has given civil society a more prominent role among non-state actors aiming to influence the global scale. For instance, the civil society engagement with the state officials might "'teach' the state to be more 'civil'" (Taylor, 2006, p. 211). Furthermore, there is a persistent assumption that democratic processes require a robust civil society (Ljubownikow et al., 2013, p. 155). For instance, civil societies participated in building cyberspace (Glen, 2014, p. 636), furthering its development as independent from the state. However, weak civil societies aiming at democratization might not be able to stop the illiberalization of the state, with post-Soviet countries like Russia, Poland, and Hungary (Piotrowski, 2020) as examples. Despite this, civil society represents "independent resistance to the state" (Lewis, 2020, p. 127), especially vital to the societies in illiberal and non-democratic countries.

In such a context, the state counteracts civil society and becomes a threat to it. Modern illiberal states can coexist with some civil society organizations, which execute a specific social function (Lewis, 2013, p. 326-8) while relying on state support

(Ljubownikow et al., 2013, p. 162). Such states disallow actions deemed threatening to the regime in the socio-political sphere. However, the "absence of political pluralism and viable civil society" (Makarychev and Medvedev, 2015, p. 46) does not equate to the total lack of the former, as civil societies still strive to remain even in the unwelcoming environment, taking different forms – e.g., "spontaneous grassroots mobilization" (Piotrowski, 2020, p. 198). Notably, this thesis focuses on socio-political activism, which leads or strives for a socio-political change rather than other forms of action. Hence, non-democratic illiberal states view civil societies as "regime challengers" and threats, which is translated into higher levels of (cyber)control and "targeted digital attacks" (Deibert, 2018, p. 535), with the state becoming a threat to the civil society itself. As a result, national (cyber)security becomes a threat to civil society's (cyber)security.

In today's world, civil society actors – NGOs and social movements – are increasingly reliant on cyberspace in their everyday practices and activities. In a non-democratic context, cyberspace is the only space where civil discussion is possible, and activists' networking occurs, making it a significant 'communicative civic space' (Van de Donk et al., 2004, p. xiii). Furthermore, it facilitates communication between members of social movements and information distribution while assisting in resource mobilization (Van de Donk et al., 2004): new members and financial donations. In other words, cyberspace is a space of 'empowerment' (Castells, 2015, pp. 45-6), making civil society more accessible and more efficient. For example, NGOs can acquire the necessary hardware and software there to increase their independence from the state (Van de Donk et al., 2004, p. 15). As a result, cyberspace allows for better communication and organization of civil society and enhances its physical presence.

1.3.2. Societal Cybersecurity

First, security means "survival and reproduction" for a 'collectivity' (Holbraad and Pedersen, 2013, p. 16). The concept does not refer to a specific referent object for which, nevertheless, for the longest time, was taken the state, "tainting" the idea politically (Holbraad and Pedersen, 2013, p. 22). State-centric definition attributes a high priority to security (Ceyhan, 2012, p. 38) as in "securing citizens and national territory against external and internal dangers" (Huysmans, 2006, p. 30). Notably, it prioritizes external dangers, "distract[ing] attention" from domestic issues (Huysmans, 2006, p. 32). Copenhagen school's securitization also imposes higher value on a threat to "our way of

life" (Goldstein, 2010, p. 492) over less significant "non-security problems" (Hansen and Nissenbaum, 2009, p. 1156). While anything could be seen as a "security issue", the state and politicians are the main actors 'securitizing' threats, with the state as a referent group.

Consequently, the possibility for a "progressive widening" of security (Holbraad and Pedersen, 2013, p. 10) leads to other spheres of insecurity being added on top of the traditional "protection of the territory" (Ceyhan, 2012, p. 40). With the growing reliance on cyberspace, cybersecurity emerged due to cyberspace's securitization (Hansen and Nissenbaum, 2009, p. 1157). For state-centric cybersecurity, cyberspace is crucial as it deals with information distribution (Dunn Cavelty, 2018, p. 306). Although many researchers consider cyber threats non-existent (Kello, 2013, p. 9), such a view is erroneous due to cyberspace's socio-political importance (Ceyhan, 2012, p. 45). Cyber threats may be less deadly than conventional weapons, but they still represent a danger to users' livelihoods. Moreover, cybersecurity is interdependent with other types of security (Willett, 2019, p. 87), in addition to cyberspace having "multifaceted spatial effects" (Balzacq and Dunn Cavelty, 2016, p. 177). Thus, cybersecurity "widens" from traditional security into a cybersphere.

Further, cybersecurity deals with "the threats to and through cyberspace" (Deibert, 2016, p. 172), constraining and enabling its "making and practices" (Balzacq and Dunn Cavelty, 2016, p. 179). Notably, it is virtual and takes physical forms due to the nature of cyberspace. For instance, cybersecurity includes repercussions like arrests for online crimes (Luger, 2020, p. 88). With the state being the primary referent object of cybersecurity, cybercrimes still promote insecurity for the state and its citizens alike (Deibert, 2015, p. 71), and related cybersecurity practices secure the nation-state and the society (Carrapico and Barrinha, 2017, p. 1255). At the same time, state cybersecurity suffers from civil disobedience (Ashenden et al., 2018, p. 47). Hence, the cybersecurity of the state might be aimed against civil society. As a result, traditionally, it represents dualities of civilian and military, public and private (Carrapico and Barrinha, 2017, p. 1255) but raises additional issues, requiring looking beyond the state's cybersecurity.

Hence, as the state-centric approach is too narrow for this research problem, I propose a society-centric lens. First, a 'human-centric' understanding corresponds with "human security" as "securing the lives and wellbeing of people, regardless of nationality, within a system of sovereign states" (Finnemore, 2018, p. 460). However, this notion is

not adequate for the security of civil society, for which nationality is crucial, linking social collectivity to the state. Moreover, far from "individual security" (Hansen and Nissenbaum, 2009, p. 1160), it deals with the security of a group with collective identities. Further, the state and the society are not the same (Bilgin, 2003, p. 211), despite the security of the former dealing with some issues relevant to the latter (Bigo, 2001, p. 95). Crucial society issues are excluded from state security based on the "personal and institutional hierarchy of dangers" (Bigo, 2013, p. 130), and the former threatening the latter (Deibert, 2018, p. 531). Thus, as national security is "the security for the state only" and human security does not account for the link to the state, societal security is the security against the state (Hama, 2017, p. 4) as a 'society-centric' approach.

Hence, I employ 'deepening' by "challenging state-centric perspective" (Huysmans, 2006, p. 34) and follow the Copenhagen school in considering society a primary referent object of security (Hansen and Nissenbaum, 2009, p. 1159). Such an outlook reinforces that the state and the society's securities are in the relationship of duality (Hama, 2017, p. 2), going against each other but being complementary. Thus, a concept of societal security accounts for the threats against society coming from state and non-state actors, endangering its identity. Specifically, the Copenhagen school proposes that identity is a critical component of societal security with it being threatened by state actions (Hama, 2017, p. 5) through the instigation of social conflict, fear (Goldstein 2010, p. 490) or damaging solidarity in the society (Bigo, 2001, p. 95). This thesis extends this understanding to include all ranges of physical and non-physical dangers to society coming from the state through cyberspace. As a result, the concept of societal cybersecurity builds upon security by simultaneously 'widening' – into cybersecurity – and 'deepening' – into societal security.

Furthermore, societal cybersecurity inherits the identity protection component from societal security (Hama, 2017, p. 5), enhancing it with cyberspace as a location for communication and identity formation. This thesis considers values, norms, institutions, and practices related to the identity of the civil society, such as solidarity (Bigo, 2001, p. 95), in-group and intergroup trust (Browning and Joenniemi, 2017, p. 5) and other forms of association (Bilgin, 2003, p. 211). Additionally, although the survival of the civil society is the primary concern of societal cybersecurity, there is also an issue of development and 'empowerment' – 'survival+' (Klein and Hossain, 2020, p. 6), which is

vital for the reproduction of the civil society. As a result, this thesis limits the scope of societal cybersecurity to civil society – in the Russian context, to liberal civil society – and widens the range of threats to cyber threats while restricting them to the threats coming from the state. Most notably, I focus on the 'survival+' practices, which entail not an 'escape' from 'dangerous' real politics to virtual politics in cyberspace but the development and 'empowerment' of the civil society through the latter for a socio-political change.

Importantly, this study does not consider national and societal securities in complete opposition, following the "Möbius ribbon" approach (Bigo, 2001, p. 95-6), which acknowledges their interconnection. However, such an outlook is suitable primarily for the liberal democratic regime. For the current context, the "Möbius ribbon" should be viewed as skewed due to imbalanced power dynamics between the state and civil society. This interdependent view allows for threats and opportunities presented to the civil society by the state (Klein and Hossain, 2020, p. 3). In the recent literature, the societal approach has begun to be viewed as more suitable for studying cybersecurity than the traditional state-centric. However, there is still little research done with such an outlook (Burton and Lain, 2020, p. 450-2). As a result, I intend to employ the theoretical concept of societal cybersecurity to investigate civil society's struggle for survival and development via cybersecurity practices. The following section discusses the context of the Russian liberal civil society as a scope for civil society.

2. CYBERCONTROL AND CIVIL SOCIETY IN RUSSIA

This section addresses the existing literature on the Russian context related to the research question. First, the study overviews stately cybercontrol. Second, I write about the Russian civil society and its cybersecurity practices. Most importantly, I discuss Russian liberal civil society as a focus of the current study. Further, the chapter produces a set of theoretical expectations and observable implications for the case.

2.1. Cybercontrol in the Russian Context

Nowadays, the Internet is an essential platform for enacting politics (Rudenkin and Loginov, 2019, p. 908). There are two spaces for politics – online and offline – in Russia, with the former producing 'real' political discussions (Rudenkin and Loginov, 2019, p. 910). However, the latter has more tangible socio-political outcomes, as decision-making occurs there. Before the 2010s, the Internet was a relatively independent space, with the opposition being widely represented (Semetko and Krasnoboka, 2003, p. 93). The protests of 2011-2013 against, initially, the 2011 Russian legislative election results and, further, against president Putin running for third-term reelection in 2012 led to a drastic shift in how the Russian leadership viewed the Internet and its impact on the 'real' world (Litvinenko, 2020, pp. 12-3). As a result, the state started paying attention to cyberspace, with military and intelligence agencies taking the lead (Burton and Lain, 2020, p. 450).

Consequently, the state has securitized cyberspace (Vendil Pallin, 2017) and is developing its cybercontrol capabilities, which are already higher than many countries, especially democratic ones, have (Nye, 2011, p. 20). Notably, the Russian state is not omnipotent due to the "multiplicity of surveillance components and dysfunctionalities" (Gabdulhakov, 2020, p. 297). However, the state's actions "resemble the Soviet past" (Gabdulhakov, 2020, p. 287) and the 'Orwellian' panopticon (Weller, 2012, p. 62). The government utilizes its biopolitical power to promote a conservative agenda (Makarychev, 2017, p. 9) in cyberspace to enforce the commitment to the obligations of its citizens rather than protect their rights (Rudnik, 2020, p. 47). Overall, the Russian government sees cyberspace as dangerous and seeks to impose cybercontrol over it.

2.1.1. Sovereign Internet

Sovereign Internet is central to the stately understanding of the ideal for cyberspace internationally and internally. Russian leadership sees national cybersecurity and Internet Governance as the same domain (Maréchal, 2017, p. 29), intrinsically connected to the concept of sovereignty. With security being an integral part of the Russian national identity (Yatsyk, 2019, p. 465), the state prioritizes the protection of its internal sovereignty in cyberspace from external threats. The state has a record of using its cyber power against other countries with such goals (Willett, 2019, p. 85), e.g. instance, a hacker attack against Estonia linked to the relocation of the "Bronze Soldier", a Soviet World War II monument (Burton and Lain, 2020, p. 452). Thus, the Russian state seeks sovereignty in cyberspace, prioritizing independence and total control over its territory and non-intervention (Claessen, 2020, p. 143).

Further, Russia wishes to establish itself as an Internet Governance leader (Budnitsky and Jia, 2018, p. 595) by promoting a state-centric vision of cyberspace. In other words, it is a space in which the state wants to achieve respect and influence globally and minimize its vulnerabilities (Kurowska, 2020, p. 88, 96) as it views cyberspace as warfare (Dunn Cavelty, 2018, p. 306). Russia supports a state-centric and sovereignty-oriented position on cyber governance (Zeng et al., 2017, p. 440) and considers cyberspace territorial to its physical space despite the loose borders (Claessen, 2020, p. 145). Hence, it seeks to delineate, protect, and control these boundaries similar to the physical borders (Kukkola and Ristolainen, 2019, p. 65), which presents a significant challenge when enacted in transnational cyberspace (Ermoshina and Musiani, 2021, p. 2). Nevertheless, the borders are present in the official discourse (Kukkola and Ristolainen, 2019, p. 74). As a result, Russia seeks to promote a bordered vision of cyberspace linked to the physical territories of the nation-states.

Control over cyberspace domestically is crucial to sovereignty and relates primarily to the 'Sovereign Internet' law[3]. Despite manifesting to protect the country from the external threat, it is an instrument reinforcing the authority of the state and isolating the Russian sector of the Internet from the global network (Epifanova, 2020, p. 2) by a 'Digital Iron Curtain' (Gabdulhakov, 2020, p. 287), a model similar to Chinese, which

[3] Amendments to the Federal Laws"On Communication" and "On Information, Information Technologies, and Information Protection".

also supports state-centric cyber sovereignty (Fliegauf, 2016, p. 79). Notably, the development of the Chinese Internet depended on the government in contrast to Russia, where until the 2010s, the state did not partake in the process and allowed Internet freedom (Ermoshina and Musiani, 2017, p. 42).

2.1.2. Cybercontrol Practices

The Russian state employs propaganda and other methods to achieve discipline and self-discipline in society. First, the government successfully frames the Internet and cyberspace as a "CIA tool" of the "Evil West" (Gabdulhakov, 2020, p. 287) and a dangerous place (Maréchal, 2017, p. 32) where criminal activities are the norm. This discourse diverges some citizens from the 'dangerous' content, to which both adults and children are vulnerable (Marx, 2001). Nevertheless, as such a method is not fully effective, the state also employs technological methods of cybercontrol. For instance, the 'Sovereign Internet' law mandates the usage of traffic prioritization hardware (Epifanova, 2020, p. 3), allowing the state to restrict access to specific Internet resources. At the same time, the Russian leadership employs control over search engines, social media, operating systems and software, hardware, and other methods (Kukkola and Ristolainen, 2019, p. 71). As a result, the state enforces cybercontrol to create a 'Sovereign Internet' independent from the West.

Nevertheless, the Russian state differs from other states with similar agendas. Unlike China, Russia has no "great firewall" to filter and block all the 'dangerous' information, so it aims primarily for disciplining (Poupin, 2021), albeit with significant restrictions on access to content. Behind it is the structure and history of independent development of the Internet in Russia and the difficulty in designing a decentralized control system on a large scale (Ramesh et al., 2020, p. 1). Hence, the state employs selective filtering of the content[4] , blocking torrents and pornography and restricting political media[5]. The latter directly attacks the liberal civil society, which loses access to crucial information, i.e., people partaking in protests watch less TV (Onuch et al., 2021, p. 14) and use the Internet as a primary source. In other words, most cybercontrol practices aim to restrict and discipline liberal civil society but do not empose complete control.

[4] Retrieved January 4, 2022, from https://onimap.citizenlab.org/filtering-soc.html

[5] Retrieved January 4, 2022 from https://www.vpnmentor.com/blog/online-censorship-country-rank

Notwithstanding, the Russian state employs extensive cybercontrol over hardware, software, data, and users. According to Ermoshina and Musiani (2017, p. 43), there are three major cybercontrol systems in Russia: 1) surveillance via the System of Operative Investigative Measures (SORM) used by FSB; 2) restrictions on data storage; 3) 'arbitrary' laws, i.e., laws which are "numerous, varied, constantly adapting, and their enforcement often arbitrary" (Ermoshina et al., 2022, p. 30). First, there are surveillance mechanisms, the most significant of which is the Yarovaya package[6] which includes SORM and other additional measures employed to empose complete visibility of the users in cyberspace. These measures require the Internet operators and companies to install software and store all the data exchanged by the users. Hence, the state having direct access to this data can sanction liberal civil society members' online activities. Additionally, there are other cybercontrol practices, e.g., video surveillance. As a result, the Russian state ensures complete visibility offline and online.

Second, the state restricts how the data should be stored, e.g., with the 'landing' law[7]. It enforces the personal data of Russian users to be geographically contained to the servers on the Russian physical territory. Hence, international technological companies should transfer all such data to Russia. On the one hand, this practice protects the users' data from misuse outside of the country. However, it also makes foreign websites insecure for the liberal civil society, similarly to the Russian ones. This law corresponds with the general trend for "control through ownership of the physical infrastructure" (Vendil Pallin, 2017): the state acquires the physical infrastructure or transfers ownership to state-owned or affiliated companies. Consequently, the state seeks to control data physically through the hardware and its geographic location.

Third, the state restricts access to information and enforces censorship by using a wide variety of 'arbitrary' laws. In other words, laws such as 'anti-extremist' and 'anti-terrorist'[8] and similar policies and extrajudicial tools are used to pressure the liberal civil society actors into compliance (Maréchal, 2017, p. 31). The state uses censorship blocklists compiled by Roskomnadzor (the Russian state agency responsible for restrictions on the Internet) to block content and resources on the country's territory for

[6] Two Federal Laws amending various Federal Laws on counter-terrorism

[7] Federal Law "On the Activities of Foreign Persons in the Information and Telecommunication Network 'Internet' on the Territory of the Russian Federation"

[8] Various Federal Laws, including Yarovaya package

transgressions under these laws (Maréchal, 2017, p. 32). These laws are 'online speech', 'fake news', and 'disrespect for authorities'[9]. Nevertheless, the state's capabilities in this area are in doubt (Ermoshina and Musiani, 2021, p. 6). For instance, Roskomnadzor attempted to block Telegram but ended up "unblocking" it in June 2020 after being unable to tackle this challenge (Ermoshina and Musiani, 2021, p. 23). Hence, the government employs various laws to mark content as 'dangerous' and block it.

Further, the Russian state uses the 'arbitrary' laws to impose self-discipline in the form of self-censorship to ensure that 'dangerous' content is avoided at creation and distribution. As a block might result in heightened interest, the state uses different framing of 'undesirable' content (Nisbet et al., 2017, p. 959). Russian leadership stimulates self-censorship by randomly arresting users (Gabdulhakov, 2020, p. 297). Hence, direct censorship laws encourage self-censorship because of the harsh sentencing for minor transgressions. For instance, regarding the case of Savva Terentyev, Voorhoof (2018) writes that the domestic charges were seen as "a clear and imminent danger" rather than a less significant offence for hate speech against police officials without the intent of actual action. Further, there is a substantial growth in the 'extremist' charges against Internet users (Gabdulhakov, 2020, pp. 284) for online activities. Additionally, there is biopolitical censorship under the 'gay propaganda' law[10] (Kondakov, 2019, p. 214). As a result, the state uses various censorship practices to foster self-censorship.

Moreover, the 'foreign agents' law[11] directly targets active liberal civil society members. Russian leadership holds to the Westphalian perspective and considers that the nation-states are the only meaningful and independent actors in international relations (Maréchal, 2017, p. 35), with other actors unable to act of their own will. Hence, the opposition is perceived as "organized anti-regime movements" dependent on the other states (Deibert, 2016, p. 174) and, consequently, a threat to national security. Hence, the state aims to destroy the connection of the liberal civil society to the outside world (Daucé, 2020), predominantly in the financial sphere, by restricting sources of income and imposing sanctions on those who receive foreign money. However, the 'foreign agents' law is applied to persons and organizations with minimal foreign transactions due

[9] Various amendments to the Federal Law "On Information, Information Technologies, and Information Protection"

[10] Federal Law "For the Purpose of Protecting Children from Information Advocating for a Denial of Traditional Family Values"

[11] Various amendments to Federal law "On nongovernmental organizations"

to this label being an effective instrument for imposing self-censorship. First, holders of this status lose their incomes and partnerships due to stigma. Second, their texts, including personal posts, must contain a specific text outlining the agent-ness of the author. As a result, 'foreign agents', predominantly influential persons and journalists, change their information distribution practices or leave the country.

At the same time, the state balances its goals with the risks which bring restriction of access to essential websites: the potential to trigger protest activity (Litvinenko, 2020, p. 13). Although, according to Levada Center, only 13% of the citizens were against the introduction of the censorship laws in 2018 (Akhmadieva et al., 2018, p. 6), specific websites with higher usage and no available Russian alternative are avoided. For instance, Twitter 'slowing' did not trigger a comprehensive reaction and has shown that the site is not widely used. Further, the state uses the Russian Troll Farm to influence the agenda internationally (Jensen et al., 2019, p. 226) and domestically. Although domestic discourse legitimises the Russian state's international actions, i.e., trolls run anti-Ukraine and anti-USA campaigns (Vesselkov et al., 2020, p. 94), the domestic aspect is discussed much less often, with Vesselkov et al. (2020) pioneering the issue. Also, the Russian state employs bots to fight the opposition (Stukal, 2022, p. 11). Nevertheless, the domestic usage of the Russian bots and trolls is severely understudied. Hence, the Russian government cannot rely only on technological means but also on other instruments to ensure content censorship, among which self-censorship appears to be the most effective.

Finally, the state uses additional methods of cybercontrol, which involve assistance from non-state actors. Primarily, non-state Internet companies are approached for user data, with Vkontakte (VK) allowing the state access to personal data being a primary example. Although officially out-of-the state control, such companies comply with all the requests. Also, there are "active citizens" forming 'cyber squads' or "neighbourhood watches" (Gabdulhakov, 2020, pp. 284) to monitor social networks and report findings to law enforcement, which coincides with panoptic "peer-to-peer" surveillance. Thus, the state ensures cybercontrol by using all the instruments available, including society.

2.2. Russian Liberal Civil Society

2.2.1. Liberal Civil Society

Although there are questions if there is a "viable" civil society in Russia (Makarychev and Medvedev, 2015, p. 46), there indeed exist entities adhering to the basic definition of civil society presented in the previous chapter. Hence, although civil society exists in Russia, it is less visible, with its features differing from the Western concept. Ljubownikow et al. (2013) provide an overview of the development of civil society since the Soviet times, presenting the argument that Russian civil society relies on the state to survive. Hence, the most visible part of the Russian civil society self-excludes itself from the political sphere to avoid clashing with the state due to its reliance on stately resources (Ljubownikow et al., 2013, p. 153). According to Ljubownikow et al. (2013, p. 155), such a situation stems from the Soviet and earlier post-Soviet periods in which civil society organizations could not survive without strong links to the government. Moreover, the state has created a "managed" civil society via a network of NGOs and social movements, faking societal participation and democracy (Hemment, 2012, p. 258). Hence, the majority of the civil society in Russia is less than self-sufficient, requiring support either from the government or from other states.

At the same time, some independent movements and organizations continue to function. Although Ljubownikow et al. (2013, p. 163) hypothesized that the civil society in Russia moves closer to the state, I focus on the part of the civil society that is independent of the latter due to its socio-politically active stance. This subgroup connects to the 'foreign agents' law as they a) receive money from abroad or b) are perceived by the state as such because they do not receive money from the government itself. Furthermore, the existence of a liberal civil society is illustrated by the cases of Ivan Golunov and Yegor Zhukov (Litvinenko, 2020, p. 14) when utilizing cyberspace for communication and mobilization assisted in freeing them from the state.

Furthermore, the 'liberal' in the 'liberal civil society' relates to procedural liberalism rather than a political stance. In other words, the primary goal of liberal civil society is to establish and develop liberal-democratic order with independent institutions, a multi-party political system, and a pluralist society through regime change. Consequently, the liberal civil society cannot rely on the state and must act as an alternative or in opposition to it to achieve its goals.

Notably, Russian liberal civil society differs from other illiberal and non-democratic states' civil societies because its organizations are legally allowed to exist and operate while facing pressure (Toepfl, 2018, p. 542). In other words, the state seeks to discontinue these NGOs and social movements but does not prohibit them entirely. One explanation could be that the Russian state wants to present itself as democratic. For instance, as most of the media in Russia is controlled by the state, there are also "niche oppositional mass media" (Toepfl, 2018, p. 541) against which the government applies cybercontrol but does not eradicate them. Furthermore, social networks allow for a limited social-political discussion (Litvinenko, 2020, p. 13). Russian social media users use various platforms with different 'average' users (Litvinenko, 2020, p. 12): Facebook, Google, and WhatsApp coexist with Russian VK, Yandex, and (arguably Russian due to its higher independence) Telegram. Facebook is considered to be a social network for 'liberals'. In contrast, the state controls VK, Russia's most popular social media (Lonkila et al., 2021, p. 136), making it less secure for activists. However, despite censorship, there are still opportunities for social-political activism.

Furthermore, liberal civil society actively uses cyberspace to mobilise and promote its values. As the government does not allow the opposition to partake in the political life of the country offline, the latter employs the Internet for campaigning (Dollbaum, 2020, p. 1) or "Internet elections" (Toepfl, 2018, p. 532), mimicking offline political processes. The most prominent example of cyberspace usage would be Alexei Navalny and FBK (Anti-Corruption Foundation), utilizing it as a strategic tool for mobilising and distributing the content (Dollbaum, 2020, p. 9) and sousveillance. For instance, during the electoral campaigns, they utilize an instrument for voters coordination, e.g., Umnoe Golosovanie (Smart Voting, a project initiated by FBK to promote oppositional candidates for parliamentary elections over United Russia pro-Putin candidates). Hence, cyberspace allows for the distribution of prohibited by state information, increasing the impact of liberal civil society on the country's political life.

2.2.2. Societal Cybersecurity Practices

As liberal civil society members are hindered from conducting their activities offline, cyberspace is an essential space for the liberal civil society's existence. Professional activists employ various practices to protect themselves from stately cybercontrol, which cannot be said about 'average' users who are less inclined to use

cybersecurity (Poupin, 2021). Some Russian Internet users' technological and non-technological practices are highlighted in the literature. On the individual level, Poupon (2021) outlines methods like filtering the friendship lists and requests on social networks depending on trust in the person, using VPN, proxy services, and browser extensions to bypass blocks, hiding or deleting social media profiles (Poupin, 2021). In other words, the activities range from non-participation in specific online platforms for political reasons to circumventing restrictions, with the latter being more resistant than the former.

On the organizational level, the NGOs buy private servers, which in Russia requires the deanonymization of the NGO representative for registration purposes (Ramesh et al., 2020, p. 2) but can be done outside of the country. Notably, the liberal civil society struggles with visibility as it is both necessary for mobilization and harmful to its members, for whom being seen by the state means being endangered. Nevertheless, Lokot (2018, p. 334) also highlights that visibility protects the most prominent activists, 'ensuring' their safety from cybercontrol. Additionally, deanonymization might increase trust in the person. Hence, in an illiberal and non-democratic state, civil society's visibility and anonymity in cyberspace play a more complex role, with the actors being both endangered and protected by their identities. Nevertheless, the stately cybercontrol actions seek to deanonymize members of the liberal civil society, including through legal means, as it benefits from knowing the real identities of the activists.

Furthermore, liberal civil society has a history of resisting cybercontrol, with Telegram being one of the most prominent cases. Lonkila et al. (2021, p. 146) call the app a "platform for technoactivism" due to the users utilizing technical skills and developing solutions to continue the usage of Telegram despite governmental pressure (Akbari and Gabdulhakov, 2019, p. 229). They employ proxy services and VPN networks to retain access. Most importantly, the app developers produce better solutions allowing access to Telegram even without client-side actions (Ermoshina and Musiani, 2021, p. 6). The state could not block the app completely, eventually deciding to 'restore' access (Ermoshina and Musiani, 2021, p. 23). This experience demonstrates that resistance is possible when dealing with cybercontrol. However, the state successfully blocks content using technological (e.g., 'slowing' Twitter; restricting access to Google Docs with Smart Voting materials before the elections) and non-technological (making Telegram restrict access to Smart Voting bot) means.

Non-technological practices are harder to circumvent for the liberal civil society than technological methods. Proposed by Lyon (1998), legal resistance appears to be the least impactful in Russia. Although there are petitions against restrictive laws (which use cyberspace as an instrument), the state does not consider them (Ermoshina and Musiani, 2017, p. 45). Also, petitions to the businesses made by the liberal civil society activists do not help the situation as the state's capacity to pressure the former into compliance is higher (Ermoshina and Musiani, 2017, p. 46). Notwithstanding, some Russian NGOs are vocal about Internet freedom (Gabdulhakov, 2020, p. 289), but they primarily monitor the situation without significant outcomes for liberal civil society. As a result, resistance is limited to rare 'successes' such as Telegram, which, as Lyon (2018, p. 76) points out in his later work, might not bring a real change. At the same time, "evasion tactics" are effective practices for minimizing individual risks (Ermoshina and Musiani, 2017, pp. 51-2), but they might not provide for a change on the societal level.

Furthermore, the liberal civil society employs self-censorship as a form of self-discipline to minimize risks related to cybercontrol. Conforming to the disciplining practices is a form of societal cybersecurity practice leading to less insecurity. First, the political situation in the country serves as a crucial factor for self-censorship as a practice on the individual level (Rudnik, 2020, p. 41). The activists refrain from partaking in online discussions by moving to more secure platforms or physically, i.e., emigration (Lonkila et al., 2021, p. 149). Hence, the latter is an effective instrument in dealing with stately cybercontrol, similarly to the physical transfer of the hardware (Ermoshina and Musiani, 2017, p. 51). The result for Russia is the end of the online "lively online political debate and activism" (Lonkila et al., 2021, p. 137). Legal restrictions directly limit the expression and speech in the Russian section of the Internet (Rudnik, 2020, pp. 33-4), with pre-publishing decisions considering these risks (Rudnik, 2020, p. 43). Nevertheless, there is a need for a better understanding of how self-censorship integrates with other cybersecurity techniques on the societal level.

2.3. Theoretical Expectations

This section outlines the main theoretical expectations stemming from the conceptualization of cybercontrol, liberal civil society, and societal cybersecurity. In the first part, the thesis considers the former and how it affects liberal civil society. Further,

the study focuses on the response produced by liberal civil society using societal cybersecurity practices. Additionally, I highlight possible observable implications.

2.3.1. Cybercontrol and its Effects on Liberal Civil Society

The expectations regarding cybercontrol relate to the specific practices, which are anticipated to become more prominent, with turning points related to the major protests and the Russian war on Ukraine. Before data collection, I presupposed that the participants might name the 'foreign agents' law and the Yarovaya package among the most potent cybercontrol methods. However, I did not construct an exhaustive list as I intended to use the empirical data to distinguish the most effective cybercontrol practices. At the same time, I expected these practices to be viewed negatively by the participants. In other words, the perceptions of the cybercontrol by the respondents might contain some positive views on specific measures (e.g., in battling cybercrime), but the predominant position was expected to be opposing to the stately actions.

Furthermore, I classify the effects of cybercontrol into two categories: physical and non-physical. The former is related to the offline consequences and the physical well-being of the persons. I expected arrests, compelling people to emigrate from Russia, and social movements and NGOs decapitation (Luger, 2020, p. 88) to be among the most widespread physical impacts on liberal civil society. Further, their impacts were anticipated to be more severe for the members of the liberal civil society than the non-physical effects. At the same time, I did not presume that such consequences are common in liberal civil society but concentrated with a small group of the most active participants, whereas the majority were expected to be affected by non-physical effects only.

Hence, I expected non-physical effects to be more widespread, with cybercontrol triggering negative emotions like fear and anxiety among the activists. This thesis presupposed that fear and trust issues are the primarily non-physical effects of cybercontrol. As cyber threats have a cognitive impact on their targets (Burton and Lain, 2020, p. 454), this impact was expected to influence activism outcomes. With surveillance generating fear and mistrust "within and between communities" (Burton and Lain, 2020, p. 466), these effects translate into "social damage" (Akhmadieva et al., 2018, p. 6) and have an immense effect on interactions with other people and daily actions (Lyon, 2018, p. 62). Moreover, "at the individual level, social movements are emotional movements" (Castells, 2015, p. 13). Hence, emotions are crucial to consider when studying liberal civil

society. With television being a significant source of fear, mistrust, and hopelessness (Wober and Gunter, 1988, p. 20), I expected similar effects in cyberspace. As existing research rarely addresses emotions related to societal actions (Lyon, 2018, p. 61), I seek to mend this gap.

I see fear as a 'repressor', triggering anxiety which, in turn, leads to "avoidance of danger" (Castells, 2015, p. 219-21). Hence, this emotion is crucial for self-discipline. Moreover, the knowledge that you are being watched results in fear and anxiety (Lyon, 2018, p. 75), making them elements of the panopticon. Consequently, fear produces a "chilling effect", an "[act] of holding back" while being watched to adhere to the authority rules (Manokha, 2018, p. 228-9). The latter is especially prominent during times of "the rapid expansion of pervasive surveillance" (Lyon, 2018, p. 65). At the same time, "anxiety need not necessarily be something to be assiduously avoided" (Browning and Joenniemi, 2017, p. 15). According to Wollebæk et al. (2019, p. 8), fear counteracts the creation of echo chambers or informational 'bubbles' in cyberspace to which anger, on the other hand, contributes. Consequently, the state might seek to increase fear even in the most opposition groups for its members to 'transfer' to more pro-state views.

However, Vargo and Hopp (2020, p. 754) note that fear – and anger – increase political engagement. Notably, as their research deals with online advertisements, they conclude that evoking negative identities leads to lower engagement with such ads. Hence, I expected that the state using negative identities (e.g., 'foreign agents') might not lead to the liberal civil society adopting a negative perception of the identity but either ignoring it or viewing it positively. Thus, liberal civil society could transform anxiety into positive actions through anger as a trigger (Castells, 2015, p. 219). Notwithstanding, the consequences of anger might also be negative (Wollebæk et al., 2019, p. 9). I anticipated some participants translating their fear into apathy. Zhelnina (2020, p. 358) characterizes "apathy syndrome" as a product of "personal frustrating experiences", resulting in "long-term cynicism and disbelief in the efficacy of collective action." Zhelnina (2020) presents empirical evidence on this coping mechanism being widespread among Russian youth after the 2011-2012 protests, which I see as relevant still. As a result, I expected fear to translate both into positive action and non-participation, with the former prevailing.

Regarding trust, I expected low levels of trust in the state and higher levels of trust in liberal civil society. As trust is a source of the social contract (Castells, 2015, p. 1), I

anticipated its erosion and "precarity" in interactions with the state (Ashenden et al., 2018, p. 43) in response to the pressure on the liberal civil society (Bruno, 2012, p. 346). As mistrust "discourages belief in the collective action and solidarity" (Zhelnina, 2020, p. 359), I see trust as necessary for moving forward for the Russian liberal civil society as the Russian society itself is deeply fragmented. Hence, I presumed that the in-group trust suffers damage from the "witch-hunting" but grows overall. An observable implication for a declining trust would be a rejection of communication with strangers on the Internet to avoid provocations (e.g., Novoe Velichie case when a group of young people from an online chat was arrested for starting an 'extremist' society after being joined by a provocateur). The latter includes the state sending its agents to provoke the members of the liberal civil society into law-breaking actions (or seemingly so) or spy on them, with the Russian state using such methods as far as during Tsarist Russia, albeit with varying success (Marx, 2012). Also, I expected participants to trust the 'foreign agents' more than people and organizations without such status when considering trust increase. The trust levels were expected to be negatively impacted by cybercontrol.

Notably, the context of the illiberal state was expected to impact the quality of liberalism in the liberal civil society through trust levels. As liberalism entails trust together with solidarity and toleration (Offe, 2001, p, 176), the illiberal context makes them dangerous as unwillingness to trust is not only an element of the illiberal thinking but also a product of fear. Hence, in the Russian context, I expected a liberal civil society to lose some qualities of liberalism related to trust as a way to survive in an illiberal context. In contrast to the part of the civil society adjacent to the state mirroring illiberalism of the state (Ljubownikow et al., 2013), I anticipated the liberal civil society to manage their trust as a security practice while still relying on liberalism.

2.3.2. Societal Cybersecurity Practices

I explored two types of practices used by liberal civil society: technological and non-technological. Among the former, the thesis presupposed using VPN, two-factor authentication, and various other data protection methods enhanced by technology (Lokot, 2018, p. 332). Lyon (2018, pp. 67-8, 76) highlights that, according to a survey, 86% of users undertake specific steps to "remove or mask their digital footprints" and adds "clearing cookies, masking IP address and encrypting emails" or "adjusting privacy settings in Facebook and covering the laptop lens" as possible actions. Hence, there are

various techniques, but I am interested in the ones used the most by the members of liberal civil society. I anticipated that such practices are growing, spreading among more people. The "acts of self-protection" (Lyon, 2018, p. 76) were presupposed as the most prominent. However, I also expected the NGOs to build their systems and cybersecurity methods beyond protection for resistance (Van de Donk et al., 2004, p. 15).

Furthermore, the study anticipated a range of non-technological practices, especially in response to the non-physical effects of cybercontrol. As a panopticon might produce conformity on one hand or resistance on the other (Bauman and Lyon, 2013, p. 54), I expected the non-technological practices to mirror this theoretical assumption. In other words, I awaited practices of both resistant and non-resistant (conforming) nature. Moreover, I expected self-discipline to be prominent via self-censorship or "limiting [user's] visibility to others" (Lyon, 2018, p. 62). The observable implication would be participants deleting profiles or not posting content ("deleting, editing, untagging" [Rudnik, 2020, p. 6]). Because self-censorship links to the "chilling effects", the users are expected to change "how [they] obtain and share information online" due to the surveillance over them (Lyon, 2018, p. 66). As a result, this thesis anticipated liberal civil society members demonstrating significant self-discipline.

At the same time, this study also expected resistance. Lyon (1994) outlines two directions in which it might happen: a fight for privacy laws (p. 170) and social movements (p. 174). Nevertheless, I argue that the former is irrelevant to the context of the current research case as a non-democratic country. The latter would also not be effective due to the weak liberal civil society, to which Lyon (2018, p. 117) himself seems to subscribe in his more recent work. However, I expected the participants to enhance liberal civil society by establishing links horizontally, for instance, through networking. Simultaneously, distrust of organizations or persons (Castells, 2015, p. 4) also produces trust networks through inclusion and exclusion.

Furthermore, Castells (2015, p. 2) writes that "togetherness helps to overcome fear". In other words, "sharing and identifying with others" (Castells, 2015, p. 221) allows one to deal with this emotion and associated anxiety. Hence, I anticipated the study participants sharing that working with other liberal civil society members helps them overcome this fear. There might be different ways of dealing with anxiety, including getting used to it. Hence, I anticipated distinguishing various practices helping people to

overcome fear. Consequently, the study expected liberal civil society employing various technological and non-technological practices to minimize the physical and non-physical consequences of cybercontrol.

As a result, this thesis approached liberal civil society and its societal cybersecurity by reviewing how it is affected by stately cybercontrol and, consequently, how it deals with its adverse effects. I expected that cyberspace would be indispensable for liberal civil society as an instrument and a platform for communication despite the insecurity. As "it creates the conditions for a form of shared practices" and helps liberal civil society's survival and expansion (Castells, 2015, p. 229), I anticipated at least some degree of resistance in addition to conformity. This study measured cybercontrol through stately practices and its impact on the liberal civil society through the fear and (dis)trust it generates, with societal cybersecurity making liberal civil society more robust.

3. METHODOLOGY

In this investigation, I use a qualitative framework with an interpretive approach. In other words, the study views the actors partaking in the cybersecurity practices as "meaningful" and possessing subjective perceptions, motivations, and understandings of the situation (Della Porta and Keating, 2008, pp. 23-4). Notably, feelings of insecurity in cyberspace are highly subjective and should be studied from this perspective. Hence, the study focuses on the perceptions and experiences of liberal civil society members against stately cybercontrol. The following section deals with the research methodology, including possible challenges and biases. It relies on the previous chapters' theoretical framework to support the data collection and analysis. First, the chapter discusses the case selection and then dives into the research design and methods.

3.1. Research Design

This thesis employs an outcome-oriented case study research design. I look into the reaction of the liberal civil society (dependent variable) against the stately cybercontrol as an independent variable. At the same time, I treat societal cybersecurity as an intermediate variable acting as a filter between the state and liberal civil society. Notably, societal cybersecurity might not be present in every interaction between the state and liberal civil society but also results from it. As a result, the current thesis's qualitative interpretive stance allows me to treat this complex connection by employing subjective perceptions of the actors without losing reliability.

Furthermore, the choice of Russia as the case country is informed by several factors, including but not limited to my research interest in the Russian liberal civil society and its struggle against the state. Hence, I understand that there is a significant degree of bias in my personal views on the issue, as I am a part of the Russian liberal civil society sharing its values and perceptions. Nevertheless, as the thesis takes an interpretive stance, I do not seek a completely objective inquiry into the research question but follow a more subject-oriented path. Moreover, being a part of the group allowed me to gain the trust of the study participants, meaning that they were more willing to share their honest thoughts and ideas with me, which are also subjective. As a result, my research interest has informed the country's selection while also being instrumental in the data collection and analysis stages.

At the same time, Russia is a valuable case for academia and policy-making because of its distinctiveness from other authoritarian countries in cyberspace development history and cyber strategy (Vendil Pallin, 2017). After an initial period of freedom, the Russian state started increasing cybercontrol physically, technologically, and legally (Nisbet et al., 2017, p. 959), which means that the liberal civil society has already established itself online. Further, Russia is a non-democratic country whose leadership promotes illiberal and conservative values (Makarychev and Medvedev, 2015), reflected in cyberspace through data and users. As the liberal civil society cannot act in the real world, cyberspace becomes the only place for the activists and other actors to partake in the country's socio-political life. Hence, the liberal civil society's reliance on cyberspace allows for a better understanding of the former through the latter. Finally, the topic of Russian societal cybersecurity is under-researched, with limited research on liberal civil society. As a result, the Russian case yields valuable results as the liberal civil society is the only independent of the state actor in Russia.

Consequently, the case study of Russia allows me to investigate this complex connection between the stately cybercontrol and the liberal civil society via societal cybersecurity practices. I intend to look deeper into the research problem, which is quite extensive, with a case study approach. Hence, a study over several cases would not produce significant results as the research question requires deepening, not widening the sample. As a result, I collected more data points for the Russian case with the methods to be discussed further.

3.2. Method and Data

I use qualitative data collection and analysis methods to understand the research problem. The methods are linked to the theoretical framework and expectations: they allow the gathering and analysing of perceptional data on a sensitive topic. The data collection and analysis were conducted in Russian. I provide translations of the participants' utterances.

3.2.1. Data collection

I employ two data collection techniques: in-depth expert interviews and focus groups. The reasoning behind these two approaches is that the Russian liberal civil society comprises people with different levels of involvement: professional activists and persons engaged in volunteer activities. Whereas the former have more profound expertise than

the latter, the latter represents most of the active population. Also, experts and professionals differ in practices from ordinary participants because they are involved in organizational cybersecurity activities. They are also more knowledgeable and experienced in liberal civil society, which yields better insight via in-depth interviews. At the same time, volunteers possess less expertise but still represent liberal civil society. Hence, studying both types of liberal civil society actors is crucial, but it must be done with different methods for efficiency.

Empirically, I follow the hypothesis to investigate the direct and indirect effects of cybercontrol. First, the study outlines cybercontrol practices and participants' perceptions about them. Second, the impact on liberal civil society is discussed. Finally, I look into the liberal civil society cybersecurity practices, distinguishing them by the use of technology and resistance. Moreover, I examine how these practices manage the effects of cybercontrol. Hence, having resistance and non-resistance in the sample would confirm the non-linear primary hypothesis. As a result, the data collected for this study aims to prove the primary hypothesis by looking into reaction and counterreaction through societal cybersecurity practices.

I employ interviewing to get an insight into the research topic from the professionals and experts working for NGOs or engaged in a social movement. This thesis presupposes them to be the most active part of the liberal civil society, with the most pressure from the state. Notably, political prisoners could also be related to this group. However, although they suffer the most pressure, this pressure is predominantly offline, with online being often restricted to them. Hence, most cybercontrol is aimed at the active representatives of NGOs and social movements, which are not imprisoned but, as cyberspace is also a panopticon and a prison, are constantly watched and disciplined. At the same time, these individuals represent liberal civil society and have significant expertise in their respective areas. As a result, the in-depth interviews allowed me to gain an insight into their personal and organizational experiences with cybercontrol and societal cybersecurity. Hence, as liberal civil society consists of individuals and groups with shared values and norms, this thesis intends to extrapolate the findings from individual to a liberal civil society level, with additional questions on the experiences.

Furthermore, as a synchronous in-depth interview allows a high degree of interaction with the participant (O'Connor and Madge, 2017, p. 420), the study utilizes a

semi-structured online interview to accommodate the geographical distance between the interviewee and the interviewer. Moreover, the semi-structured interview allows me to direct the interviewee into a specific area without imposing strict limits. Appendix 1 shows the Interviewer Guide with a basic outline of the in-depth interview. The questions are divided into several topics covered during the interviews but depend on the previous answers. Notably, there are additional 'spillover' questions on the experiences of acquaintances of the interviewee for better saturation of the data on the level of liberal civil society. Hence, during the interview, I used this guide to collect the necessary data on the research topic.

Overall, this thesis planned for ten interviews with the representatives of the socio-politically relevant subgroups of civil society: political movements, human and civil (in particular, electoral) rights protection NGOs and media. Initially, the thesis planned for two interviewees per sector as an ideal ratio. However, due to the issues with the interviewee's availability, I could not achieve a fully balanced representation of the liberal civil society. Nevertheless, the balance is contained with some participants representing two categories after moving professionally from one sector to another. Notably, I include media as a sector as this thesis sees media representatives as valuable for their insights into the issue. Although they might not relate to NGOs or social movements, they are valuable actors for the Russian liberal civil society, providing critical information for the society, including through cyberspace. Further, media practitioners also experience heightened cybercontrol from the state and, consequently, are expected to apply societal cybersecurity to reduce their insecurity.

For recruitment, I have employed networking and snowballing to broaden the sample. During this process, I used several criteria for the interviewees' selection:

- Tenure: how long the person is active in the liberal civil society, favouring more experienced actors;
- Broad social connections, favouring interviewees with a broader network;
- Deep expertise, favouring people with vast professional experience and reputation.
- Relevance to cyberspace and cybersecurity, favouring those who use cyberspace in their activities.

I did not use the snowballing technique extensively due to the respondent's unwillingness to trust distant acquaintances. Hence, a possible recruitment bias is attributed to the short degree of acquaintance, which did not 'stretch' beyond 1-2 contacts between them and me. To control for this, I approached interviewees with different backgrounds. Also, I collected some rejection statistics as the lack of response might be interpreted as a statement, albeit with a hidden meaning. Nevertheless, Russia's liberal civil society is compact and not significantly spread out, so studying this group using networking and limited snowballing still gives valid results.

Hence, due to my involvement with one of the Russian NGOs as a volunteer, I used my pre-existing connections for interviewing and, later, focus groups, which allowed me to establish trust with participants. Otherwise, if contacting people without a reference from another trusted actor, I would not be able to arrange interviews on a sensitive topic. Speaking about the state's actions might be risky in the Russian context; discussing cybersecurity practices could produce adverse effects if the state finds out about them. Consequently, I made the process transparent and secure for the interviewees. I used the initial message, consent form (see Appendix 2), and an interview introduction to explain all the potential issues that might arise and answer questions. Hence, the participants had all the information needed to choose whether they wanted to partake in the study, with anonymity being a cornerstone. I also stressed that they could refuse to talk about sensitive topics or discuss them off the record. Simultaneously, the study did not refer to the personal data at any stage following the interview. Next, the collected data was stored securely on an encrypted device outside the Russian Federation territory and not transferred to other people. Finally, I also did not collect data which could lead to dangerous outcomes. As a result, I applied all the necessary steps to prevent avoidable risks for the interviewees.

Furthermore, I used synchronous online focus groups to collect data from active volunteers, referring to Moderator Guide (see Appendix 3). Despite being underused in the past, the legitimacy of the focus group as a research method is growing (Stanley, 2016, p. 237), and it is excellent for the research question focused on societal practices. With focus groups, I sought to distinguish the feelings and real-life practices of the respondents. While interviews provided more information on cybercontrol and institutional response, focus groups concentrated on individual practices. Moreover, as the target audience for

focus groups is more prominent in size, I had more observations with a higher variation, adding to the research's validity. As a result, focus groups investigated members of the liberal civil society who might be less active or knowledgeable about the liberal civil society but represent it and broader civil society.

I recruited the participants for focus groups through the interviewees of the in-depth interviews. The study focuses on NGOs, some of which engage volunteers in their activities. For recruitment, it was crucial to establish trust with an NGO or social movement representative, possibly through an interview, and then ask for volunteers to join focus groups. I used the Google Forms for a pre-survey to collect preliminary information about the participants seeking a) to inform participants about the goals of the focus group and possible risks, b) to receive consent for participation in the focus group (see Appendix 4), c) to receive confirmation for the confidentiality agreement (see Appendix 5), d), to gather sociodemographic data (see Appendix 6), e) to gather contact information, f) to gather dates and time slots for scheduling purposes. Online form allowed for efficient and structured data collection through several NGOs at once, with anonymity but an opportunity for the researcher to check on the trustworthiness of participants via their demographic and contact data.

Further, I planned for at least ten focus groups, but due to the participants' availability had to extend the number to fourteen to accommodate different schedules, albeit with a smaller number of participants in some focus groups. Due to the topic's sensitivity, I did not recruit participants who were not vetted by the NGO, as it could bring additional risks, despite confidentiality agreements. Further, I intended to have focus groups of 4-5 participants in size. However, some of the focus groups ended up including 1-2 participants, turning into mini-interviews. Although Barbour (2007, pp. 8-10) refers to a higher number of sources being optimal, they also point out that the size of the focus group depends on a multitude of factors, including time constraints and the moderator's ability. Hence, more participants in one focus group could lead to some not speaking up and me being unable to engage all the participants. Also, focus groups were arranged for 1 hour – 1 hour 30 minutes slots which I found hard to accomplish with more than 5 participants. As a result, I conducted 14 focus groups, one being a mini-interview.

For the focus group formation, I used the data on the participants' availability, with dates and times being the primary factor. While I planned for 40-50 participants, I

was able to speak with 52 people. Appendix 6 includes the participants' sociodemographic characteristics. Figure 8 shows gender distribution as skewed but still representative. Figure 9 demonstrates age distribution, underlining that participation in liberal civil society might depend on age as younger people appear more likely to be activists. Figure 10 shows that although almost half of the respondents are from Moscow, the sample also includes participants from other regions and people who left Russia. Hence, the sample is representative of people from distinct sociodemographic groups.

Additionally, while referring to the Moderator Guide (see Appendix 3), I used Menti[12] to gather additional data from the respondents during the interview (see Appendix 7). The visual questions add structure, organise the participants, and allow them to enter ideas and their answers anonymously. Nevertheless, the primary purpose of the focus groups is to engage the persons in a discussion and gather their subjective perceptions, with Menti being supplementary to the cause. The focus group allowed this study to gather a broader range of observations for the qualitative analysis.

At the same time, focus groups have yielded biases connected to the 'bubble' as the in-group connections are more robust than inter-group ones. As the liberal civil society can be seen as a network with NGOs being nodes of concentration, the participants of the focus groups might be too closely related to each other. Nevertheless, providing that recruitment was initiated through several NGOs and social movements, the coverage of the liberal civil society was achieved, with participants from various subgroups partaking in the focus groups. As the scope of the study is restricted to the liberal civil society, the study's validity did not suffer from the weakness of the links between the liberal civil society and other parts of the civil society. Hence, the selection bias did not damage the analysis quality correlating with the restrictions imposed on the research.

Simultaneously, the focus groups share similarities and notable distinctions with the interviews in sensitivity and confidentiality. Similarly to the in-depth interviews, the briefing of the participants was essential. I provided them with a description of the study and explained the whole process in writing. Additionally, the respondents could refuse to answer but were given an instrument to submit their answers anonymously via Menti during the focus group. They gave informed consent before initiating the process (see Appendix 4). Due to the multiple participants partaking in the interview, confidentiality

[12] Link: www.mentimeter.com

was essential (see Appendix 5): participants were asked not to record and not share any information outside of the focus group. Finally, I did not use the participants' real names, with each assigned a pseudonym to use during the recording. The anonymity of the participants means that other focus group interviewees could not misuse the information. Next, I anonymized the responses by using a second set of pseudonyms. The recordings and the personal data of the respondents were deleted, erasing the link between the data and participants. Hence, the focus group required additional steps to ensure that the respondents' answers would not endanger them or their identity. As a result, per the "near paranoia" approach (Fujii, 2021), I handled the data and participants so that the state could not deanonymize them and that participation in this research would not have negative consequences.

3.2.2. Data Analysis

This thesis used qualitative content analysis (QCA) to analyze the data acquired at the previous stage. As this approach focuses on latent meanings (Schreier, 2012, p. 15), I investigated the participants' perceptions through in-depth interviews and focus groups. Due to the sensitivity of the research topic, latent meanings are crucial because participants might hide their true feelings or intentions intentionally or unintentionally. Hence, feelings and emotions were coded as fear or tiredness acting as repressors or anger and hopefulness as triggers (Castells, 2015, p. 219). As a result, with QCA, I analyzed the research question linking cybercontrol, its effects and social cybersecurity practices.

Further, the QCA utilized the coding system based on the conceptual framework developed in Chapter 2. The main themes (Saldaña, 2021) were generated directly from the research's theoretical background: cybercontrol, its effects, and societal cybersecurity. More specific categories and codes stem from these themes. Cybercontrol encompasses physical and non-physical stately practices, including surveillance, discipline, and aimed at self-discipline. There are non-physical, i.e., feelings stemming from the theoretic framework: fear and (dis)trust, and physical effects: e.g., incarceration. Finally, societal cybersecurity includes the practices of the liberal civil society enacted in response to these impacts: technological and non-technological – e.g., VPN and self-censorship. Importantly, I devised subcodes from the empirical data that referred to specific practices or effects in the first coding round. As a result, the coding framework was built from subcodes and codes into categories relying on theoretical themes.

Consequently, this thesis applied the QCA to investigate the connection between cybercontrol and the societal cybersecurity of the liberal civil society. I used in-depth interviews data to distinguish the relevant cybercontrol practices of the state as seen by the experts. I validated the interview data with focus groups. Further, I approached the effects cybercontrol has on liberal civil society. Here, both interviews and focus groups were utilized to reinforce each other. The latter generated more data on the emotions and other effects on the individual level, while the former spoke more at length about the liberal civil society and its organizations. Finally, the practices of liberal civil society at the individual and organizational level also stem from both in-depth interviews and focus groups. Hence, the analysis proceeded in three stages, from investigating the relevant cybercontrol practices to their effects on the liberal civil society and how the latter reacts to the former with the societal cybersecurity practices.

Furthermore, the credibility and trustworthiness of the study grow from expert interviews supported by the focus group data. Although the latter cannot provide a thorough perspective on the research question, broader coverage of the liberal civil society through focus groups allows for the research's higher credibility and validation of the findings from the interviews and the novel insights gained from the focus groups themselves. In other words, although focus groups are used for testing the hypothesis, they also enforce the study's validity by confirming the interview's insights. Overall, the thesis used empirical data and the theoretical background to validate the findings and improve the study's credibility.

This thesis answers the research question using the data collected through in-depth interviews and focus groups and analyzed via qualitative content analysis. Hence, the study investigates the primary hypothesis that cybercontrol has not only a direct negative impact on liberal civil society but also indirectly enhances its societal cybersecurity capabilities. Although I expected the immediate direct impact to be negative, the research adopts a methodology that might lead to an opposite conclusion to avoid biases. Thus, based on this Chapter, I collected the data and conducted its empirical analysis to gain valid and reliable findings for the research question. The following chapter outlines the main results of the investigation.

4. EMPIRICAL EVIDENCE FROM RUSSIA

For the empirical part of the study, I have conducted ten interviews with the experts and fourteen focus groups as described in the methodology. Appendices 8 and 9 contain the lists of interviews and focus groups, including basic information on their layouts. Due to ethical considerations, I do not include the transcripts themselves in this thesis. Further, the interviews were conducted from March 2021 to January 2022, whereas focus groups took place from January until mid-February 2022. Thus, the focus is on the period prior to the Russian attack on Ukraine on February 24, 2022.

With the QCA, the acquired data was coded in two consecutive rounds, starting with interviews, and proceeding to the focus groups. I composed the primary codes based on the theoretical framework and the expert interviews. Next, I organized them, forming a tree structure with categories, themes, codes, and sub-codes. Furthermore, I codded the focus groups, enhancing the code system. I have finalized the coding system by re-organizing them further. Finally, I conducted the second coding round to apply the final code system to the data. In the following sections, I present findings stemming from the data analysis.

4.1. Cybercontrol Practices

4.1.1. Evolution of Cybercontrol

The data has reinforced the previous research on the evolution of cybercontrol in Russia. Expert 10 (Interview 10, 30.01.2022) highlighted that the state did not interfere much during the initial period of cyberspace development (the 1990s and 2000s). However, Expert 6 (Interview 6, 12.10.2021) added that the protests of 2012 drew more attention to cyberspace. Nevertheless, the state's actions were not consistent during these years. For instance, the Russian leadership has promoted video surveillance at the voting stations but, at the same time, started prohibiting the publication of the discovered violations on an Internet platform (Expert 8, Interview 8, 12.11.2021). Hence, the state has started restricting information distribution despite the manifested transparency.

Furthermore, the start of the Russo-Ukrainian war in 2014 has led to more cybercontrol exerted by the state (Expert 6, Interview 6, 12.10.2021). In 2014, the state's censorship increased via the 'foreign agents' law (Expert 7, Interview 7, 22.10.2021), which many study participants perceived as an efficient cybercontrol instrument with significant offline consequences. Notably, for an offline-online axis of cybercontrol,

Expert 4 (Interview 4, 05.10.2021) said that "the problem is not only with the Internet" but with pressure on the liberal civil society in general. Hence, although cybercontrol is exerted online, its impact is significant overall as cyberspace becomes the only space of freedom. For instance, Expert 4 (Interview 4, 05.10.2021) noted that "before there was more pressure offline [than online], but as there is almost nothing to press offline right now, they pressure online." When speaking about the media in cyberspace, Expert 6 (Interview 6, 12.10.2021) noted, "In ten years, a prosperous landscape turned into a very not prosperous one". In other words, following the successful nationalization of offline TV and other forms of the media (Expert 1, Interview 1, 27.03.2021), the state has started to increase its cybercontrol significantly in the mid-2010s.

Furthermore, the state continued introducing other laws and practices, especially in 2019-2020: 'fake news', 'disrespect towards authority', 'Sovereign Internet' laws and the Yarovaya package (Expert 1, Interview 1, 06.04.2021). The latter is a surveillance law exerted over any activity on the Russian Internet segment, including but not limited to storing messages and even "any information transferred by the employee of a diplomatic mission who uses Russian networks" (Expert 1, Interview 1 06.04.2021). Moreover, Expert 1 highlighted the concept of information distribution organizers, which requires any website with communicative functions to install an expensive surveillance system allowing access to any data to FSB (Federal Security Service) without a court order or to be fined and shut down. Further, the focus group participants highlighted the surveillance activities of SORM (The System for Operative Investigative Activities) as harmful. Hence, Expert 1 considered Yarovaya law an excess in "combating terrorist operations", with significant pressure on ordinary citizens. Notably, apart from technological and law enforcement surveillance, there was also mention of 'cyber squads' in university settings which enforce adherence to rules by the student community.

4.1.2. The Current Situation

From 2020 to 2022, the state has used the COVID-19 pandemic to increase its cybercontrol. For example, changes to the 'foreign agents' law made it possible for persons to be assigned this status (Expert 1, Interview 1, 06.04.2021). Since then, the 'foreign agents' list has grown significantly (Expert 7, Interview 7, 22.10.2021). Nevertheless, the primary reason for the censorship increase could be attributed to the spread of coronavirus 'fake news', with Expert 1 summarizing the position of the

Roskomnadzor as follows: “we will not let anyone spread the coronavirus fakes. We are fighting the pandemic with exceeding force and insist that the information should be absolutely correct”. Moreover, Expert 1 stressed that previously introduced ‘fake news’ legislation started to be applied “super-actively” – at a much higher rate than before. In April 2020, the state introduced changes to the ‘fake news’ law with criminal responsibility, which according to Expert 1, were “radical and unnecessary” as the existing administrative offence clauses were not yet widely applied.

Furthermore, Expert 9 (Interview 9, 26.11.2021) underlined that in 2021, the pressure by the state on social networks had grown significantly following the return of Alexei Navalny to Russia in January 2021. Expert 9 connected increasing rates of content monitoring with the spread of oppositional information by FBK, including the sousveillance investigation on Putin’s palace. The poisoning of Alexei Navalny could also be attributed to online activity, especially online mobilization (Expert 3, Interview 3, 27.09.2021). Further, changes were made to the slander legislature, making it a criminal offence and extending the definition of slander to cover any “unclear” group of people instead of a specific person (Expert 1, Interview 1, 06.04.2021). Finally, the surveillance creep went to the streets with the state installing more cameras and promoting services with face recognition, thus enhancing ubiquitous cyberspace. Participant 52 (Focus Group 14, 08.02.2022), who lives abroad, noted the striking contrast in the number of cameras in Moscow after visiting the city for the first time in three years since 2019 and said, “it looks like you are being watched everywhere”. As a result, the state has continued actively increase surveillance and censorship pressure during the pandemic.

The current situation with cybercontrol in Russia is constantly changing, with new restrictive measures being introduced and applied. The state works in several directions, blocking content and resources, pressuring VPN and Internet companies into cooperation, and threatening them with liquidation for not complying (Expert 1, Interview 1, 06.04.2021). For instance, in 2021, the state successfully blocked information related to the Umnoe Golosovanie (Smart Voting), even on Telegram. Notably, the state previously failed to block this messenger (Expert 5, Interview 5, 09.10.2021). The state also increased the number of censorship laws (Expert 2, Interview 2, 31.08.2021). Finally, it has “destroyed” anonymity in cyberspace by mandating the account connected to identified phone numbers (Expert 1, Interview 1, 27.03.2021).

4.1.3. Perceptions of Cybercontrol

Nevertheless, as cybercontrol becomes increasingly widespread, the liberal civil society sees its impact and efficiency differently. For instance, while blocking (but not banning as the state has no capacity to prohibit and enforce using the resources) is common, Expert 8 (Interview 8, 12.11.2021) still considered that the "state has not yet learnt how to use the Internet". Similar perceptions are shown by the focus group participants noting the state's limited abilities:

"[The state] cannot win, at least completely, but it tries to control [cyberspace]."

(Participant 36, Focus Group 9, 31.01.2022)

"I think that because of their 'crooked hands' and total bribery, it [the cybercontrol] will be holey like a fence, and there will always be some loopholes".

(Participant 4, Focus Group 1, 15.01.2022)

"Often, they do not have brains for something more than slowing the pictures on Twitter."

(Participant 48, Focus Group 12, 05.02.2022)

"[…], the state was not very successful in controlling [the information]. Look at the situation with Telegram; they were not able to block it!"

(Participant 46, Focus Group 11, 01.02.2022)

In other words, the participants doubted that the state could impose an efficient cybercontrol because of its "lack of skills". Importantly, they doubted the abilities of the technical personnel working for the state (Participant 3, Focus Group 1, 15.01.2022). At the same time, some participants admitted that "the state has more resources and will always have" (Participant 42, Focus Group 10, 01.02.2022) and considered a total Internet shutdown as the most efficient tool in the hands of the state:

"Today, they jam signal during the protests, and tomorrow they can shut down the connection completely if needed […]."

(Participant 45, Focus Group 11, 01.02.2022)

Despite such perceptions, there was also a view that such a practice would not be beneficial for both actors:

"From one perspective, [shutting down the Internet] is the state losing, but, on the other hand, it will not give anything to the free people; they will lose too."

(Participant 46, Focus Group 11, 01.02.2022)

Hence, the participants doubted that the state would want to shut down the Internet entirely and hinted at the Chinese scenario's impossibility in the Russian context (Participant 1, Interview 1, 15.01.2022). Nevertheless, Expert 3 (Interview 3, 27.01.2022) expected the state to impose restrictions similar to the Chinese firewall after improving its skills. Consequently, there is no consensus on the issue, but the predominant view is that the state cannot act in cyberspace better than ordinary users with technical skills.

Although a complete shutdown is the only practice perceived as hard to circumvent, there are other cybersecurity practices that the study participants treated as 'important': blocking, slowing and deleting content and preventing its distribution. More specifically, these are blocking by the Roskomnadzor, censorship, 'foreign agents' and usage of bots (see Appendix 7, Figure 4). Notably, the latter – bots or 'kremlebots', trolls – are seen as harmful to the freedom of speech and an effective instrument of propaganda and control over public opinion, creating a favourable to the state background:

"It is also a way to put people in a box to think that there are not many of them."

(Participant 41, Focus Group 10, 01.02.2022)

As a result, the participants viewed some of the cybercontrol practices as successful but still doubted the ability of the state to apply cybercontrol efficiently. The most 'powerful' instruments are related to publishing and distributing information restrictions.

4.2. Effects on Liberal Civil Society

Among the stately cybercontrol effects, I distinguish three groups: general security perceptions and physical and non-physical impact. Starting with how the study participants measured their safety, most of them saw cybersecurity as a part of broader security rooted in the offline world. Such perceptions are common among focus group participants and experts. For instance, Expert 8 (Interview 8, 12.11.2021) noted "some background feeling of the lack of security". Figure 3 (see Appendix 7) demonstrates the quantitative cybersecurity measures from focus group participants. Hence, on average, participants feel neither safe nor unsafe.

Nevertheless, there is a potential bias in the recruitment of the participants. First, experts with insufficient security are more likely to reject the interview. For instance, during the data collection, my request for an interview was rejected because the potential interviewee had stricter cybersecurity rules. Additionally, I have faced a lower

recruitment rate when publishing a call for focus group participants. In one of the NGOs, where the response rate on the tasks for volunteers is roughly 10%, the response rate to my investigation was 3.2%. Hence, I assert that the measures could be biased towards people feeling less insecure.

Furthermore, personal cybersecurity depends not only on the feeling of a threat but also on preparedness. Cybersecurity skills, methods, and overall preparedness impact the feeling of security. For instance, Participant 1 (Focus Group 1, 15.01.2022) accounts that the cyberspace is "friendly" and "safe" because "if [police] will attempt to enter into my apartment right now, I will have these 30 seconds […] to write on Facebook: 'Guys, I need help!' – And I know that they will help me." Moreover, Figure 12 (see Appendix 6, Figure 12) demonstrates that, on average, participants assess their cybersecurity skills as moderate, with only 1/5 of them measuring as less than average. Notably, only a fifth of the participants are employed in the IT sphere (see Appendix 6, Figure 11). Hence, considering Figures 2 and 3 (see Appendix 7) and qualitative data, the Internet is perceived as an instrument that could be turned against the liberal civil society. However, at the same time, the cybercontrol pressure on liberal civil society is compensated by the societal cybersecurity practices, resulting in an average level of insecurity. The following sub-sections focus more on the physical and non-physical effects of cybercontrol, including trust and fear, before I present findings on their cybersecurity practices.

4.2.1. Physical Effects

Physical effects are the consequences for the liberal civil society members offline, i.e., on their physical bodies and lives. Physical repercussions inspired the study participants most fear (see Appendix 7, Figure 6). These effects are deeply interconnected with any actions of the members of the liberal civil society against the state: offline or online. First, most participants expected visits by the police and arrests or fines on administrative charges. Surveillance, especially before critical offline events, is widely cited too. For instance, Participant 36 (Focus Group 9, 31.01.2022) said, "I am already used to police coming to me before protests." In other words, the state seeks to hinder coordination via the Internet by eliminating key participants tracked through cyberspace. For instance, Participant 47 (Focus Group 12, 05.02.2022) saw a sentence to a detention centre as the most undesirable offline consequence. As Expert 6 (Interview 6, 12.10.2021) noted, criminal cases and sending people to jail are the state's most influential and

dangerous instruments. The participants appeared to consider such cases as a consequence of overall resistance to the state, not only their activities in cyberspace.

At the same time, Participant 1 (Focus Group 1, 15.01.2022) remembered a situation when their friend was visited by a law enforcement agents, who attempted to scare them by "[demonstrating] printouts of their social network accounts" with posts for which they could be punished. Hence, many physical visits are linked to the actions done online without a specific event offline. Further, Participant 1 (Focus Group 1, 15.01.2022) noted that these people might not even be activists but be just randomly selected. Notably, the participants attribute such selection either to the special surveillance agents (e.i., Department E, *Отдел Э*) or non-state 'cyber squads'. Overall, visits and arrests are seen as random or directly a consequence of resistance.

Furthermore, visits result in searches during which devices – such as laptops and smartphones – are taken by the police, creating additional risks for their data. For example, Participant 40 (Focus Group 10, 01.02.2022) mentioned that all their devices were taken away during a search, leaving them without access to accounts. Hence, through visits and searches, the state attempts to a) generate fear in the activists; b) take away their resources and physical devices.

4.2.2. Non-Physical Effects

Many cybercontrol effects relate to data and users, their feelings and emotions. As per the theoretical framework, I have focused on fear as a repressor with secondary feelings such as anger acting as triggers. Moreover, the change in trust is essential for social capital and is a non-physical consequence of cybercontrol. As a result, this sub-section covers, first, emotions and, second, trust as the effect of the cybercontrol. First and foremost, Figure 6 (see Appendix 7) demonstrates the responses of the focus group participants to questions related to fear. Overall, the data demonstrate that the study participants feel, on average, both neither fully secure nor insecure. Notably, the selection bias might appear as more fearful respondents would not partake in the study. Hence, the levels of fear might be higher. Moreover, among the participants, the feelings of anxiety were not prominent but connected to the possibility of physical consequences.

Nevertheless, the experts considered fear to be the most crucial effect of cybercontrol, with Expert 3 (Interview 3, 27.01.2021) noting that "censorship [and] fear work" and adding that "people have no strength to resist as they are intimidated". Further,

Expert 4 (Interview 4, 05.10.2021) admitted to feeling "more fear than before", characterizing it as a "discomfort" rather than an intense fear, with Expert 7 (Interview 7, 22.10.2021) sharing the same position. Additionally, Expert 9 (Interview 9, 26.11.2021) reported that volunteers working with them fear legal consequences for participation. As a result, experts highlighted heightened fear in the liberal civil society.

Furthermore, they also noted that the fear does not increase intensively. Expert 6 (Interview 6, 12.10.2021), who works in the media, stressed that there is a "selection for braver and tougher" people. In other words, the expert highlights that cybercontrol creates a situation in which only less fearful people "survive" and stay in the profession. Similarly, Expert 5 (Interview 5, 09.10.2021) said about political activists' rationale behind lack of fear, "It could be if I understood that I was breaking some significant law […]. However, there is no law and no court. So, there is no reason to be afraid." Participant 43 (Focus Group 11, 01.02.2022) also highlighted having no feeling of fear due to previous extreme experience with the state. In other words, 'arbitrary' laws lead the members of the liberal civil society to stop feeling fear and act more rationally.

At the same time, the focus group participants also reported the existence of fear, but its levels were moderate, with background anxiety and discomfort but with little paranoia. Similarly, the data shows that people fear the physical consequences. For instance, Participant 1 (Focus Group 1, 15.01.2022) stated that "fears and anxiety are […] connected […] with offline consequences." Further, many participants have expressed concern over online actions (posts, reports, likes) having real-life consequences. Although some mentioned "criminal cases for likes" without recalling specific situations, the likes were considered the safest action. At the same time, the fear of doing posts and reposting differ among the participants as some considered producing content as more dangerous while others, on the contrary, see posts by organizations and 'foreign agents' as such. For instance, there are participants for whom their content is seen as a threat:

"Yes, I am significantly afraid [of doing posts] because there are precedents."

(Participant 14, Focus Group 4, 20.01.2022)

"I also have fears related mostly to producing the content."

(Participant 11, Focus Group 3, 19.01.2022)

At the same time, other respondents highlight that reposts as more dangerous, primarily due to their connection to the organization (NGO or social movement):

"Making your post is not so scary – who needs me? However, likes and reposts are scarier: if [the state] surveys [reposted] organization, they can find me."

(Participant 9, Focus Group 2, 16.01.2022)

Hence, there is no clear consensus on which action is the most dangerous. Further, among the main reasons for fear is the randomness of the punishment due to the 'arbitrary' laws. For instance, Participant 49 (Focus Group 13, 05.02.2022) said, "there were more or less visible cases, […] a lot of such cases. You start to think ten times […] what you have written on the Internet before. […] You do not need to be a super activist for [the state] to catch you for something." Participant 18 (Focus Group 5, 26.01.2022) also noted that "you do not know when you can become interesting [to the state]." In other words, the randomness of the selection for the punishment generates fear.

Nevertheless, there is a significant level of the "no one needs me" mentality as many participants did not perceive themselves as "prominent activists" (although some respondents have the opposite experience). Many participants also reflected on their personal data and the possibility of being hacked as not worrisome:

"It could be connected with the fact that I do not present any interest to the state or someone else. So, my data does not interest anyone."

(Participant 39, Focus Group 10, 01.02.2022)

Hence, most participants were aware of the possibility but did not see themselves at high risk. Moreover, most participants thought personal data was "already" stolen, referring to the recent data leaks attributed to the state – e.g., from FBK. Some also highlighted that the state already has all the data through Gosuslugi (e-governance website) and entrance intercom cameras. Consequently, many study participants did not fear repeated hacks and leaks. Nevertheless, they did fear hurting others:

"I am afraid not only for myself but mostly for […] volunteers [of my organization]. For my messages, I am not particularly afraid. However, I am scared that [it] will be released, and another person will have problems."

(Participant 30, Focus Group 8, 29.01.2022)

Therefore, the data demonstrates that the members of the liberal civil society have fears predominantly about the offline consequences and impacting other people rather than their personal data.

Furthermore, other feelings are triggered by cybercontrol, including "powerlessness" and "apathy", albeit at a lower rate. Again, there is a potential bias for people who leave the liberal civil society due to burnout. For instance, Expert 9 (Interview 9, 26.11.2021) highlighted those negative experiences and stories decreasing the motivation among their volunteers. Nevertheless, some participants cited apathy in the past due to extreme cybercontrol (Participant 19 [Focus Group 5, 26.01.2022] told their story of being tapped by the law enforcement agency) or when significant events did not catch the attention of society (Participant 45, Focus Group 11, 01.02.2022). However, most respondents did not express such feelings.

At the same time, some focus group participants reported triggers like anger, irritation and discontent. These feelings were not always directly triggered by cybercontrol but are transformed from fear. For instance, Participant 45 (Focus Group 11, 01.02.2022) said, "happens, […], that the fear transforms into anger, and it is no more fear, but a feeling which motivates me to do something." Further, reflecting on their self-censorship, Participant 2 (Group 1, 15.01.2022) explained that "it is so maddening when you restrict yourself in some instruments or do not write [something]." Hence, anger was rarely a primary feeling but a way of coping with negative emotions triggered by cybercontrol. At the same time, this trigger is more productive, albeit negative. Participant 19 (Focus Group 5, 26.01.2022) also noted that the liberal civil society "unites but unites unconstructively, on anger and similar feelings." However, the data did not show a radicalization among the participants. Hence, irritation, anger, and even disgust are widespread triggers resulting from the participants' experiences with cybercontrol.

Finally, the changes in trust are crucial for liberal civil society as high levels of atomization and distrust do not allow Russian civil society to work effectively. Hence, the state destroys links between the people, resulting in changes in how people perceive each other and societal organizations. Thus, I sought to see whether the state was able to impact the trust in the liberal civil society negatively. First, the participants do not trust the state or affiliated organizations. The increasing cybercontrol has only deepened the distrust towards the state. For instance, Participant 31 (Focus Group 8, 29.01.2022) said, "there is no trust towards the state – fewer and fewer remains. [Because the person's life is at the bottom,] the further, the worse."

Notwithstanding, trust in liberal civil society is not unconditional among the participants. On average, the respondents do not blindly trust the media (even independent), people and organizations (see Appendix 7, Figure 7). However, some default level of trust exists. I selected two reference points to review how stately cybercontrol impacts trust: the Novoe Velichie (New Greatness[13]) case and the 'foreign agents' law. For the former, as the case itself was not cited to the participants, only one focus group participant recalled it and triggered a discussion on how it had impacted their behaviour in group chats. Hence, Participant 21 (Focus Group 6, 27.01.2022) noted that "after the story with the Novoe Velichie, I am particularly wary of the chats". Otherwise, most participants demonstrated a high level of trust in the group chats, predominantly related to specific NGOs. As a result, most participants did not distrust people in online communications, especially when following cybersecurity practices.

Furthermore, the 'foreign agents' law was explicitly referenced in a question to ask whether such status impacts trust among the members of the liberal civil society. The participants themselves cited that it is unclear how the same label is viewed outside of the community, for which this study does not attempt to provide an account. However, status holders envoke higher trust among the respondents than organizations, people, or media without it. For instance, Participant 35 (Focus Group 9, 31.01.2022) remarked that they trust 'foreign agents' more on the Internet, highlighting that "if it is some website or an account with 'foreign agent' status, but I know nothing about it, then the initial sympathy towards it is much higher […] like some friend recommended it to you."

Although the participants do not express unconditional trust towards 'foreign agents', many cite sympathy and understanding that the media, organization, or person are working against the state if it had decided to 'cancel it'. Hence, for the most part, the 'foreign agents' law allows the liberal civil society to distinguish similar-minded sources and persons. It does not damage the trust inside the liberal civil society but assists in making institutions more trustworthy. As a result, the findings demonstrate that the state does not decrease in-group trust by using said instruments. However, it does not mean that trust levels do not suffer. Some respondents comment on searching for traitors in some organizations, bordering on paranoia, marking them negatively. As the state has expertise in tapping and hacking, data leaks are not necessarily a consequence of the

[13] A criminal case against participants of a group chat with opposition views see more info.

traitors' actions, but as many participants noted, "if the state needs something, they will open it anyway" (Participant 50, Focus Group 13, 05.02.2022).

4.3. Societal Cybersecurity Practices

I distinguish between technological versus non-technological and resistance versus non-resistance practices. The former classification relates to the distinction between cyberspace as an instrument and cyberspace as a communicative space. In other words, technological practices employ cyberspace capabilities, whereas non-technological stem from behavioural practices enacted in cyberspace. The latter classification relates to practices used for defence or resistance. Notably, I consider non-resistance practices as survival only, whereas resistant ones make the liberal civil society more robust.

4.3.1. Technological Practices

As cyberspace is rooted in technology, few purely non-technological or technological practices exist. Among the latter, I distinguish three types of activities: data protection, online defence and proactive methods. First, the data defence includes a significant hardware component which is especially relevant during searches when the devices are taken away by the police. For instance, Participant 12 (Focus Group 3, 19.01.2022) remarked that they "try to keep all the important data on the cloud". Furthermore, the participants talked about quickly deleting data from all the devices in an emergency. For example, Participant 2 (Focus Group 1, 15.01.2022) said that it is crucial to know how "to delete all the data from the PC in one minute, when [the state] is breaking into your door." Also, physical territoriality is crucial as organizations and people prefer to store critical data on servers outside of the Russian Federation.

Physical security includes mobile devices, which must employ passwords and two-factor authentification instead of a face or fingerprint identification. Although Expert 9 (Interview 9, 26.11.2021) noted that people related to liberal civil society still use the latter methods and some focus group participants also admitted to it, there was a consensus on preferring passwords so the state could not open their phones against their will. Hence, password and two-factor authentification practices are widespread, especially for critical accounts, e.g., Telegram. Further, the participants also mentioned encryption. Hence, the participants take the necessary steps to protect their data and accounts physically and virtually.

Furthermore, online defensive practices directly respond to stately cybercontrol to prevent adverse effects. For instance, on the organizational level, the NGOs protect their websites from DDOS attacks, using such services as Cloudflare (Expert 10, Interview 10, 30.01.2022). On an individual level, the issue of deanonymization was mentioned, for which the study participant utilized more resistant practices such as buying anonymous SIM cards or using the TOR browser. However, such methods are not widespread, with most respondents accepting deanonymization. Further, VPN usage for such a purpose is not common, but most participants admitted employing VPN to access blocked resources. For instance, Participant 44 (Focus Group 11, 01.02.2022) said that "[their] favourite websites are being blocked, so [they] have to use VPN more and more." Overall, VPN is one of the most popular technologies among the study participants.

At the same time, there were less resistant practices like abandoning previously used instruments, e.g., specific social networks, which borders on self-censorship as proactive online actions such as posts, reposts, likes, and subscriptions depend on the platform. For instance, Participant 21 (Focus Group 6, 27.01.2022) said, "I deleted the page in VKontakte in 2018, after many people went to jail. Maybe, I just got scared." Many study participants have stopped using VK (VKontakte) because the state has full access to its data. Expert 4 (Interview 4, 05.10.2021) mentioned that "any actions and messages in VK are open to the controlling authorities." However, Expert 1 (Interview 1, 27.03.2021) noted that this social network is "really very popular": even among study participants, it (37) is used more than Facebook (35) (see Appendix 6, Figure 13). Hence, activists interested in spreading the information on any available platform still employ this social network despite the risks. The respondents cited that people who do not relate to the liberal civil society use VK, and they are a target audience for the information distributed by the activists (Participant 11, Focus Group 3, 19.01.2022).

Moreover, some respondents noted that they do not link distinct social networks among each other, separating their communications with real-life acquaintances and anonymizing spaces where they discuss the socio-political situation in Russia. Most participants prefer foreign social networks (Facebook, Twitter, Instagram and YouTube) to Russian ones, especially in security. Overall, leaving the space is a non-resistance practice, whereas staying there is resistance. At the same time, there are such practices as making accounts private and filtering subscribers and friend lists. These practices cannot

be considered fully resistant as they restrict information exchange outside the community. However, they make the remaining exchange safer. As a result, such practices propagate an information 'bubble' but help the people inside the liberal civil society to communicate with each other.

Furthermore, messengers are increasingly used, with all participants using Telegram more than any social network (see Appendix 6, Figure 13). For instance, Participant 13 (Focus Group 3, 19.01.2022) said, "I try to communicate more in Telegram, [which does not] always depend on me, but I feel more secure there [than in other messengers]." Notably, Telegram has a mixed reputation. From one perspective, "[the state] was not able to block it" (Participant 46, Focus Group 11, 01.02.2022), but on the other – "Telegram had blocked the Smart Voting channel exactly when it was needed the most" (Participant 49, Focus Group 13, 05.02.2022). Thus, some respondents use Signal (see Appendix 6, Figure 13), a more secure but less widespread messenger. For instance, Participant 11 (Focus Group 3, 19.01.2022) said, "I also have Signal […] [which, however, is] not used by anyone; […] there is still no critical mass." Similarly, although Gmail was a dominant post-service among the respondents, some also mentioned a more secure Proton. However, more secure instrument usage depended on engagement in activism or occupation. Overall, the study participants preferred independent from the state, encrypted, and secure communication via social media, messengers and email but utilized the instruments relevant to their personal situation.

Finally, the participants also mentioned their technological skills. On the institutional level, various projects utilize technology as a tool. For instance, Umnoe Golosovanie (Smart Voting) is the FBK project utilizing cyberspace to spread instructions to voters. Notably, it used not only a website but also a Telegram bot, which was blocked by the state. Telegram has also demonstrated the importance of IT skills on the individual level. Participant 41 (Focus Group 10, 01.02.2022) said it was "a wonderful Internet story when everyone was making small VPN services, teaching grandmothers how to use it." Notably, technological preparedness appears to be an essential component of societal cybersecurity practices. Some participants noted their lack of skills but added that they are willing to improve if needed and prepare for various scenarios. Hence, there is a general trend for learning to use technology with resistance purposes.

4.3.2. Non-Technological Practices

Non-technological practices rely on cyberspace as a communicative space while still utilizing its technological capabilities. Among these methods are non-resistance practices applied to minimize the adverse impact of cybercontrol. First, “no reaction” practices include ignoring or avoiding actions often based on risk calculation. Common phrases said by the study participants are “they will do it anyway”, “no one needs me [personally]”, “I am not the most prominent activist”, and “they already know/have everything [personal data]”. Some respondents remarked on their lack of personal experience with the negative consequences of cybercontrol, although they seemed to normalize cybercontrol with which they interact daily, e.g., censorship. Respondents also reported that randomness and ‘arbitrary’ laws make it impossible to predict which actions might be punished. For instance, Participant 25 (Focus Group 7, 28.01.2022) said, “it is unclear from where it will blow up”, and noted not seeing a reason to avoid using cyberspace in this situation. Hence, many participants do not react to practices of cybercontrol deeming them unavoidable.

The most widespread non-resistance practice is self-censorship, to which the stately cybercontrol compels the members of the liberal civil society. This practice includes deleting previously posted content and selecting what and how to write new content. The majority of the study participants admitted to employing self-censorship. Notably, the journalists are not immune to it, despite aiming to eradicate such a practice. For instance, Expert 7 (Interview 7, 22.10.2021) described that self-censorship impacted them when writing about terrorism as some phrases could be perceived as breaking the anti-terrorist law. At the same time, focus group participants wrote posts for organizations and reported that they follow stricter guidelines to avoid risky situations. Participant 34 (Focus Group 9, 31.01.2022) said, “in the work posts, I must apply some self-censorship […]. Accusing the mayor of theft is impossible. You need proof. Even if you have proofs – you still cannot do it.” Hence, stately cybercontrol leads to self-censorship among journalists and media activists.

Nevertheless, self-censorship is even more widespread among non-professionals and volunteers publishing on their personal pages. Respondents reported different degrees of self-censorship, ranging from not publishing content to selecting how to write. For instance, Participant 27 (Focus Group 7, 28.01.2022) said, “I openly write my opinion on

the Internet," but highlighted that they "know how to explain my position the way it sounds [compelling], but there are no words or phrases to which [the state] could find a fault." At the same time, Participant 16 (Focus Group 4, 20.01.2022), when speaking about online posts related to the protests, said, "I have to think deeply about the post, delete, cypher the date and time, so it would not be treated as a call [for participation]." Participant 37 (Focus Group 9, 31.01.2022) also considered changing the writing style as self-censorship.

Further, Participant 38 (Focus Group 10, 01.02.2022) underlined that self-censorship results from fear of such online actions as posting and reposting connected to offline consequences. Hence, some respondents reported avoiding posting on specific topics. Expert 1 (Interview 1, 27.03.2021) highlighted that "there is a significant effect of the self-censorship when people think […] [they] better not publish anything." Also, Expert 9 (Interview 9, 26.11.2021) stated that "when you want to write some post, now you think more on whether you need to write it on the Internet". Many participants adhered to the view that the "Internet remembers everything" and that any information put on it is available to the state. At the same time, some participants reported social supervision from friends and relatives, pressuring them to conform to the 'rules'. However, most respondents ignore this pressure or hide their actions from their relatives. Finally, Expert 10 (Interview 10, 30.01.2022) commented that "the requirements of the Russian laws are already stronger than any self-censorship". Thus, the decision for self-censorship stems from fear and the rational ground and allows for some resistance, albeit losing efficiency.

Nevertheless, there are more resistant non-technological practices. First, there is sousveillance, e.g., FBK investigations on corruption and electoral video surveillance. Regarding the latter, Expert 8 (Interview 8, 12.11.2021) spoke about their organization preparing an AI tool to speed up the analysis of elections video recordings. Although the state had restricted access to the video surveillance system for societal organizations to avoid it, this situation demonstrates the potential for growth in the liberal civil society. However, the state could not prevent all the resistance practices as few rely on the state as video sousveillance did. Among such resistant practices is "doing something [meaningful]", under which participants see actions of socio-political change rather than just minimizing their fear and other negative emotions, although the latter aim is also

present. For instance, Participant 45 (Focus Group 11, 01.02.2022) said, “when you are busy with a matter and with [this matter] invest in the fight […], you distract yourself by this action, and there is no time and strength left on fear.” This outlook was dominant among the study participants, informing their volunteering activities.

Another widespread practice is having possible “scenarios” in mind on how to act in a specific situation. For instance, Participant 39 (Focus Group 10, 01.02.2022) said, “I keep in mind possibilities, dangerous scenarios, [based on] the information from the media”, but remarked that these thoughts do not impact their behaviour as an activist. Participant 48 (Focus Group 12, 05.02.2022) added that “if anything happens, I know well enough, what I will do, how I will behave”. Moreover, Participant 34 (Focus Group 9, 31.01.2022) commented that they use “security protocol” developed by their organization. As a result, most respondents demonstrated awareness and preparedness for various “scenarios” with “security protocols”, helping them combat fear.

Furthermore, a majority of resistant non-technological practices relate to information distribution. Participants highlighted the importance of sharing their opinions, with information being the strongest positive association with the Internet (see Appendix 7, Figure 2). However, Participant 9 (Focus Group 2, 16.01.2022) said that “you share your life and position, but you still feel in danger and censored, because [the state] can send you to jail for the repost.” Further, Participant 26 (Focus Group 7, 28.01.2022) said that they “measure reposts and likes not from the standpoint that [the state] will not punish [for them], but if it not goes against [their] values and beliefs.” The study participants also commented on the stately disinformation, including trolls and bots (“kremlebots”), which create a background noise or attack users with oppositional views. The predominant strategy towards them is ignoring or banning, a defence practice, as respondents admitted they could not distinguish a “real person” from a paid troll. Most importantly, some appeared to brand any person with a contrary view as a “kremlebot”, contributing to the ‘bubble’. As a result, many participants highlighted their struggle against self-censorship and censorship but continued spreading the information.

Consequently, the liberal civil society conducts coordination and mobilization in cyberspace, which is essential due to the state completely controlling offline. For instance, Participant 2 (Focus Group 1, 15.01.2022) highlighted that “during the pandemic, the liberal civil society has acquired skills to coordinate human rights activities

without physical presence", adding that "if everything becomes even worse [than now], we will be able to sit in our kitchens and continue to do the same". Highlighting a possibility for decentralization, Expert 8 (Interview 8, 12.11.2021) noted that the state could not do anything with online social movements, despite numerous attempts because "there is no headquarters, no [defined] leadership." As a result, the liberal civil society uses cyberspace for coordination without creating a rigid structure.

Regarding mobilization, the participants observed opportunities for finding like-minded people and uniting with them. For instance, Participant 3 (Focus Group 1, 15.01.2022) said they met new people online and saw an influx of real-life friends joining the liberal civil society through cyberspace. Also, Participant 16 (Focus Group 4, 20.01.2022) added that in cyberspace, "people can find like-minded people, understand that they are not alone, that some of their beliefs are normal and not abnormal." Further, Expert 9 (Interview 9, 26.11.2021) highlighted that more and more people join protest and opposition chats, seeking truthful information because "they are touched by [important] event so much, that they want to find likeminded people to discuss it with them," adding that "on the wave of the Alexei [Navalny] return the number of participants in the chats has grown by three times." Also, Participant 3 (Focus Group 1, 15.01.2022) noted the constant growth of the community because of which "you can see that there are many of us which make [activism] easier for you." Moreover, the study participants cited support from the liberal civil society as a crucial factor giving them strength and protection. For example, Participant 48 (Focus Group 12, 05.02.2022) said that belonging to an organization or a movement is something that "gives [them] understanding that if something happens, [they] will not be left alone and will receive necessary help and support." Through support from friends, family, community, and solidarity, the study participants deal with the fear and adverse effects of cybercontrol.

Simultaneously, support connects to trust, which is essential for liberal civil society's growth and unity. Some participants reported non-resistant practices as searching for traitors inside the societal organizations. However, these instances are sparse, with most respondents addressing the opposite – building stronger horizontal connections. Notably, the respondents have discussed their participation in the study from this standpoint: they had agreed because they trusted their NGO. Although most respondents did not say they have a high level of trust, the consensus is that trust is a more

productive way of developing liberal civil society than searching for "agents of the state". For instance, Participant 15 (Focus Group 4, 20.01.2022) remarked that "there must be the presumption of trust between people in and out of our volunteering circle, so we can create higher quality social links and do a more effective job in the societal space."

Further, the participants have discussed "review" to confirm that the organization or a person could be trusted. For instance, Participant 39 (Focus Group 10, 01.02.2022) said that "[for them] it is important that these sites and people went through [their] review." Respondents mentioned "affiliation", "reputation", "visibility", "goals and values", and "actions" as criteria. Notably, most participants used the "I trust, but I check" principle (Participant 43, Focus Group 11, 01.02.2022). However, although they conducted the "review" themselves, there were positive comments on the screening methods used by organizations, saying that they trust their expertise. Hence, despite the "review", the participants trust their organizations, including the latter's members, even without meeting in real life. As a result, the members of the liberal civil society employ cyberspace to check their 'counteragents' or trust an already established 'trust network'.

Furthermore, the 'trust network' ensures the NGOs and social movements' survival through crowdfunding, possibly due to cyberspace as an instrument. For instance, Participant 38 (Focus Group 10, 01.02.2022) noted that "there is two-way trust" when speaking about their positive experience with collecting money for the needs of the movement. In other words, despite the financial question being not an easy one, the data shows that the participants view cyberspace as the only space available for gathering resources for the needs of the liberal civil society when the state closes other channels. As a result, cyberspace allows the members of the liberal civil society to establish and carry out activities. Despite the cybercontrol, they find novel ways to transform these opportunities into well-working institutions based on the practices mentioned above.

4.4. The Impact Assessment

As the liberal civil society reacts to cybercontrol with both resistance and non-resistance practices, the overall reaction cannot be measured quantitatively. Nevertheless, proxying it through the study participants' perceptions and cybersecurity practices, the liberal civil society appears to become stronger despite the increasing cybercontrol. Notably, the participants were not blind to the state having more resources. There were perceptions that the state was prevailing. For instance, Participant 51 (Focus

Group 13, 05.02.2022) said, “I do not see neither action nor reaction of the civil society. Everything fell apart in the last two years. The current network structures are the remains and not the upgraded systems that existed 2-3 years ago.”

Nevertheless, most of the study participants held a more positive view, seeing that the liberal civil society is still able to enhance itself. For instance, Participant 43 (Focus Group 11, 01.02.2022) said, “despite all the attempts to restrict civil society, I see a trend for self-organization, protecting their rights, and solidarity among certain people.” Further, Participant 52 (Focus Group 14, 08.02.2022) said, “people are trying to change something happening around them. […] I think that there are some [positive] changes”. Also, Expert 2 (Interview 2, 31.08.2021) rhetorically questioned, “if you are not an optimist, why would you even work here?” The participants talked highly about cyberspace. Participant 50 (Focus Group 13, 05.02.2022) noted that “the Internet is the only thing that can unite us and help us.” Hence, despite the significant cybercontrol of the state, the liberal civil society members had hope and a positive outlook.

Furthermore, another factor helping the liberal civil society is that with cyberspace leaving the territory of the Russian Federation does not mean leaving altogether. Notably, Expert 10 (Interview 10, 30.01.2022) stressed that this option is available only to activists and professionals whose physical location does not affect their activism. Nevertheless, some study participants have reported living abroad; others have acquaintances who immigrated but remain active with the liberal civil society through cyberspace. In other words, cyberspace allows the liberal civil society members to continue their activities even in ‘exile’, which is a widespread practice allowing for a stronger community.

Notwithstanding, I must address the information ‘bubble’ between the liberal civil society and other parts of the society. Many participants noted that their perceptions might be clouded by belonging to the former. For instance, Participant 32 (Focus Group 8, 29.01.2022) said that “some active part of the society becomes stronger [than before]” but then remarked that “we trust ours and do not trust ‘not ours’, but this separation ‘ours’/’not ours’ deforms [us]”. Expert 10 (Interview 10, 30.01.2022) also noted that the informational reality in ‘bubbles’ differs significantly, with Expert 1 (Interview 1, 27.03.2021) commenting that there is a high polarization when “these two realities spread out in different directions”. Moreover, polarization has strengthened with the participants seeing opposite opinions produced by trolls.

All in all, the primary hypothesis must be accepted. The empirical evidence has demonstrated that society becomes more insecure as it cannot prevail against the state, with its vast resources and growing pressure. Hence, the first part of the hypothesis holds. The respondents commented on growing cybercontrol leading to them feeling more insecure than before. Thus, the more cybercontrol the state exerts, the less cybersecure the liberal civil society becomes. At the same time, the second part of the hypothesis is also validated. With growing cybercontrol, the participants reported using more cybersecurity to protect themselves and their activities with the liberal civil society. Also, the findings provide for the spread of cybersecurity practices, learning and development of new instruments aimed at the resistance to the state. Hence, the more cybercontrol the state exerts, the more societal cybersecurity practices the liberal civil society develops, enhancing itself. As a result, the primary hypothesis of this thesis is accepted.

Moreover, accepting the primary hypothesis means that there indeed exists non-linearity in how cybercontrol affects liberal civil society. The latter weakens in the short term due to imposed restrictions. However, the development of societal cybersecurity practices leads to a potentially stronger liberal civil society in the long run. Most importantly, the state cannot wholly hinder this process entirely as it builds upon the existing trust network of connections within a community with deep distrust towards anything state-related. Notably, this window of opportunity is not yet utilized because the state's main actors do not use cyberspace as younger generations of Russians do, including the liberal civil society. As a result, the impact of cybercontrol on liberal civil society is not only direct and damaging but also indirect, providing an opportunity for growth and development.

As a result, I argue that the members of the liberal civil society do not use cyberspace solely as an instrument of 'escape' to protect themselves from the stately pressure but utilize it for practical actions going beyond mere survival. Despite participants highlighting the dangers they are expecting offline, they continue contributing to the liberal civil society and seek novel ways to do so. In other words, the prevalence of the resistance practices demonstrates that the liberal civil society uses cyberspace as a communicative space and an instrument to impact real-life politics. Although this influence is limited due to the authoritarian context, practical results go

beyond preserving the existing liberal civil society for its long-term development. Among these impacts, but not limited to them, are:

- Using crowdfunding to sponsor people after protests by bringing them food and water to the police department and paying the lawyers demonstrates growing societal support, increases trust and reduces atomization in the society.
- The Smart Voting project empowers the liberal civil society, gives a direction and has some success stories when people supported by it were elected over pro-state candidates.
- The 'visibility' granted by human rights NGOs protects people arrested and imprisoned from harsher treatment and promotes unity and solidarity among the actors: OVD-Info compiles lists of people detained during protests and publishes updates; activists write letters to political prisoners, signalling that there is sousveillance from the outside of the prison system.

To conclude with the answer to the research question, the Russian liberal civil society reacts to stately cybercontrol with protective measures and resistance. In other words, the liberal civil society seeks to mitigate the harm done to it by the state, albeit struggling. However, it also develops practices to circumvent the cybercontrol and continue joint action with other community members. The findings of the interviews and focus groups have demonstrated that there is still hope and strength among the respondents. Most importantly, the liberal civil society has a developed 'support' system for protection and help among its members. Moreover, the liberal civil society still resists the state and continues to grow through horizontal connections and various initiatives. As a result, the reaction of the Russian liberal civil society to the stately cybercontrol is complex, but it is far from inaction and succumbing to fear and compliance.

CONCLUSION

Although the conventional war has reemerged into the limelight, cyberspace remains a centre of an ongoing informational war. With the Russian Federation waging war in Ukraine, the state has not abandoned but dramatically increased its pressure on the opposition inside the country. Nevertheless, the Russian government has led the assault against the liberal civil society for many years, employing various cybercontrol practices to fear people into silence. Hence, this study attempted to provide an insight into how the liberal civil society in Russia reacts to stately cybercontrol. Notably, I did not aim to address the developments on the issue since February 24, 2022, but consider a timeframe from March 2021 to mid-February 2022. This way, the study sheds light on the Russian liberal civil society and its societal cybersecurity practices during the state preparation of the ground for the upcoming invasion.

In this thesis, I approached the research question from the perspective of the liberal civil society – a section of the Russian society independent from the state and fighting in opposition to it for procedural liberalism. Consequently, these people suffer the most pressure from the state, including imprisonment and significant control in all spheres of their lives, including in cyberspace. At the same time, the latter is the only sphere left for resistance in Russia, which means that the liberal civil society must find ways to utilize it for coordination, mobilization, distribution of information and other purposes without endangering its members even more. This study has distinguished such defensive and resistant practices of societal cybersecurity against stately cybercontrol.

Methodologically, this thesis has employed interviews and focus groups with experts and members of the liberal civil society. I have used qualitative content analysis to analyze this data. Overall, 62 people from various backgrounds and branches of the liberal civil society were able to speak with me – and each other – about their experiences with cybercontrol and cybersecurity. They discussed how the state seeks to intimidate them and stop them from activism. However, they also spoke about other members of the liberal civil society support and its evolution over time. Hence, the gathered data has demonstrated various reactions to the cybercontrol resulting in distinct practices of societal cybersecurity. However, there are common tendencies with people overcoming their fear of physical repercussions to continue their actions for the common good.

As a result, I argue that the Russian liberal civil society reacts to the stately cybercontrol with resistance – seeking ways to defend its members in the short run and developing practices aimed at long-term development and strengthening of the liberal civil society. In addition to protecting themselves and their close ones, its members are still looking for ways to improve the communication and spread of information, even when they must conform to the cybercontrol. Consequently, the Russian liberal civil society demonstrates significant resistance, even if acceptance, fear and a feeling of being overpowered exist in the Russian society in its entirety.

In other words, I confirm the primary hypothesis of this study as more cybercontrol leads to the weakening of the liberal civil society in the short perspective but results in additional strength to it through societal cybersecurity. In other words, the members of the liberal civil society protect themselves and seek other ways of "doing something [meaningful]." Although not all societal cybersecurity practices are strictly resistant, they demonstrate how the network survives, albeit losing efficiency due to the cybercontrol. The respondents highlighted that the state has more resources than society. However, they also believe that the state cannot utilize them efficiently and fully overpower the liberal civil society. Further, although participants note how the previously built resistance structures were destroyed, they also see positive trends within the society in which it grows and strengthens its ties, albeit with higher costs. As a result, I conclude that liberal civil society is becoming more potent despite cybercontrol.

Notwithstanding, the study has several limitations. First and foremost, the study does not include the Russian civil society in its entirety but limits the scope to the liberal civil society. Consequently, the results cannot be translated to Russian society due to its higher level of fragmentation. Moreover, they cannot be used for the analysis of the official Russian policies as the latter is guided not only by the group of people that is out of the scope of this investigation but which is also significantly different from the liberal civil society in its usage (or not usage) of cyberspace. Second, due to the high level of unwillingness to trust – which also impacts the liberalism of the liberal civil society – the participants of the study might not fully represent the whole liberal civil society. Nevertheless, I believe that in the autocratic context, there will always be bias towards people willing to talk with the researcher.

Regarding the timeframe, I want to comment on how the results apply to the developments after February 24, 2022. The data collection was finalized by the time when the state had increased the pressure on the liberal civil society to prevent the spread of information on the Russo-Ukrainian war. Most notably, most independent media outlets active in cyberspace were closed, and foreign social networks previously used by Russian users were blocked. Although I cannot comment on the impacts on the broader Russian society, the liberal civil society seemed to be prepared for increasing cybercontrol as the state used the same instruments seen as inefficient by the respondents a month prior. Without introducing new cybercontrol practices, it can only expect to slow the liberal civil society down without hindering its activities.

In other words, the existing societal cybersecurity practices appear to be transferrable to war censorship. For instance, using VPN was already widespread in the liberal civil society to circumvent blocks. Hence, access to the blocked sources could be gained through VPNs. Similarly, the Russian state still could not block Telegram despite being the primary communication instrument for the opposition. Hence, the communications among its members were not hindered by the state's actions. The liberal civil society already expected an increase in cybercontrol. I hypothesise that despite the shift being more significant than expected, the liberal civil society was still prepared well. As a result, the study on this natural experiment administered by the Russian government could be a direction for future research on Russian societal cybersecurity.

These results are valuable for academia and policy-makers as they provide qualitative insight into the Russian liberal civil society. As the data collected during wartime has low validity, this empirical investigation is invaluable. When speaking up against authority equates to a prison sentence, we cannot expect people to be ready to share their experiences with the stately cybercontrol. The findings acquired from this – latest possible – data provide a better understanding of the Russian liberal civil society processes. With the conclusion of this thesis being that it grows in strength, we can only expect it to be tested by the current events. The study might be helpful for policy or academic purposes by the actors seeking to understand or support the liberal civil society. However, it should not be of any use to the Russian state, which, I assert, cannot stop societal cybersecurity practices from existing. I conclude that with more pressure, the Russian liberal civil society also has more potential, even in the darkest times.

BIBLIOGRAPHY

Abu-Laban, Y. (2012). The politics of surveillance. *Routledge Handbook of Surveillance Studies*, 420-27.

Akbari, A., & Gabdulhakov, R. (2019). Platform surveillance and resistance in Iran and Russia: The case of Telegram. *Surveillance & Society, 17*(1/2), 223-231.

Akhmadieva, R. S., Ignatova, L. N., Bolkina, G. I., Soloviev, A. A., Gagloev, D. V., Korotkova, M. V., & Burenina, V. I. (2018). An attitude of citizens to state control over the internet traffic. *Eurasian J. Anal. Chem*, *13*(1).

Ashenden, D. M., Coles-Kemp, L., & O'Hara, K. (2018). Why should I? Cybersecurity, the security of the state and the insecurity of the citizen. *Politics and Governance*, *6*(2), 41-48.

Ball, K., Haggerty, K., & Lyon, D. (2012). Routledge handbook of surveillance studies. Routledge.

Balzacq, T., & Cavelty, M. D. (2016). A theory of actor-network for cyber-security. *European Journal of International Security*, *1*(2), 176-198.

Barbour, R. (2008). *Doing focus groups*. Sage.

Batko, R. (2016). Panopticon–cybercontrol in liquid modernity: What does control really mean. *Strategic Imperatives and Core Competencies in the Era of Robotics and Artificial Intelligence*, *1*.

Bauman, Z., & Lyon, D. (2013). *Liquid surveillance: A conversation*. John Wiley & Sons.

Baur, D., & Schmitz, H. P. (2012). Corporations and NGOs: When accountability leads to co-optation. *Journal of Business Ethics, 106*(1), 9-21.

Bebber, R. J. (2017). Cyber power and cyber effectiveness: An analytic framework. *Comparative Strategy, 36(*5), 426-436.

Biennier, F., & Favrel, J. (2005). Collaborative business and data privacy: Toward a cyber-control?. *Computers in Industry, 56*(4), 361-370.

Bigo, D. (2001). The Möbius ribbon of internal and external security (ies). *Identities, borders, orders: Rethinking international relations theory*, *18*, 91-116.

Bigo, D., Carrera, S., Hernanz, N., Jeandesboz, J., Parkin, J., Ragazzi, F., & Scherrer, A. (2013). Mass surveillance of personal data by EU member states and its compatibility with EU law. *Liberty and Security in Europe Papers*, (61).

Bigo, D., Guild, E., & Kuskonmaz, E. M. (2021). Obedience in times of COVID-19 pandemics: a renewed governmentality of unease?. *Global Discourse: An interdisciplinary journal of current affairs, 11(*1-2), 1-2.

Bilgin, P. (2003). Individual and societal dimensions of security. *International Studies Review*, *5*(2), 203-222.

Bogard, W. (2012). Simulation and post-panopticism. In *Routledge handbook of surveillance studies* (pp. 3-37). Routledge.

Broeders, D. (2007). The new digital borders of Europe: EU databases and the surveillance of irregular migrants. *International Sociology*, *22*(1), 71-92.

Browning, C. S., & Joenniemi, P. (2017). Ontological security, self-articulation and the securitization of identity. *Cooperation and conflict*, *52*(1), 31-47.

Bruno, F. (2012). Surveillance and participation on Web 2.0. In *Routledge handbook of surveillance studies* (pp. 343-351). Routledge.

Budnitsky, S., & Jia, L. (2018). Branding Internet sovereignty: Digital media and the Chinese–Russian cyberalliance. *European Journal of Cultural Studies, 21*(5), 594–613.

Burton, J., & Lain, C. (2020). Desecuritising cybersecurity: towards a societal approach. *Journal of Cyber Policy*, *5*(3), 449-470.

Carrapico, H., & Barrinha, A. (2017). The EU as a coherent (cyber) security actor?. *JCMS: Journal of Common Market Studies, 55*(6), 1254-1272.

Castells, M. (2015). *Networks of outrage and hope: Social movements in the Internet age*. John Wiley & Sons.

Ceyhan, A. (2012). Surveillance as biopower. *Routledge handbook of surveillance studies*, 36-46.

Christou, G. (2018). The challenges of cybercrime governance in the European Union. *European Politics and Society, 19*(3), 355-375.

Claessen, E. (2020). Reshaping the internet–the impact of the securitisation of internet infrastructure on approaches to internet governance: the case of Russia and the EU. *Journal of Cyber Policy, 5*(1), 140-157.

Daucé, F. (2015). The duality of coercion in Russia: cracking down on "foreign agents". *Demokratizatsiya: The Journal of Post-Soviet Democratization*, *23*(1), 57-75.

Deibert, R. (2015). Authoritarianism goes global: cyberspace under siege. *Journal of Democracy*, *26*(3), 64-78.

Deibert, R. (2016). Cyber-security. In *Routledge handbook of security studies* (pp. 186-196). Routledge.

Deibert, R. (2018). Trajectories for future cybersecurity research. In *The Oxford Handbook of International Security*.

Della Porta, D., & Keating, M. (2008). How many approaches in the social sciences? An epistemological introduction.

Dollbaum, J. M. (2020). Social policy on social media: How opposition actors used Twitter and VKontakte to oppose the Russian pension reform. *Problems of Post-Communism*, 1–12.

Dunn Cavelty, M. (2018). Europe's cyber-power. *European Politics and Society*, *19*(3), 304-320.

Elmer, G. (2012). Panopticon-discipline-control. In *Routledge handbook of surveillance studies* (pp. 21-29). Routledge.

Epifanova, A. (2020). Deciphering Russia's "Sovereign internet law": Tightening control and accelerating the Splinternet.

Ermoshina, K., & Musiani, F. (2017). Migrating servers, elusive users: Reconfigurations of the Russian Internet in the post-Snowden era. *Media and Communication, 5*(1), 42-53.

Ermoshina, K., & Musiani, F. (2021). The Telegram ban: How censorship "made in Russia" faces a global Internet. *First Monday, 26*(5).

Ermoshina, K., Loveluck, B., & Musiani, F. (2022). A market of black boxes: The political economy of Internet surveillance and censorship in Russia. *Journal of Information Technology & Politics, 19*(1), 18-33.

Fasana, K. G. (2018). Another manifestation of cyber conflict: Attaining military objectives through cyber avenues of approach. *Defence Studies, 18*(2), 167-187.

Finnemore, M. (2018). Ethical dilemmas in cyberspace. *Ethics & International Affairs, 32*(4), 457-462.

Fominaya, C. F. (2014). *Social movements and globalization: How protests, occupations and uprisings are changing the world*. Macmillan International Higher Education.

Foucault, M. (1975). Surveiller et punir. *Paris*, *1*, 192-211.

Fujii, L. A. (2012). Research ethics 101: Dilemmas and responsibilities. *PS: Political Science & Politics, 45*(4), 717-723.

Gabdulhakov, R. (2020). (Con) trolling the Web: Social media user arrests, state-supported vigilantism and citizen counter-forces in Russia. *Global Crime, 21*(3-4), 283-305.

Garrido, M. V. (2015). Contesting a biopolitics of information and communications: The importance of truth and sousveillance after Snowden.

Glen, C. M. (2014). Internet governance: territorializing cyberspace?. *Politics & Policy, 42*(5), 635-657.

Goldstein, D. M. (2010). Toward a critical anthropology of security. *Current Anthropology*, *51*(4), 487-517.

Greitens, S. C. (2020). Surveillance, security, and liberal democracy in the post-COVID world. *International Organization, 74*(S1), E169-E190.

Hama, H. H. (2017). State security, societal security, and human security. *Jadavpur Journal of International Relations, 21*(1), 1-19.

Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International studies quarterly*, *53*(4), 1155-1175.

Hemment, J. (2012). Nashi, youth voluntarism, and Potemkin NGOs: Making sense of civil society in post-Soviet Russia. *Slavic Review, 71*(2), 234-260.

Holbraad, M., & Pedersen, M. A. (Eds.). (2013). *Times of security: ethnographies of fear, protest and the future*. Routledge.

Huysmans, J. (2006). *The politics of insecurity: Fear, migration and asylum in the EU*. Routledge.

Jayawardane, S., Larik, J. E., & Kaul, M. (2016). Governing cyberspace: Building confidence, capacity and consensus. *Special Section: Governing Cyberspace: Building Confidence, Capacity and Consensus*, *7*(1).

Jensen, B., Valeriano, B., & Maness, R. (2019). Fancy bears and digital trolls: Cyber strategy with a Russian twist. *Journal of Strategic Studies*, 42(2), 212-234.

Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2), 7-40.

Klein, J., & Hossain, K. (2020). Conceptualising human-centric cyber security in the Arctic in light of digitalisation and climate change. *Arctic Review*, *11*, 1-18.

Kohn, M. (2010). Unblinking: Citizens and subjects in the age of video surveillance. *Constellations, 17*(4), 572-588.

Kondakov, A. (2019). The censorship "propaganda" legislation in Russia. *State-sponsored homophobia.*

Kukkola, J., & Ristolainen, M. (2018). Projected territoriality. *Journal of Information Warfare, 17*(2), 83-100.

Kurowska, X. (2020). What does Russia want in cyber diplomacy? *Governing Cyberspace: Behaviour, Power and Diplomacy*, 85-106.

Lambach, D. (2020). The territorialization of cyberspace. *International Studies Review, 22*(3), 482-506.

Lewis, D. (2013). Civil society and the authoritarian state: Cooperation, contestation and discourse. *Journal of Civil Society, 9*(3), 325-340.

Lewis, D., Kanji, N., & Themudo, N. S. (2020). *Non-governmental organizations and development*. Routledge.

Limonier, K., Douzet, F., Pétiniaud, L., Salamatian, L., & Salamatian, K. (2021). Mapping the routes of the Internet for geopolitics: the case of Eastern Ukraine. *First Monday*.

Litvinenko, A. (2020). Social media in Russia: Between state and society. *Media Capture, 9*(258), 12.

Ljubownikow, S., Crotty, J., & Rodgers, P. W. (2013). The state and civil society in Post-Soviet Russia: The development of a Russian-style civil society. *Progress in Development Studies, 13*(2), 153-166.

Lokot, T. (2018). Be safe or be seen? How Russian activists negotiate visibility and security in online resistance practices. *Surveillance & Society*, 16(3), 332-346.

Lonkila, M., Shpakovskaya, L., & Torchinsky, P. (2021). Digital activism in Russia: The evolution and forms of online participation in an authoritarian state. In *The Palgrave Handbook of Digital Russia Studies* (pp. 135-153). Palgrave Macmillan.

Luger, J. (2020). Planetary illiberalism and the cybercity-state: n and beyond territory. *Territory, Politics, Governance, 8*(1), 77-94.

Lyon, D. (1994). *The electronic eye: The rise of surveillance society*.

Lyon, D. (2018). *The culture of surveillance: Watching as a way of life*. John Wiley & Sons.

Lyon, D., & Zureik, E. (Eds.). (1996). *Computers, surveillance, and privacy*.

Makarychev, A., & Medvedev, S. (2015). Biopolitics and power in Putin's Russia. *Problems of Post-communism, 62*(1), 45-54.

Manokha, I. (2018). Surveillance, panopticism, and self-discipline in the digital age. *Surveillance & Society, 16*(2), 219-237.

Maréchal, N. (2017). Networked authoritarianism and the geopolitics of information: Understanding Russian Internet policy. *Media and Communication, 5*(1), 29-41.

Marx, G. T. (2001). Censorship and secrecy, social and legal perspectives. *International Encyclopedia of the Social and Behavioral Sciences.*

Marx, G. T. (2005). Camerica? Two cheers (or less) for the indiscriminate spread of video cameras in public areas. *ID Track Mix*.

Marx, G. T. (2012). Agents provocateurs as a type of faux activist. *Encyclopedia of Social and Political Movements.*

Nisbet, E. C., Kamenchuk, O., & Dal, A. (2017). A psychological firewall? Risk perceptions and public support for online censorship in Russia. *Social Science Quarterly, 98*(3), 958-975.

Nye, J. (2011). Nuclear lessons for cyber security?. *Strategic Studies Quarterly, 5*(4), 18–38.

O'Connor, H., & Madge, C. (2017). Online interviewing. *The SAGE Handbook of Online Research Methods*, 2, 416-434.

Offe, C. (2001). Political liberalism, group rights, and the politics of fear and trust. *Studies in East European Thought*, 167-182.

Onuch, O., Mateo, E., & Waller, J. G. (2021). Mobilization, mass perceptions, and (dis) information: "New" and "old" media consumption patterns and protest. *Social Media+ Society, 7*(2).

Ormrod, D., & Turnbull, B. (2016). The cyber conceptual framework for developing military doctrine. *Defence Studies*, 16(3), 270-298.

Piotrowski, G. (2020). Civil society in illiberal democracy: the case of Poland. *Politologický časopis-Czech Journal of Political Science, 27*(2), 196-214.

Ramesh, R., Raman, R. S., Bernhard, M., Ongkowijaya, V., Evdokimov, L., Edmundson, A., & Ensafi, R. (2020, January). Decentralized control: A case study of Russia. In *Network and Distributed Systems Security (NDSS) Symposium 2020*.

Rudenkin, D. V., & Loginov, A. V. (2019, December). Transformation of political process in digital society: case of contemporary Russia. In *International Scientific and Practical Conference on Digital Economy (ISCDE 2019)* (pp. 623-628). Atlantis Press.

Rudnik, A. (2020). Why do bloggers keep silent? Self-censorship in social media: cases of Belarus and Russia.

Saldaña, J. (2021). *The coding manual for qualitative researchers*. Sage.

Schou, J., & Hjelholt, M. (2019). Digital state spaces: state rescaling and advanced digitalization. *Territory, Politics, Governance, 7*(4), 438-454.

Schreier, M. (2012). *Qualitative content analysis in practice*. Sage Publications.

Semetko, H. A., & Krasnoboka, N. (2003). The political role of the Internet in societies in transition: Russia and Ukraine compared. *Party Politics*, *9*(1), 77-104.

Shackelford, S. J., Sulmeyer, M., Deckard, A. N. C., Buchanan, B., & Micic, B. (2017). From Russia with love: Understanding the Russian cyber threat to US critical infrastructure and what to do about it. *Neb. L. Rev.*, *96*, 320.

Stanley, L. (2016). Using focus groups in political science and international relations. *Politics, 36*(3), 236-249.

Sternberg, E. (2010). NGOs vs civil society: Reflections on the illiberal, the illegitimate and the unaccountable. *Economic Affairs, 30*(3), 22-28.

Stukal, D., Sanovich, S., Bonneau, R., & Tucker, J. A. (2022). Why botter: How pro-government bots fight opposition in Russia. *American Political Science Review*, 1-15.

Švedkauskas, Ž., & Maati, A. (2021). Long-term prescription? Digital surveillance is here to stay. *Mezinárodní Vztahy, 56*(4), 105-118.

Taylor, B. D. (2006). Law enforcement and civil society in Russia. *Europe-Asia Studies, 58*(2), 193-213.

Toepfl, F. (2018). From connective to collective action: internet elections as a digital tool to centralize and formalize protest in Russia. *Information, communication & society*, *21*(4), 531-547.

Van de Donk, W., Loader, B. D., Nixon, P. G., & Rucht, D. (Eds.). (2004). *Cyberprotest: New media, citizens and social movements*. Routledge.

Vargo, C. J., & Hopp, T. (2020). Fear, anger, and political advertisement engagement: A computational case study of Russian-linked Facebook and Instagram content. *Journalism & Mass Communication Quarterly, 97*(3), 743-761.

Vendil Pallin, C. (2017). Internet control through ownership: The case of Russia. *Post-Soviet Affairs, 33*(1), 16-33.

Vesselkov, A., Finley, B., & Vankka, J. (2020, July). Russian trolls speaking Russian: Regional Twitter operations and MH17. In *12th ACM Conference on Web Science* (pp. 86-95).

Voorhoof, D. (2018). Savva Terentyev v. Russia: criminal conviction for inciting hatred against the police violated a blogger's freedom of expression. *Strasbourg Observers Blog*, 5.

Weller, T. (2012). The Information state: A historical perspective on surveillance. In *Routledge Handbook of Surveillance Studies* (pp. 57–63). Routledge.

Whyte, C. (2018). Dissecting the digital world: A review of the construction and constitution of cyber conflict research. *International Studies Review, 20*(3), 520-532.

Willett, M. (2019). Assessing cyber power. *Survival, 61*(1), 85-90.

Wober, M., & Gunter, B. (1988). *Television and social control*. Avebury.

Wollebæk, D., Karlsen, R., Steen-Johnsen, K., & Enjolras, B. (2019). Anger, fear, and echo chambers: The emotional basis for online behavior. *Social Media+ Society, 5*(2), 2056305119829859.

Yatsyk, A. (2019). Biopolitical conservatism in Europe and beyond: The cases of identity-making projects in Poland and Russia. *Journal of Contemporary European Studies, 27*(4), 463-478.

Zeng, J., Stevens, T., & Chen, Y. (2017). China's solution to Global Cyber Governance: unpacking the domestic discourse of "Internet Sovereignty". *Politics & Policy, 45*(3), 432-464.

Zhelnina, A. (2020). The apathy syndrome: How we are trained not to care about politics. *Social Problems, 67*(2), 358-378.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

APPENDICES

Appendix 1

Interviewer Guide for In-Depth Interviews

Pre-Interview

1. Research the interviewee: personal information ☐, organization ☐
2. Initial message: prepare ☐, send ☐
3. Arrange meeting: time and mode ☐, online environment settings ☐
4. Consent form: prepare ☐, send ☐
5. Interview Guide: review and adapt for the specific interview if needed ☐
6. Prepare note-taking materials ☐.
7. If possible, send a reminder about the interview 1-2 hours prior ☐.
8. Arrive at the interview 5-10 minutes earlier ☐.

Interview

1. If the interviewee did not show up in time, follow up before 30 min. ☐.
2. Turn on the recording while notifying the interviewee ☐.

Section	**Timing**	**Stage**	**Preliminary questions**
Initial greeting	2 min.	Ice breaker	"Thank you for agreeing to meet with me!"
Introduction section	2 min.	Recording information	"I will be recording our interview. The recording will not be used for any other reason but transcription."
	5 min.	Consent information	"I do not seek sensitive or confidential information. Please read and sign the consent form. If you have any questions or want to add something to the consent form, we can do it at any interview stage."
	3 min.	Intro to the research	"My study looks into how the society reacts to the control of the state on the Internet: censure, access restrictions."
Initial questions	5 min.	Personal questions	"First, could you, please, tell me about yourself: your background?"

	5 min.	Institutional questions	"Could you tell me with which issues your organization works?" "On which topics do you focus?"
Specific questions	10 min.	Control questions	"Could you please characterize the overall situation with state's control in Russia?"
	10 min.	Cyberspace questions	"Is the situation on the Internet different?"; "Are there specific trends?"; "How the situation changed in 2020-2021?"
	10 min.	Cybercontrol questions	"Which specific instruments of control by the state on the Internet, you know?";
	15 min.	Feelings and Practices questions	"Do you deal with these issues professionally and personally?"; "Fear: Are you afraid of acting on the Internet?"; "Self-Censure: Do you detect changes in your behaviour?" "Do you use any cybersecurity instruments?" "Trust: Do you trust online [media, social media]?"; "Did you have negative experiences with the state online?"
Extra questions	10 min.	Spillover questions	"Do you think [know] about any similar effects from the RuNet on your [friends/colleagues] abroad? Are they able to remain a part of the civil society?"
Concluding questions	5 min.	Closing remarks	"How do you think the situation evolves – does cyberspace make the society stronger, or there are only negative effects of cybercontrol?" "Thank you!"
Off-the-record	-	-	Remind about the consent form or sign it right away if possible. Ask for a reference from another interviewee (snowballing).

3. Stop the recording (before off-the-record) ☐.

Post-Interview

1. Apply sensitivity and confidentiality settings discussed with the interviewee ☐.
2. Transcribe recording ☐.
3. Send transcripts to the interviewee if agreed ☐.
4. Collect consent form if not signed during the interview ☐.
5. Analyse data while keeping up with the confidentiality/sensitivity agreements.
6. Keep in touch with the interviewee in case of publication.

Appendix 2

Interview Consent Form (ENG)

CONSENT FORM

INFORMED AND VOLUNTARY CONSENT

I have been told about the purpose and topic of the interview and how my responses will be used.

I have been able to ask questions about the interview, and they have been answered.

I understand that any attributed quotes from the interview will only be used for study projects or published academic work. If I have agreed to conduct the interview anonymously, I understand that quotes will be attributed to "a party source familiar with the situation".

I understand that I am not required to answer any of the questions, and I can withdraw from the interview at any time.

I agree to participate in this interview and to it being digitally recorded.

Name: (print name) _____

Signature: _____ **Date**:

Appendix 3

Moderator Guide for Focus Groups

Pre-Focus group

1. Compile a list of participants ☐
2. Select participants randomly ☐
3. Contact participants ☐
4. Compile groups of 4–5 people ☐
5. Arrange meeting: environment ☐, time ☐
6. Prepare space for the meeting: materials ☐
7. Send a reminder to the participants 1-2 hours before the FG ☐

Focus group (1 hour 00 minutes – 1 hour 30 minutes)

Section	**Appr. time**	**Stage**	**Preliminary question**
Initial greeting	5 min.	Waiting/greeting	"Thank you for coming!";
Introduction section	1 min.	Moderator introduction	"Hello to everyone! Welcome, my name is Mariia Maksimova, and I will be moderating today's session.";
	1 min.	Recording information	"This focus group will be recorded as our research will need all that will be discussed today. However, these tapes will only be accessible to me and destroyed later. Do you have any questions?"
	2 min.	Consent information	"You were given a consent form to read through earlier. Do you have any questions regarding it?"
	2 min.	Confidentiality information	"The topics which we will discuss today might be controversial for some. Because of this, no personal information must go beyond this room."

	3 min.	Ground rules	"Finally, we need to establish some ground rules of how this focus group will go. First, everyone should participate. We will be discussing questions that do not have right or wrong answers. However, they do have *your* answers which are always correct. So, try to be as honest with the group as possible. Secondly, remember about privacy. Third, please speak up only when addressed to make things easier and more organised: raise your hand, and I will call you. However, if you need to ask something or tell us, write in the chat. Thank you!"
Initial questions	5 min.	Basic experience	"Let us introduce each other and comment on how long you have been volunteering and how much you use the Internet in your daily, professional, and volunteering lives?"
Overall Questions	10 min.	Associations and Safety level Mentimeter https://www.menti.com/zaz9zyxb1q SL. 1-2	"As most of us spend the Internet a lot of our time, let us think about what we associate Internet." (1) "Also, do you feel safe on the Internet?" (2)
Specific questions	10 min.	Knowledge Mentimeter https://www.menti.com/iieyu9egph SL. 1-2	"What do you know about control of the state on the Internet? Maybe you or your relatives/friends somehow interacted with it?"
	10 min.	Feelings – Fear Mentimeter	"How do you feel while being on the Internet? Did these feelings change

		https://www.menti.com/shaoct73eo SL. 1	over time or because of the control by the state we just discussed?" "Do you feel fear? How do you manage it? Is it more offline than online?" "Do you use technology to increase your security?" "Do you use non-tech methods to increase your security?"
	10 min.	Feeling – Trust Mentimeter https://www.menti.com/shaoct73eo SL. 2	"Do you trust other people on the Internet? Media? How do you decide to whom you can trust?"
Concluding questions	5 min.	Balance questions	"What prevails in the end? Trust grows vs fear => society stronger?" "Does society only answer or also resist the state?"
Ending section	1 min.	Thanking	"Thank you for your participation! If you have any questions or comments for us, feel free to approach us."

Post-Focus group

1. Sensitivity and confidentiality: apply agreed settings ☐
2. Transcribe recording ☐
3. Keep in touch with participants if needed ☐

Appendix 4

Consent Form for Focus Groups (ENG)

University of Tartu

Societal Security under Cybercontrol: the Case of Russia

Principal Investigator: Mariia Maksimova

What is the goal of this focus group?

You have been asked to partake in the study focused on how Russian society perceives the control of the state on the Internet. Thank you for agreeing to participate! This study will be beneficial in understanding how Russian society develops and how the state impacts it.

Why me?

You have been asked to participate in this focus group as you are a part of the Russian society and have valuable insights on the question because of your work [volunteering] with [NGO].

Can I decline participation?

Yes, you are free to stop partaking in the focus group at any point. You might decide to decline before the beginning or stop at any point during the interview itself. You also are free not to answer specific questions or can ask to exclude some answers from further consideration.

Is it dangerous for me?

We understand that you are taking some risks when participating in this focus group. Due to the pressure under which Russian society is right now, it is an understandable concert. However, we want to ensure that any information you provide for us will not be connected to you.

Will the focus group be recorded?

Yes, the focus group will be audio recorded. However, the recordings will be erased after the research is completed. Moreover, we will not use your name or anything that might point at you in the project. This information will be available only to the research group.

If you have any questions, raise them during the initial stage during the focus group or contact us via phone [phone number] or e-mail [e-mail].

If you agree to partake in the focus group, please tick the box and sign the consent form.

☐ Yes, I, (*name or alias*) _____, agree to participate in the focus group study.

Signature: _____ Date:_____

Appendix 5

Confidentiality Agreement for Focus Groups

Confidentiality Agreement

This additional form is meant to ensure that the information obtained during the focus group will not be used outside of the research project by any focus group participant, including the moderator, assistant of the moderator, and focus group participants.

By signing the confidentiality agreement, you confirm that you are not to disclose the information discussed during the focus group in any way, including publicly. You will not communicate it in any way (verbally or in written form) outside of the focus group or the research project.

Name:_____

Signature:_____

Date:_____

Appendix 6

Focus Group Participants Sociodemographic Data (Pre-Survey)

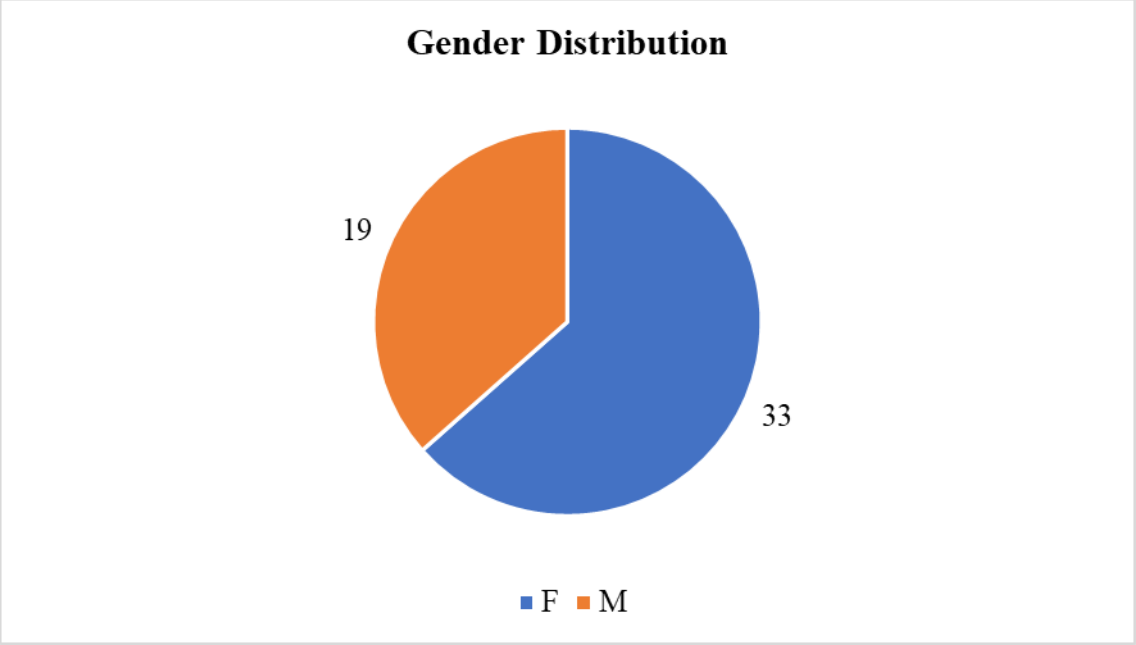

Figure 8. Gender Distribution for Focus Group Participants

Source: Focus Groups data (pre-survey)

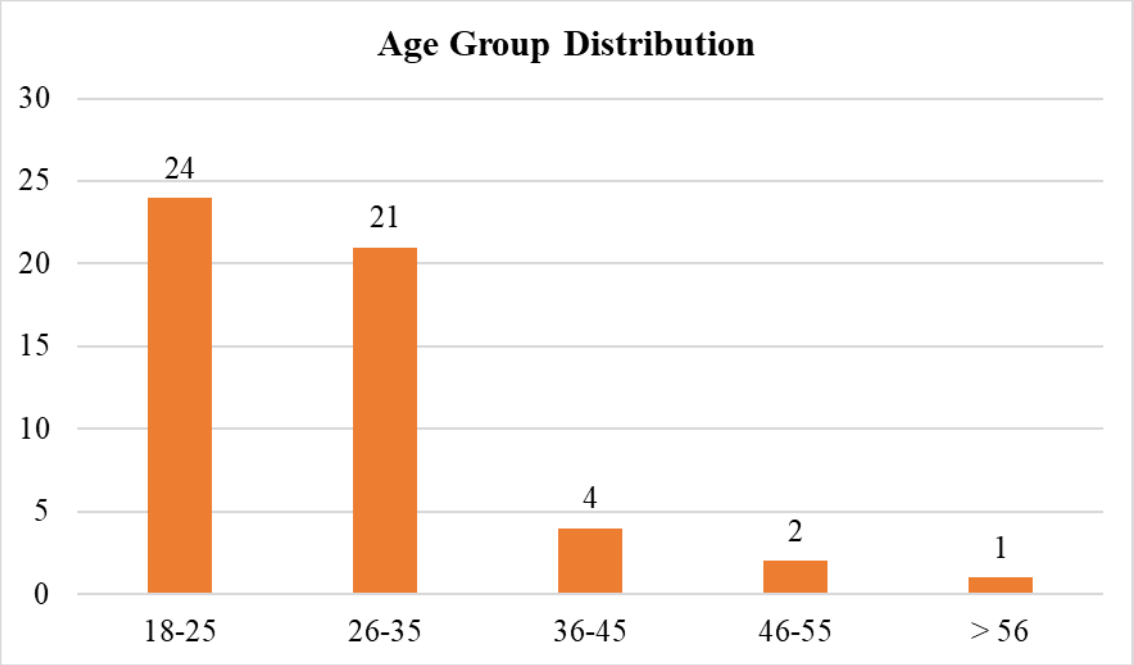

Figure 9. Age Group Distribution for Focus Group Participants

Source: Focus Groups data (pre-survey)

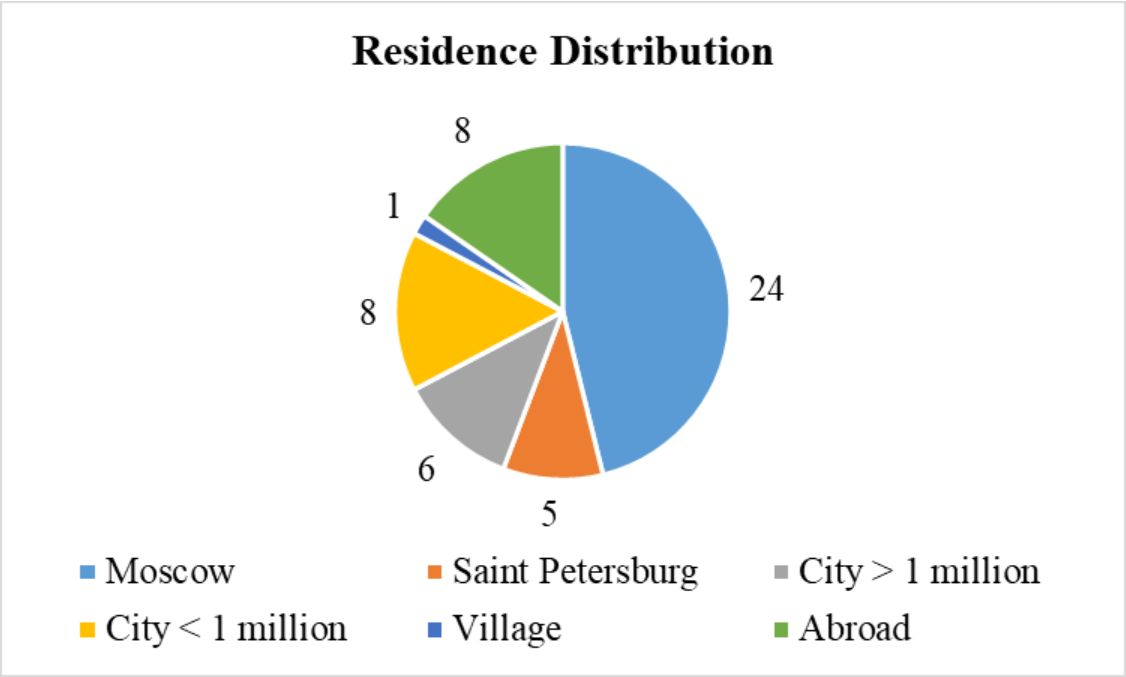

Figure 10. Residence Distribution for Focus Group Participants

Source: Focus Groups data (pre-survey)

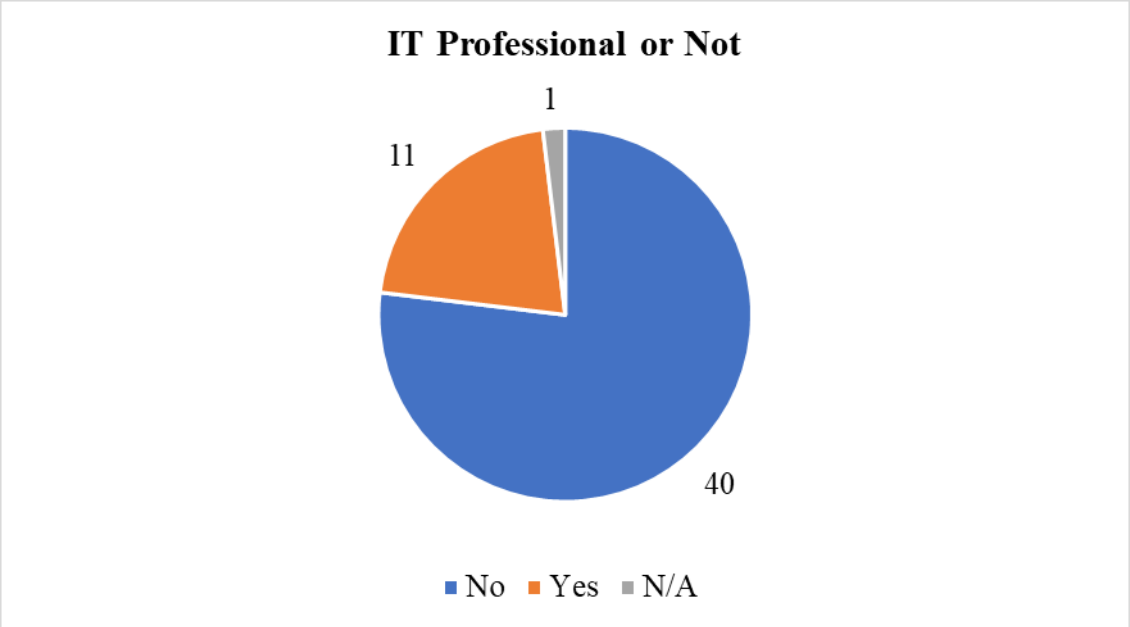

Figure 11. Share of IT Professionals among Focus Group Participants

Source: Focus Groups data (pre-survey)

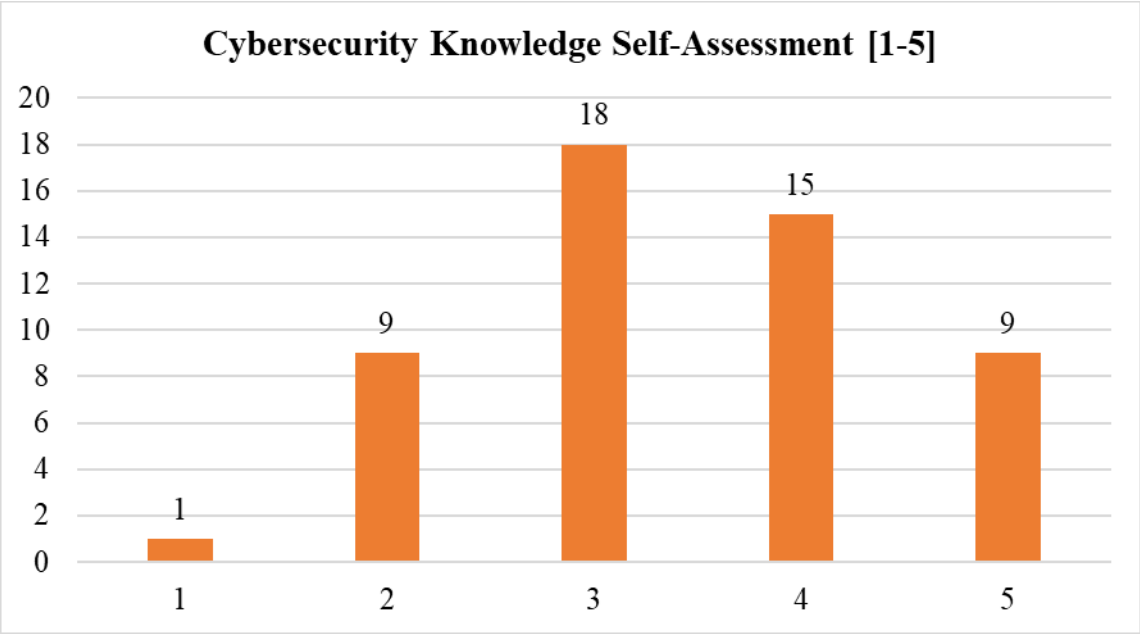

Figure 12. Cybersecurity Knowledge Self-Assessment by the Focus Group Participants

Source: Focus Groups data (pre-survey)

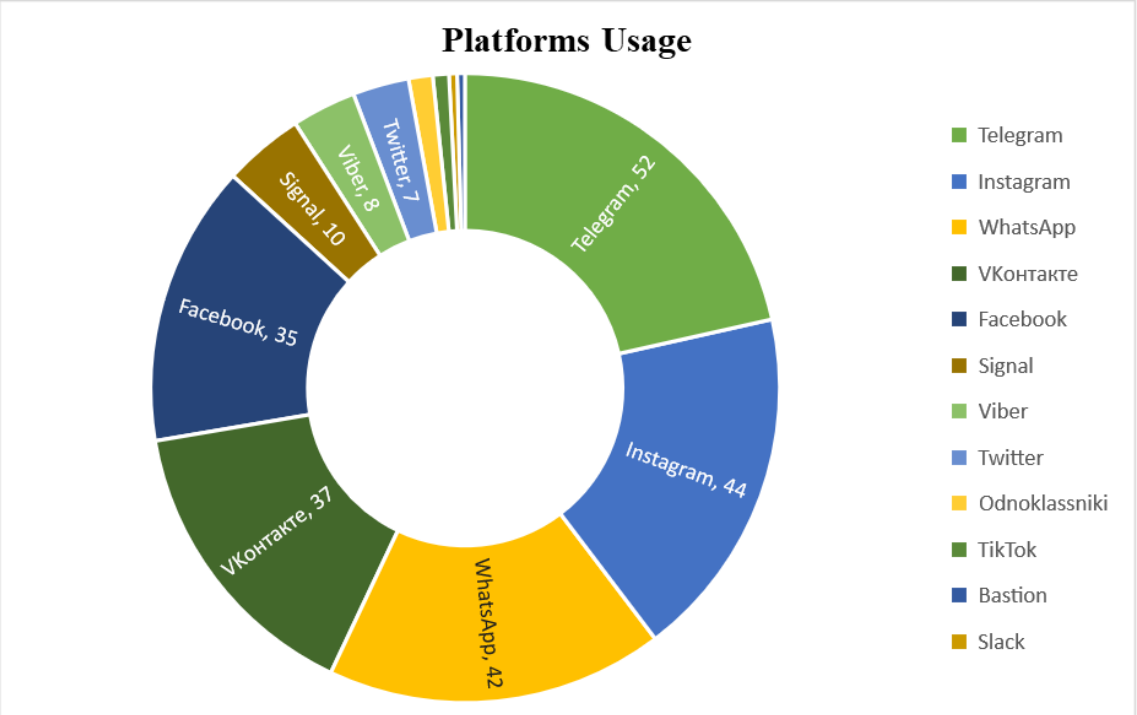

Figure 13. Usage of Web Platforms (Social Networks and Messengers) among Focus Group Participants

Source: Focus Groups data (pre-survey)

Supplementary Materials (Menti) for Focus Groups and Their Results

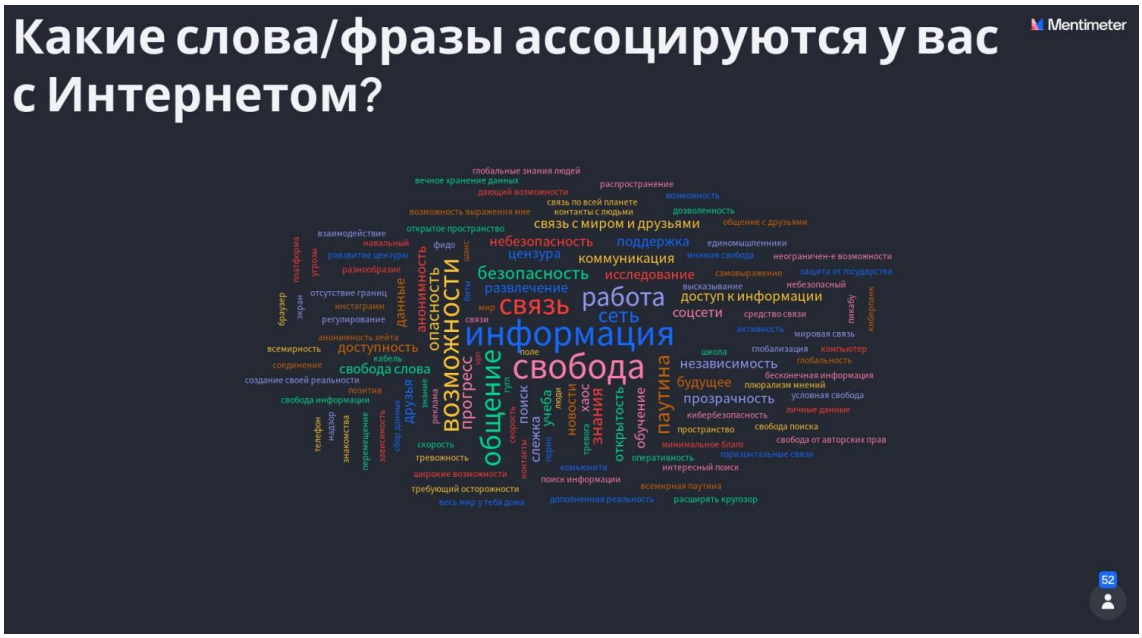

Figure 2. Associations

Source: Focus Group data

Figure 3. Perception of Insecurity/Security

Source: Focus Group data

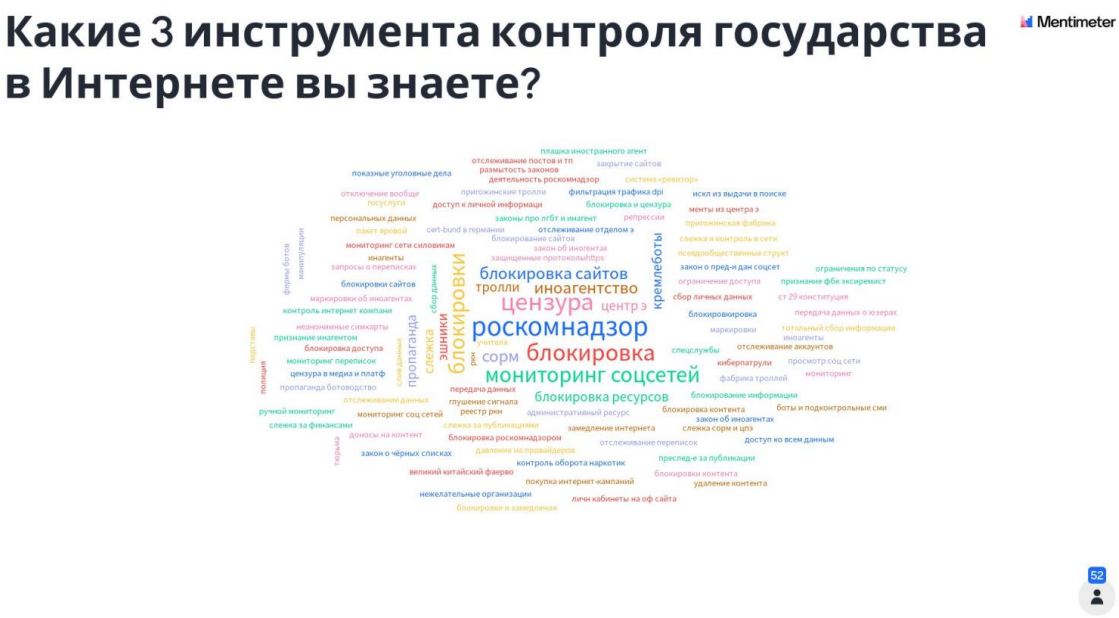

Figure 4. Cybercontrol practices

Source: Focus Group data

Figure 5. Personal/Related stories

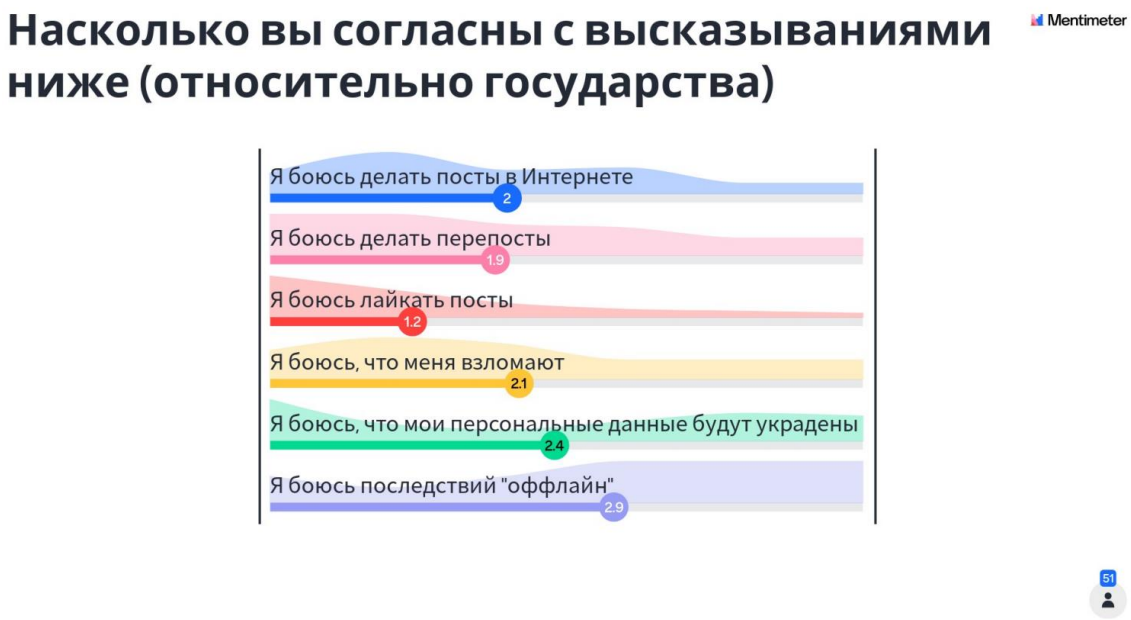

Figure 6. Fear

Source: Focus Group data

Figure 7. Trust

Source: Focus Group data

Appendix 8

List of Interviews

Interviewee			Overall Length	Format	Language
Code	**Organization**	**Date**			
Expert 1	Civil rights Human rights Media	27.03.2021 06.04.2021	01:37:00	Online, Zoom	Russian
Expert 2	Civil rights Human rights	31.08.2021	00:31:30	Online, Zoom	Russian
Expert 3	Civil rights Human rights	27.09.2021	00:41:04	Online, Zoom	Russian
Expert 4	Political mov.	05.10.2021	00:27:00	Online, Zoom	Russian
Expert 5	Political mov.	09.10.2021	00:35:12	Online, Zoom	Russian
Expert 6	Media	12.10.2021	00:44:04	Online, Jitsi	Russian
Expert 7	Media Human rights Civil rights	22.10.2021	00:30:34	Online, Zoom	Russian
Expert 8	Electoral rights	12.11.2021	00:40:43	Online, Zoom	Russian
Expert 9	Electoral rights	26.11.2021	00:44:10	Online, Zoom	Russian
Expert 10	Media	30.01.2022	01:17:55	Online, Zoom	Russian

Appendix 9

List of Focus Groups

Code	Date	Number of Participants	Overall Length	Format	Language
FG1	15.01.2022	5	01:10:33	Online, Zoom	Russian
FG2	16.01.2022	5	>1 hour	Online, Zoom	Russian
FG3	19.01.2022	3	00:50:29	Online, Zoom	Russian
FG4	20.01.2022	4	01:10:47	Online, Zoom	Russian
FG5	26.01.2022	2	01:08:31	Online, Zoom	Russian
FG6	27.01.2022	5	01:22:50	Online, Zoom	Russian
FG7	28.01.2022	5	01:34:18	Online, Zoom	Russian
FG8	29.01.2022	4	01:00:59	Online, Zoom	Russian
FG9	31.01.2022	4	01:31:27	Online, Zoom	Russian
FG10	01.01.2022	5	01:17:29	Online, Zoom	Russian
FG11	01.01.2022	4	02:10:15	Online, Zoom	Russian
FG12	05.02.2022	2	00:39:00	Online, Zoom	Russian
FG13	05.02.2022	3	01:05:53	Online, Zoom	Russian
FG14	08.02.2022	1	00:36:59	Online, Zoom	Russian

Non-exclusive licence to reproduce thesis and make thesis public

I, Mariia Maksimova (personal identification code: 49603080023)

1. herewith grant the University of Tartu a free permit (non-exclusive licence) to reproduce, for the purpose of preservation, including for adding to the DSpace digital archives until the expiry of the term of copyright,

Civil Society against Stately Cybercontrol: the Case of Russia

supervised by Andrey Makarychev, PhD and Catarina Fróis, PhD.

2. I grant the University of Tartu a permit to make the work specified in p. 1 available to the public via the web environment of the University of Tartu, including via the DSpace digital archives, under the Creative Commons licence CC BY NC ND 3.0, which allows, by giving appropriate credit to the author, to reproduce, distribute the work and communicate it to the public, and prohibits the creation of derivative works and any commercial use of the work until the expiry of the term of copyright.

3. I am aware of the fact that the author retains the rights specified in p. 1 and 2.

4. I certify that granting the non-exclusive licence does not infringe other persons' intellectual property rights or rights arising from the personal data protection legislation.

Mariia Maksimova
16/05/2022