Exercising Power in Social Media:

Margarita Jaitner
C Thesis
Political Science with a Focus on Crisis Management and International Cooperation
01June“This in turn has kept protesters“This in turn has kept protesters 2012
Contents

Glossary 3

1. Introduction 4
   1.1. Background 4
   1.2. Statement of the Problem 6
   1.3. Research Question 7
   1.4. Significance of the Study 8
   1.5. Scope, Limitations and Assumptions 9
   1.6. Previous Research 11

2. Theory 12
   2.1. Hard and Soft Power 12
   2.2. Social Media 14
   2.3. Hard and Soft Power in Social Media 16
   2.4. Summary 18

3. Methodology 18
   3.1. Case Study 18
   3.2. Source Criticism 21

4. Findings 21
   4.1. Events During the Elections 21
   4.2. Microblogs – Twitter 23
   4.3. Social Networking Sites – Facebook, VKontakte 25
   4.4. Blogs – ZhivojZhurnal 27
   4.5. Content Communities – YouTube 27
   4.6. What else happened 28
   4.7. Summary 29

5. Analysis 30
   5.1. Countermeasures 30
   5.2. Means of Power 33

6. Results and Discussion 37
   6.1. How to exercise power in Social Media 37
   6.2. Discussion 38
   6.3. Criticism 40
   6.4. Recommendation for Future Studies 40

7. References 42

Appendix 47
**Glossary**

**Bot:** A computer program that runs automated tasks.

**(D)DoS:** Distributed Denial of Service attack, a type of cyber attack that aims to make a website or a web service inaccessible.

**Duma:** Госдума, State Duma, the lower house of the Federal Assembly of Russia.

**Hashtags:** Words marked with # in the beginning that are used to group discussions for example on Twitter.

**OMON:** Отряд милиции особого назначения, Special Purpose Mobile Unit, a collective name for a number Russian police units.

**MMORPGs:** Massive multiplayer online role-play games, games that are designed to be played online by a large community.

**Proxy server:** Web proxy servers can be used to access websites that are blocked on the local host.

**Search engine:** A tool to search information online, such as Google.

**Spam:** High volume bulk messaging, not delimited to e-mail.

**Troll:** A person who posts inflammatory or non-related comments online in order to disrupt the ongoing discussion.

**Yabloko:** Russian social liberal party, one of the main oppositional parties.

**YedinoRos, YedRo:** ЕдиноРос, ЕдРо Abbreviations for Yedinaya Rossiya and its supporters. Often used in a derogatory way.
“Information is power, and today a much larger part of the world’s population has access to that power. “
Joseph S. Nye Jr. ¹

1. Introduction

1.1. Background

Undeniably, social media has a great impact on many people’s lives and is used for far more than personal networking and entertainment. The career-networking tool LinkedIn, for example, is well used with it’s over 100 million accounts.² But social media is more than just networking - it enables people to express themselves and speak for their cause in many different ways. One can post a blog entry, upload a picture to Tumblr or share an article on Pinterest. While a certain part of these actions are aimed at the users friends and have a strictly private context and another aims to advertise a product or service, there is a significant amount that targets a wider audience and is meant to speak for a certain cause.

The role of social media in organizing protest movements or disseminating information on sociopolitical issues has undoubtedly attracted attention amongst journalists as well as scientists. The significance of technologies, such as text messaging, and social media tools has been widely discussed in the wake of the events that are today known as the Arab Spring. During early 2011 social media, particularly Twitter, and text messaging were widely used to disseminate information on people’s dissatisfaction with the governments and to coordinate protests in Algeria, Bahrain, Egypt, Morocco, Tunisia and Yemen. Journalists coined the term “twitter revolution” quickly and scholars have noted the significance of information technology for political movements.³

For the sake of completeness it should be mentioned that the events of Arab Spring were not the first case of political uprisings with help of social media. Protesters in Iran, for example have also used social media during the election protests in 2009.⁴ However,

² LinkedIn (2011)
³ Hounshell (2011)
⁴ Zuckerman (2011)
scholars also argue that social media does not change the nature of uprisings but merely facilitates them and does not necessarily have an impact on the outcome of the uprising.\(^5\)

Social media can be used as a tool for exercise of power as demonstrated by the Zapatista movement in mid 1990's. \(^6\) The movement used social media to spread their agenda and to inform the regular press, volunteers and non-governmental organizations about ongoing actions in their struggle against the Mexican government. They managed to get the different organizations and traditional media to “swarm” to places where the movement wanted publicity and presence of non-government actors. Through use of social media they managed to get their agenda through not only to their followers, but also to the international forum and could thereby place some pressure on the Mexican government.\(^7\)

On 6 August 2011 a peaceful protest turned violent in a northern district of London, UK. The riot quickly spread first into the capital’s other neighborhoods and later even to other larger cities. During the following days the country’s major cities faced widespread riots, arson and looting. Social media came to play a significant role during the protests in various aspects. Rioters used it to organize mass gatherings via various social media platforms and BlackBerry Messenger service.\(^8\)\(^9\)

Investigators also used social media during and after the riots to identify persons who were taking part in hooliganism, looting and arson via pictures of the events that were posted online.\(^10\) The impact of social media was deemed to be of such significance that the British Prime Minister David Cameron suggested the possibility of limiting access to certain social media upon suspicion of it being used for plotting criminal actions.\(^11\)\(^12\)

\(^5\) Zuckerman (2011)
\(^6\) Zapatista (the Zapatista National Liberation Army, EZLN) movement, active 1994-1998; Arquilla; Ronfeldt (2001) pp. 171-172
\(^7\) Arquilla; Ronfeldt (2001) pp. 178ff
\(^8\) Dodd; Davies (2011)
\(^9\) Halliday (2011a)
\(^10\) Halliday (2011b)
\(^11\) Guynn (2011)
\(^12\) “[…] whether it would be right to stop people communicating via these websites and services when we know they are plotting violence, disorder and criminality […]” BBC (2011)
In Russia the Duma elections held in December 2011 spawned numerous protests after allegations of falsification by Putin’s party Yedinaya Rossiya were spread online. Social media outlets such as YouTube and blogs were used to spread claims supporting the allegations of rigged elections. The widespread use of platforms such as Twitter, Live Journal, YouTube and other social networking sites have kept the protesters’ outrage over the allegations fresh in people’s minds. This in turn has kept protesters going. At the time of writing the protests have not calmed down.

These “new” ways to make use of information technologies can be seen as tools of democratization, however their use isn’t unproblematic. As the example of riots in UK has shown there is a need to research ways of handling violence that arises through coordination on the Internet.

1.2. **Statement of the Problem**

The Internet provides for a number of activities that can be connected to promotion of a movement. As identified by Arquilla and Ronfeldt these are:

- Collection of information\textsuperscript{13}
- Publication of own information\textsuperscript{14}
- Dialogue and debate concerning the issue\textsuperscript{15}
- Coordination of action with like-minded people and groups\textsuperscript{16}
- Lobbying decision makers by creating a discourse in the population\textsuperscript{17}

Subsequently, it is suggested that it is possible to react to any of these activities in a particular and suitable way.

There are a number of ways to react to protest or unrest in the social media. However, not all responses are feasible due to various sociopolitical considerations, such as international political pressure, the country’s economical situation, technological abilities or protesters’ anger.

\textsuperscript{13} Arquilla; Ronfeldt (2001) p. 242
\textsuperscript{14} Op. cit. p. 244
\textsuperscript{15} Op. cit. p. 246
\textsuperscript{16} Op. cit. p. 248
\textsuperscript{17} Op. cit. p. 250
One of probably the most basic responses is to block off access to the Internet entirely or for certain sites. However, as the experience has shown in the case of Egypt\textsuperscript{18}, this way of handling the problem is highly problematic in a number of areas. For one, Mubarak’s blocking off access to social media resulted in harsh criticism by the international community putting a strain on cooperation with his government and weakening the regime externally.\textsuperscript{19} For another, the blockage resulted in a financial loss for Egypt’s economy likely resulting in decreasing support for Mubarak internally.\textsuperscript{20} Also blocking off access to social media is not a simple task to perform due to the nature of technology: There are various means to work around a blockage, such as using proxy servers as it was done in Tunisia.\textsuperscript{21} A total shut down of access to the Internet can also result in difficulties in investigating the origin of the unrest or possible lines of support from unfriendly nations or organizations.

The previous section suggests a variety of cases in which a movement grows with help of social media. In some cases the government might see a need to interfere in order to calm down or even suppress the movement.

It is suggested that the government has more options to do so than the ones publicly discussed in context of the cases mentioned above. The very essence of social media offers a broad spectrum of conceivable methods to interfere with a growing movement within. Particularly exercising power by attraction within social networks seems logical. But is it possible to achieve immediate results by interfering within social media in any other way but shutting down access?

\textbf{1.3. \quad Research Question}

Non-state actors are increasingly using social media to organize and coordinate activities. Therefore a need arises to find practical solutions that enable the state or it's

\begin{flushleft}
\textsuperscript{18} Obama (2011)  \\
\textsuperscript{19} BBC (2011b)  \\
\textsuperscript{20} Zuckerman (2011)  \\
\textsuperscript{21} Ibid.
\end{flushleft}
sympathizers to counteract. These methods of counteraction can be seen as exercise of power and thus be classified with help of Nye’s theory of hard and soft power.\textsuperscript{22} This results in the following research question:

- What methods can be used within social media in order to deter an opposition from growing? How can these be classified in terms of hard and soft power?

Because this paper focuses on the events in the context of legislative and presidential elections in Russia that were held in late 2011 and the beginning of 2012, the sub-questions:

- What actions did the opposition perform in social media in Russia during the election period 2011-2012?
- How did the legal constitution and their sympathizers counter these actions?
- How do these counteractions constitute exercise of hard and soft power?

\textbf{1.4. Significance of the Study}

This study aims to identify methods and strategies that state actors and their supporters can apply when dealing with agitators in social media and place them in recognizable theoretical categories. Using a well-established theory for categorizing the different methods makes it easier to handle this relatively new phenomenon academically and even potentially estimate how the counter action might influence the public opinion nationally and internationally. Knowledge of this type can also be relevant for other groups. For example, the opposition might use the findings to plan an campaign supported in the social media, international observers could make use of the findings in order to estimate the level of democracy in a country, and in cases of authoritarian regimes the findings might provide a lead how to support democratization processes.

After years of state controlled press during the communist rule and the “half-freedom of speech” of the Putin era\textsuperscript{23} there is little trust into media outlets such as TV or news papers amongst the population. People resorted to discussing politics in private and to expressing themselves in a humoristic way. Therefore social media in Russia, and in

\footnotesize\textsuperscript{22} Nye (2004)  
\footnotesize\textsuperscript{23} Lonkila (2012)
other countries that experienced a prolonged period of regime-controlled media, has the potential to reach a different status and fill a different function than in fully democratic countries where the conventional media is regarded as a fairly credible source of information.

1.5. **Scope, Limitations and Assumptions**

The scope of this thesis is to give a broad overview over options that a state actor has when encountering an uprising carried out in social media. This can be a sensitive subject as the very subject of this study may be used in contexts that conflict with the western view on human rights and freedoms, and the findings can be used by actors with highly questionable goals, such as authoritarian regimes.

Thus one of the difficulties when conducting research in this area is to stay clear from putting value into actions from a moral point of view. When an actor is required to handle unrest his reactions might quickly become questionable from a democratic point of view. Some of them result in condemnation by the population, leaders of the international communities or human rights groups. However, these actions do exist and it is important to include them in a study like this.

This study does not aim to research the concept of Internet or the different technical solutions to act on the Internet. However the assumption is that the average reader is somewhat familiar with the concept of social media and has a basic understanding of the technical solutions that can be used on the Internet. It is also assumed that the reader is at least somewhat familiar with the political situation in Russia and has a sense for culture-related differences in information campaigns.

This paper focuses on Russian-language Internet, RuNet. Due to the language barrier and it’s specific cultural context it remains comparably isolated from the rest of the Internet. For that reason, the assumption is that even if an actor from abroad chooses to post something in RuNet, it is aimed at Russian society.

---

24 Lonkila (2012)
This study will scrutinize the political actors, and their sympathizers, behavior in a few social media platforms, namely Twitter, the Russian Live Journal blogs (known as Zhivoy Zhurnal, Живой Журнал or ЖЖ), Facebook and VKontakte (ВКонтакте, a Russian-language web platform similar to Facebook). The Russian-language Internet is of course not limited to these platforms, however these have been deemed the most relevant for the study due to their high popularity in Russia\textsuperscript{25} and their comparability to platforms popular outside RuNet. This limitation means however that an extremely popular platform “Odnoklassniki” (Одноклассники, Classmates)\textsuperscript{26} was omitted despite being second in popularity in Russia. This platform was omitted because it appears to be “out of the loop” of the otherwise interlinked political debate within social media.

The study does not aim to research political protests on the Internet, but is delimited to social media. Despite this limitation it is important to understand that these platforms do not exist in a vacuum but live off the interconnection with the rest of the Internet. In practice this means that social media is used to popularize information found elsewhere online: Articles, opinions, videos and pictures gain popularity by being posted, re-posted and judged in social media thus becoming a part of it. For this reason the study is going to include elements found outside social media, however only to observe these elements’ significance in social media.

Furthermore the is sometimes a need to take a look at the events taking place off line due to the extreme inter-linkage between the on-line and off-line world. Off-line events trigger on-line events and vice versa. For this reason the study is going to touch upon events outside the Internet, although they are not the subject of the study. The key is to understand how these events are relevant to the context of social media and at the same time to delimit the focus to studying to the effects in the social media. Applying this assumption denial of access to the Internet or particular parts of it means both acting within and outside the Internet.

The study focuses on the time period between the legislative (Duma) elections held on 4 December 2011 and 10 May 2012, the day after the yearly large scale parade that is held in honor of veterans of the Great Patriotic War and the Victory Day. The reasoning

\textsuperscript{25} Lonkila (2012)
\textsuperscript{26} Ibid.
behind the choice of this particular end date was the desire to see whether the oppositional activity would continue with the same intensity during this important holiday.

In many cases the government is opposed by a number of different ideologies and political opinions rather than one single more or less cohesive group with a highly aligned agenda. However, for the purpose of this research there is no need to differ between these groups. Throughout this paper the term opposition will be used to refer to any group that is opposing Yedinaya Rossiya. Furthermore, any action that interferes with oppositional operations will be classified as a countermeasure if any other actor including a pro-Yedinaya Rossiya movement can adopt this action for its own purposes.

1.6. Previous Research
Nye’s theory on the use of hard and soft power was firstly published in the 1990s and has since then been confirmed by peers and further developed as a theory and applied in different contexts. Thus this theoretical framework can be used to scrutinize a government’s exercise of power.

The subject of social media and its effects on society and politics has drawn a lot of attention amongst scholars. Especially after the uprisings in northern Africa in the beginning of 2011 this subject has been on the scientific agenda and several studies on this issue have already been published in a variety of scientific disciplines. These studies research a wide variety of aspects concerning social media from different scientific points of view and have partly different geographical foci.27

A lot of research has been conducted in the area of sentiment detection within Twitter for example or aiming to classify the use of social media. Also, a number of studies are concerned with the use of social media for advertising purposes. Many of these studies’ main concern was to evaluate effects and benefits of using social media. Often these studies are conducted within the areas of communication sciences or sociology. Although these studies belong to other disciplines they can lend raw data as well as interesting reasoning to studies within political science. Many of the studies are highly

27 Cornell University Library Guides (2011)
multidisciplinary because they require an in-depth understanding of technology, society and political discourse.

A number of recently published studies aim to describe and analyze the political discourse in RuNet. Scholars of the Berkman Institute for Internet and Society at Harvard University presented an extensive study in 2010. This study resulted in a thorough description of RuNet with it specific culture. An article by Deibert and Rohozinski, which was also published in 2010, focuses on subversion and exercise of power within RuNet. It answers the question whether RuNet is likely to become as content restricted as for example Internet in China particularly with regard to possible development of members of the Commonwealth of Independent States towards more authoritarian regimes. The Finnish Institute of International Affairs has recently published a working paper by Markku Lonkila that scrutinizes the role of social media in mobilizing the protests in December 2011.

Another good example for works that focus on social media platforms with focus on political science is the study conducted by Vladimir Barash and John Kelly of Harvard University. “Salience vs. Commitment” concentrates on Twitter and the use of hashtags in the Russian political information campaigning. This study delivers an information sociological background to studying the political discourse during the election period.

This study differs from research presented above because it puts the focus on methods of exercise of power rather than on the use of a particular tool.

2. Theory

2.1. Hard and Soft Power
Joseph Nye’s work on concept of “soft power” as a way to “get what you want through attraction rather than coercion and payment” as Nye puts it himself, was firstly published in the 1990’s. The distinction between “soft” and conventional “hard power”

---

28 Etling et al. (2010)
29 Deibert et al. (2010)
30 Lonkila (2012)
31 Barash; Kelly (2012)
32 Nye (2008)
requires a sound understanding of the term “power”. Nye defines power as “the ability to influence the behavior of others to get the outcomes one wants”\(^{33}\) and to do so by utilizing threats and/or inducements is exercise of “hard power”\(^{34}\).

Exercise of hard power is based on those who are being subject to this type of power know about it means. The very essence of hard power is that those whose actions one intends to influence have to become knowledgeable of the existence of the means in one way or another. A threat is only a threat when the person exposed to it knows or believes in it. This makes the means of hard power often tangible and definable. According to Nye economical sanctions, payment or utilization of forces are means of hard power.\(^{35}\)

Soft power is far more impalpable. It is about ”attraction to shared values and the justness and duty of contributing to the achievement of those values”. It is an attraction that comes from within, disregarding attraction that comes from incentives.

The two types of power do not necessarily exclude one another, in some cases they can even enhance each other. In certain cases with power comes attraction, as well as it might be easier for an attractive actor to argue for his cause. However, overuse or misuse of hard power can lead to diminished attractiveness and thus to loss of soft power.\(^{36}\) Nye calls the co-utilization of hard and soft power “smart power” and recognizes that this fitted mixture of elements of hard and soft power might be the most effective way to exercise power in general.\(^{37}\)

In the global information age, the ability to utilize soft power is increasingly becoming a necessity. Nye exemplifies this with the need to exercise soft power to meet today’s security threats.\(^{38,39}\) Although the concept of soft power as a contrast to hard power has been continuously developed by Nye and other scholars of international relations and

\(^{35}\) Nye (2008)  
\(^{36}\) Nye (2004) p. 25  
\(^{37}\) Nye (2009)  
\(^{38}\) Nye (2004) p. 95  
\(^{39}\) Nye (2008)
enjoys great popularity in this field, it can also be applied in domestic policy.\textsuperscript{40} Obvious examples can be found in American election campaigns where candidates strive to create a positive public picture of their person. This is often regarded as an element equally important as the candidate’s political agenda. Even states regarded as more coercive apply soft power with internal politics: The Communist Party of China, for example, explores the effects of utilization of soft power within China’s domestic governance and claims to be doing so successfully.\textsuperscript{41}

The distinction between hard and soft power is not clear-cut. As noted earlier, tools of hard power can also include elements of soft power in various degrees. Different means of hard power also employ different levels of threat or offer various levels of incentives. Thus the transition between hard and soft power is a smooth one rather than a definitive. Or, as Christian Wagner puts it, “Concepts of hard and soft power can be regarded as two poles on a continuum of power.”\textsuperscript{42}

\textbf{2.2. Social Media}
Social media comprises those parts of the Internet that promote and require participation, openness, conversation, community and connectedness. Participation, openness, conversation, community and connectedness can be found in various places of the Internet. Social media comprises those platforms that promote and require most of these characteristics.\textsuperscript{43}

While traditional media delivers a very restricted two-way conversation, social media encourages its users to become authors on their own. Common news outlets have had a letter to the editor section for a long time and those who have taken the step into the Internet now offer the option to comment on articles directly. Social media however does heavily rely on a two-way communication. It encourages comments and sharing of information, a blog’s popularity, for example, is often shown by the number of people who follow, comment and share the information in different outlets, or, simply put, by the conversation it creates.\textsuperscript{44}

\begin{thebibliography}{9}
\bibitem{40} Zhang, Jiang (2010)
\bibitem{41} Ibid.
\bibitem{42} Wagner (2005)
\bibitem{43} Mayfield (2008) p. 5
\bibitem{44} Op. cit. p. 5
\end{thebibliography}
There are various ways to classify social media, Kaplan and Haenlein, for example suggested a classification of six different types of social media:

- Collaborative projects such as Wikipedia
- Blogs and microblogs such as Twitter
- Social networking sites, such as Facebook
- Content communities like YouTube, Twitpic or Pinterest
- Virtual game worlds such as MMORPGs
- Virtual social worlds such as SecondLife

What these have in common is the platforms need of participating audience.45

The suggested classification is not universal: Social networking sites have also been described as platforms that “allow individuals to construct a public or semi-public profile within”46 the platform, “articulate a list of other users with whom they share a connection, and view and traverse their list of connections and those made by other users within the system”47. This definition is true for Facebook, LinkedIn, Badoo and many others, however it is also true for platforms that are not classified as social networking sites if applying Kaplan and Haenlein’s definition: Twitter allows for creation of a personal mini profile, the user can disallow followers and construct it’s own semi-public environment within the system, and it’s a common use of Twitter messages to be reused by a number of other users thus creating a cross-connection.

Therefore a different classification system may be more meaningful when scrutinizing a certain aspect of social media. Within this study a classification according to how the site is used in relation to organization of protests is applied:

- Microblogs - Using Twitter it is possible to quickly disseminate information and thus use it for ad-hoc organization and real-time updates for co-protesters
- Social networking sites - Using the built in calendar functions (events in Facebook and VKontakte (мероприятие) protesters can coordinate and plan actions upfront
- Blogs - This type of media acts quasi-independent information outlet similar to conventional media sources such as newspapers. These are used to form opinions and disseminate propaganda.

---

45 Kaplan, Haenlein (2010)
46 Boyd, Ellison (2007)
47 Ibid.
2.3. **Hard and Soft Power in Social Media**

Social media today is used as much more than just a tool for people to communicate and share private information. It has become an important platform for companies to present their products and services. With help of advanced technical solutions for user profiling companies can advertise directly to their target group. Social media has also become a platform for promoting political and social causes.

The interconnectedness of social media makes it easy to promote different causes with a variety of requirements for participation. Sites like www.causes.com suggest that everyone can change the world right from the comfort of his or her home.

Slacktivism\(^{48}\) and clicktivism are terms that are used to describe the low-input type of activism within social media, sometimes in a derogatory way. However there is reason to believe that even this type of low-commitment, low-risk and low-cost activism within social media can lead to impact on the political discourse.\(^{49,50}\) Thus we can ascribe social media certain means of power.

In order to be able to apply the theory of hard and soft power on events and action in the social media there is a need to create a framework for classifying actions as means of hard of soft power. Such a framework is suggested in Chart 1.

As noted earlier there is a near seamless transition from hard to soft power and thus means often will be classified as elements of “rather hard than soft power” and vice

---

\(^{48}\) Oxford Dictionaries (2012)
\(^{49}\) Rotman et al. (2011)
\(^{50}\) Lindquist (2011)
versa instead of labeling them as an element of one single type of power. This implies that in terms of using social media the amount of hard and soft power can vary depending on how and what type of media is used, or in what combinations they are present, as well as who is using it for his or her purposes.

In international relations the utmost exercise of hard power is often exemplified by military action against the subject of power. A parallel to this in the world of social media would be a complete denial of access to the platform. This can be done in a variety of ways within and outside the Internet. This has been done for example in Egypt in spring 2011, employing means outside social media and cyberspace, and in Estonia in April 2007 using the Internet.\textsuperscript{51}

Means of soft power on the other hand can seem more diffuse. They include any action that aims for co-option by the power’s subjects. An appealing self-presentation online, that does not include elements of coercion or induction and is regarded to be worthy to share by users online with others, is an example for exercise of soft power in social media.

\begin{center}
\begin{tikzpicture}[scale=1.5]
\node at (0,0) {\textbf{Social media}};
\node at (-2,0.5) {\textbf{Hard power}};
\node at (2,0.5) {\textbf{Soft power}};
\node at (-2,-2) {\textbf{i.e.}};
\node at (2,-2) {\textbf{Appealing self presentation}};
\node at (-2,-2.5) {Denying access};
\node at (2,-2.5) {(deliberate) Rumours on social media};
\end{tikzpicture}
\end{center}

\textbf{Chart 1. Exercise of power in cyberspace}

\textsuperscript{51} Davies (2007); Kanally (2011)
2.4. **Summary**

The conditions of exercising power have become more complex in the global information age. Joseph Nye argues that there are two types of power: the power of coercion - hard power, and the power of attraction - soft power. Smart power, according to Nye is a purposeful combination of both. As this definition implies an evaluation of results, it will be omitted in this study. It was suggested that it is possible to exercise both types of power in social media and a framework of classification was presented.

3. **Methodology**

3.1. **Case Study**

Case study was the method of choice for this study as it aims to identify a broad range of means and tools that can be used to hinder the growth of an opposition within social media. It is argued that the use of many means can be amplified and it is their existence that is in primary focus for this study rather than to what extent they were used. This approach calls for a method that supports qualitative research rather than quantitative.52

This method relies on observation53, however since a large portion of data (Tweets, comments, blog entries) is text it also possesses similarities to text analysis54. However the elements of text analysis are limited to categorizing the presented texts in 3 categories: oppositional, pro-governmental and irrelevant to political discourse.55 The decision to use one single case rather than a number of cases was based on the aim to deliver an overall and coherent picture rather than exemplifying the use of social media in a political struggle.56 The approach was lent from the General Morphological Analysis57 that insofar as social media is complex due to its inter-dependency. It is simply unrealistic to believe that someone would use only one type of social media and never follow any links to other types. With this reasoning use of social media in the context of a real life event has to be treated as a whole single case.

---

52 Bryman (2008)
53 Silverman (1997) pp. 30-31
56 Bryman (2008)
57 Ritche (2011)
In order to be able to provide a structured analysis rather than a narrative of events the variables have been clustered within the single case study, lending the approach from a clustered analysis. As suggested by Byrne, it is possible to cluster variables within a single case in contrast to clustering actual cases. Applying this approach the different variables can be understood as sub-cases to the case study. Using cluster analysis the aim is to establish how the cases relate to one another with regards to their relative similarity and/or dissimilarity to one another and thereby classify whole sub-cases into types or clusters. Thus the cluster analysis method focuses on the relationship between the cases or sub-cases, and not, as with most variable based statistic analyses, on the relationship between the variables. In this study the sub-cases are constituted by the different means and methods that can be used within social media. This method can be described as a single pass in a non-hierarchical finished cluster method. Applying the morphological analysis data describing a complex sociopolitical problem can be divided into a number of non-quantified variables and ranges of conditions. At a later stage these variables can be grouped into well-defined relationships. The theoretical framework of the method used is presented in chart 2.

Chart 2. Theoretical framework for the applied methodology.

---

58 Byrne (2009) pp. 138-139
60 Ibid.
61 Byrne (2009) p. 136
62 Ritchie (2011)
In order to achieve the most suitable clustering the data has been iteratively grouped and re-grouped, which resulted in a number of different clusters. In the next stage these groupings were compared and the most optimal cluster was selected for further analysis. In practice this means that the selected data was clustered in order to achieve a representable category of information, which in its turn could be compared to other types of actions in terms of hard and soft power.

The data for this study was collected from various social media with the starting point being verified events: the legislative elections, the presidential election and the presidential inauguration. Twitter has been deemed to be vantage points for researching the discourse in social media because it constitutes a hub for the inter-linkage within social media. In practice this means that tweets often link to Facebook or Vkontakte events, blog posts and even secondary media. The goal was to generate systematic samples that were to represent the use of social media in the context of the political struggle during the researched time frame.

During the period of the study the webpages were examined on a routine basis as well as randomly inbetween in order to be able to identify abnormalities. The examination frequency was increased during important events; such as the election days, important holidays, or when a larger demonstration was announced. Whenever activity on a webpage increased significantly, the examination of that webpage intensified as well.

Individual Twitter and LiveJournal accounts were not specifically targeted for examination. Whatever topics the Runet community as a whole was talking about were focused on. However, some individuals were very active in maintaining the community interest in some topics. In the case of Alexey Navalny it meant that his name was used in a Twitter hashtag that was fairly popular during the course of this study. Due to that popularity it was included in the pool of keywords that were used to probe the websites studied. Similarly, whenever the activists on both sides created a significant new keyword it was added to the pool.

63 Bryne (2009) p. 143
64 Bryman (2008) pp. 278-279
The study relies mainly on primary sources many of which are unique because they do not necessarily persist over a long period of time. Tweets, blog posts and other content can be deleted and groups or events and their descriptions can be changed with a number of clicks. Some of the data can be retrieved from secondary sources such as Google Cache but not all. In many cases one has to know what to look for in order to retrieve it afterwards. The study also uses sources that would normally be described as secondary, such as articles in online media outlets. However they are rather seen as a method to amplify the events by making them known to a broader public rather than common secondary sources.

3.2. **Source Criticism**

The data used in this study is unique primary data collected through observation. This includes postings in various social media as well as articles and news found in various news outlets. This type of material is usually very problematic in an academic context. This is also true for statements that are found in official Russian outlets such as state TV.

However unreliability is not relevant in the context of this study because of the way the data is used: When something is posted online, it creates a discourse and influences the public opinion. No official statement to correct the untruth will return the public opinion to what it has been before the untruth was disseminated.

Applying this assumption the question that is sent to the data is not whether or what happened in reality but whether a piece of information was posted online and has promoted a discourse. This means that the data is not used to document events that are described in the data but rather to observe the reaction it creates.

4. **Findings**

4.1. **Events During the Elections**

Depending on the individual situation a government might limit its actions online to observing the growing unrest and collecting information on those inciting the unrest and activities. This would allow the government to react with meaningful real-life measures. In the case of riots in the UK in 2011 where the findings in social media were
used to identify and prosecute those who committed crimes during the riots. The
government may also use data collected in social media to try to estimate the number or
type of security personnel needed to handle a mass gathering or whether there is a need
to protect a certain object.

Depending on the overall aims, desirable outcomes and it’s own abilities the government
has to carefully consider the ways it wants to respond to an unrest rooted in the social
media.

The Russian legislative elections (Выборы в Государственную думу) were held on 4.
December 2011. There were seven parties registered to be elected, however the
opposition expected the then-ruling party, United Russia (Единая Россия), to win this
election using dishonest methods and voiced their mistrust.

In the evening of December 4th indeed activists considered the election process flawed
and gathered to demand the election results to be annulled. During the following weeks
many demonstrations and “meetings” (митинги) were held. These culminated in
protests in many Russian cities and even abroad on the 10th of December, the march on
Bolotnaya Square in Moscow was said to be one of the largest in Russia during the past
decade. During the demonstrations activists from various parties formed an ad-hoc
opposition with a common enemy - Yedinaya Rossiya, and a common symbol - a white
ribbon. However each party continued arguing for it’s own cause at the same time.

The Russian police, who were ordered into Moscow on the 6th of December, and pro-
Putin activists, Nashi (Нашi), who organized demonstrations in favor of Yedinaya
Rossiya countered the “meetings”. In many cases arrests were made, amongst others
one of the opposition’s front men, Alexey Navalny (Yabloko) was taken into custody on
various occasions. Another large-scale demonstration was held on the 24. December and
even during the following months people gathered to show their lack of trust for
Yedinaya Rossiya and the elections.

Putin’s candidature in the 2012 presidential election was disputed loudly by the
opposition and following the debacle about falsifications during the Duma elections
some precautions were taken by the elections committee: The earlier used solid urns were replaced by transparent ones and web cams were installed in the country’s polling stations. These web cams were livestreaming during the elections and could be watched on www.webvybory2012.ru. Vladimir Putin took 63.60% of the vote in the first round and won the election.

However the committee’s measures to raise trust for the procedure did not hinder the opposition to gather for new demonstrations. The largest “meetings” were held on the 5th and the 10th of March. Again, numerous arrests were made on several occasions. According to official statements security agencies would only interfere with demonstrations when they turned violent or would otherwise break the law. Several allegedly not previously state-approved demonstrations were stopped by the special police forces (OMON).

The opposition started planning the Million’s March (Марш Миллионов) shortly after the official results of the presidential election were released. On 6th of May, a day before Vladimir Putin’s third inauguration, the large demonstration took place in Moscow. During the demonstration different sources claimed that one or several people have died in the masses. However it turned out that only one blogger died following a fall from a fire escape while trying to photograph the march. This time the security agencies were claimed to be more brutal than during the previous months’ demonstrations and many arrests were made. The demonstration continued until late at night and next day the opposition gathered once again on Manezhnaya Square, Kitay-Gorod (Китай-Город) where protesters stayed during the night and continued demonstrating their discontent during the remaining days covered by this study.

4.2. Microblogs – Twitter

Opposition and supporters of Yedinaya Rossiya campaign and organized their protests via Twitter and other online platforms while the traditional media chose to focus on

---

65 After the elections the videos were archived and are accessible via the State and Municipal Services web site http://epgu.gosuslugi.ru/pgu/service/-1000000413_418.html; Appendix: scr1a, scr1b
66 Nummelin (2011)
67 Allegedly state-controlled official media outlets such as TV, radio, printed press.
other news and barely mentioned the protests. Interestingly, the online news outlet Utro (Утро, Morning) was quick on calling the previous days’ events a “try to start a twitter revolution” on the 5. December. During those first demonstrations the derogatory term for the opposition “little net hamsters” (сетевые хомячки) was coined and used as a hashtag on Twitter.

Shortly thereafter pro-Kremlin and completely non-related messages started showing up in the Twitter feed, these were using the same hashtags as the opposition, particularly #триумфальная, and quickly multiplied to a vast amount that complicated coordination of protests. Cyber security experts had also identified unusual sudden raise in new Twitter account registrations and connected these to those messages using the opposition’s hashtags. A number of accounts have been identified as bots and were blacklisted.

Whether a user account is used by a bot or not is in many cases easy to identify even by non-experts. Typically bots would post new tweets much more frequently than a regular user. Some bots post several different or similar tweets per minute, something a human user would not be able to do no matter how fast they would type. Other bots are seemingly human with a slower pace of posting.

Two types of bot accounts can be identified: The first type uses accounts that were newly registered for the bot, while the other account uses accounts that were registered by regular users. The latter can be identified by the pattern of their historical activity. These accounts’ history typically includes a number of private non-bot-related tweets followed by inactivity with most recent tweets being activity that can be attributed to bot activity.

68 TT via Dagens Nyheter(2011)
69 Gasparov (2011); Appendix: scr2
70 Appendix: scr3
71 Keen (2011)
72 Appendix: scr7a, scr7b
73 Goncharov (2011): Listing of Twitter bots recognized in December 2011.
74 Rusecurity (2011)
75 Goncharov (2011)
76 Appendix: scr4
77 Appendix: scr5a, scr5b
As mentioned earlier there were several types of information that might be disseminated by bots. For one a number of pro-Kremlin or contra-opposition tweets could be observed. These include pro-Kremlin information or derogatory speech directed at the opposition. Other bots post completely non-related tweets including links to different products. These can be compared to conventional SPAM many users receive in their e-mail. Since spamming is against the terms of usage, bot accounts are regularly identified and blocked by Twitter. However it is only a matter of time until new bots become active.

Some human-only contra activity could also be identified. In these cases groups of users that can be assumed to be human try to make a trending topic on Twitter that would compete with hashtags used by the opposition. An interesting observation of activity-contra-activity pattern was made in the period of 6th to 9th of May when very little contra-opposition could be observed during the first two days with the exception of a non-related hashtag peaking in trends for a short while. The non-related tag Мяу (a cat’s meow) was allegedly brought up by the pro-Yedinaya Rossiya movement. The picture changed radically during the afternoon of the 8th when Twitter was swamped by contra-opposition tweets using the opposition’s hashtags making coordination difficult. This continued next day, with Victory Day topics trending.

### 4.3. Social Networking Sites – Facebook, VKontakte

A number of oppositional and pro-Yedinaya Rossiya groups were created on social networking sites Facebook and VKontakte before during and following the elections. Alexey Navalny’s group RosPil (РосПил) soon became one of the more popular groups with over 140 000 members. Alexey Navalny also maintains a page on Facebook, which however does not reach the popularity of RosPil. According to various sources the Russian Security Service FSB (ФСБ) contacted the head of

---

78 Appendix: scr6
79 Appendix: scr7b
80 Appendix: scr8a, scr8b
81 Appendix: scr9
82 Appendix: scr10
83 Appendix: scr11, scr12
84 de Calbonnel (2011)
85 Portalinski (2011)
86 Appendix: scr13a, scr13b
87 Appendix: scr14
Exercising Power in Social Media

Margarita Jaitner

Vkontakte Pavel Durov during the week after the elections asking him to take down RosPil. Pavel Durov declined to do so.88 89

These groups were used to discuss the events, disseminate information about upcoming events, and, as in case of RosPil, acts as a continuous campaigning platform. Many comments and entries include pictures hosted on sites like Twitpic and videos hosted on content sites such as YouTube.90 Many event pages were created for the upcoming demonstrations ranging from 0 to over 20000 users planning to attend. Some of the event pages were later reused for following demonstrations and do not hold the original description anymore. Long lists of comments that point to preparation towards the demonstrations during the researched period, however, tell the event pages’ stories.

A closer look at opposition’s groups and events on reveals a set of problems when planning and promoting demonstrations via these platforms. In order to gain more popularity these groups and events were made open and free to join by anyone, which resulted in a strange pattern of participating members. The event “Белая площадь” (Belaya Square in Moscow) for example had over 3700 members signed up to attend the demonstration, 505 that replied they would “maybe” attend and over 3000 other invited.91 Amongst attendees were a remarkably high number of accounts that had little or no ties to Russia or Russian politics.92 A number of these accounts seem to have been abandoned by their original user and hijacked by bots. This irregularity had also been noted by the opposition and resulted in further discussion about trustworthiness of either political movement.93

Occasionally groups were joined by non-supporters eager to discuss or disseminate propaganda. Despite the non-supporters being referred to as “bots” there was no evidence of automated or coordinated behavior of this type. The term bot refers in this case to the lack of own independent thinking in a machine. More often regular members would refer to the non-supporters as “trolls”, meaning provocateurs.

88 Forbes (2011)
89 Soldatov (2011)
90 Appendix: scr15, scr16
91 Appendix: scr17a
92 Appendix: scr17b, scr17c
93 Appendix: scr18a, scr18b
4.4. **Blogs – ZhivojZhurnal**

Blogs were widely used to create and maintain a political discourse. They also were used as a platform to disseminate YouTube video links to demonstrate cases of alleged electoral fraud. Bloggers were the platform to share political opinions, news or rumors, pictures taken during different actions and demonstrations. On several occasions opposition’s blogs were “trolled” by what were said to be pro-Kremlin activists and in some cases the events were similar to those on Twitter: Many previously inactive users would post more or less generic pro-Kremlin comments drowning out the opposition’s conversation. A lot of times these comments included vulgar language and insults towards the owner of the blog. Amongst the opposition these are now known as “Yedroboty”, an acronym for Yedinaya Rossiya’s bots - “Едроботы”.

Members of the opposition have tried to follow up and analyze the occurrence of bots on Live Journal. What they came across, as Eduard Kot stated on his popular blog edvvvard, was an ad for a freelance assignment searching for 5 people who would post 70 comments per day using 50 different user accounts in assigned blogs for a salary of 12.000 RUB ($ 389) per month. Eduard Kot then claimed to have traced the origins of the ad back to supporters of Yedinaya Rossiya. These findings triggered a further discussion about Yedinaya Rossiya’s and Nashi’s integrity. Some discussion regarding automated versus manual spamming of blogs was observed; however no evidence was found that would support a distinction between manual and automated spamming.

The popular blogging platform Live Journal suffered several so called DDoS attacks during the period of this study. This resulted in service outages during the second week of December.

4.5. **Content Communities – YouTube**

Accusations of electoral fraud were backed up by a vast amount of videos from polling stations across the country that were posted on YouTube. Some of these were
amateur videos recorded with help of smartphones by ordinary people; others were semi-professionally or professionally made by independent web-TV studios such as nk-tv. 103

Another group of videos and pictures posted in content communities were documentations of demonstrations and meetings, in many cases they aimed to document the behavior of security personnel.104 Many times videos and pictures are posted together with links to Facebook or VKontakte groups or blogs contributing to interlinkage of social media.105

Live streaming platforms, particularly ustream.tv, are a noteworthy subgroup of content communities. These sites provide a possibility to upload video content to the internet while creating it, for example with a smartphone camera, making these similar to live transmission of events on TV.106

Surprisingly no reference to political vlogs, video blogs, was found although vlogging has found it’s way into the Russian online society.107 Other content sites were mainly used to support activity within other social media platforms, providing content to blogs, social network groups and tweets.

4.6. What else happened

The following events occurred outside social media, however they were part of the discourse in blogs and social network groups and thus were deemed relevant for the study.

On 4 December 2011 websites of the radio station Ekho Moskvy (Эхо Москвы, Moscow’s Echo), news outlets Kommersant (Коммерсантъ), slon.ru, Bolshoi Gorod (Большой Город, Big City) and The New Times were subject of a DDoS attack which resulted in temporary unavailability. Website of the civilian association to protect
Russian electoral rights Golos and its project “Map of Fraud” (Карта Нарушений) and suffered same fate.\(^{108}\)\(^{109}\)\(^{110}\)

Recently, on 6 May Kommersant, Ekho Moskvy, slon.ru were once again victims of a DDoS attack together with the web TV station Dozhd (Дождь, rain.tv)\(^{111}\)\(^{112}\). On 9. May the streaming service ustream reported to be under attack that seemed to target the account reggamortis1. This user is known to stream videos of protests.\(^{113}\)

DDoS attacks were not the only hacker activities during the period covered by this study. A group calling itself Anonymous Op_Russia claimed to have hacked a number of e-mail accounts belonging to activists of Nashi and published their e-mail conversations. These leaked e-mails withheld information on planning paid bot-like attacks on popular blogs of the opposition as well as paying news outlets for publishing pro-government articles.\(^{114}\)\(^{115}\). Via Twitter Anonymous claimed to have conducted a number of other attacks, most recent being attacks against kremlin.ru and other government websites during the last week of study.\(^{116}\)\(^{117}\)

In the wake of mass protests a number of tools to support protesters has been introduced. The site Philanthropy, for example, published a selection of resources such as phone numbers to lawyers volunteering their help to protesters in case of arrest as well as a number of links to groups of civil assistance. For example the site helpwall.info “Стена помощи на митингах” provides a platform for organizing acute help via Twitter. Using the hashtag #help495 on Twitter or via text message protesters can for example notify the public about their arrest or get in contact with a lawyer.\(^{118}\)

4.7. Summary

\(^{108}\) BBC (2011c)
\(^{109}\) Newsru.com (2011)
\(^{110}\) Etling (2011)
\(^{111}\) Gazeta (2012); Securitylab (2012)
\(^{112}\) Appendix: scr31b
\(^{113}\) Taylor (2012); Appendix: scr28a, scr28b
\(^{114}\) Taylor (2012); Elder (2012)
\(^{115}\) Appendix: scr30a, scr30b
\(^{116}\) EHN (2012); DI (2012); Infosecurity Magazine (2012)
\(^{117}\) Appendix: scr31a, scr31b
\(^{118}\) Appendix: scr32a, scr32b
A number of different types of activity within social media were identified in the course of this study. The majority of online activity consists of planning real life activities, promoting one’s cause through blog entries, discussions in various groups, pictures and videos of events as well as propaganda. In many cases entries aim to defame one’s antagonists.

Another element that was identified is spamming which is done both manually and automated. Large amount of unwanted entries interferes with a group’s ability to converse and plan events.

Making social media unavailable by attacking websites lies technically outside the social media domain. However it has a significant impact on its usage and is thus relevant for this study.

5. Analysis

5.1. Countermeasures
The collected data shows a lot of online activity directly or indirectly connected to the protest. While some of the activity can easily be ascribed to either side of the conflict other activities’ origin is more ambiguous. Although there are technical means to trace a piece of information such as a blog entry, a comment or a picture back to its source, these means are in many cases unavailable to users or even researchers. This makes it difficult if not impossible for the researcher to verify pieces of information posted online. However those the information is primarily aimed at, in this case the Russian population, face similar difficulties, especially when a certain level mistrust towards official news outlets and government has been fostered in the populace for a long period of time.

Fortunately neither the truthful origin of a piece of information or activity nor the validity of the information is necessary for this research. Instead it is more important to consider the perception of information or activity amongst Russian population. As noted earlier this research focuses on activities that hinder the opposition in gaining influence, therefore the first step is to extract these from the pool of activities in social media.
Social media related activities that complicate the opposition's operations can be summarized as follows:

Countermeasure 1: Shutting down or limiting access.
Shutting down or limiting access to the opposition's tools of communication and coordination within social media by attacking the media as demonstrated by conducting a successful DDoS attack against Live Journal. This countermeasure can lead to significant monetary losses.

Countermeasure 2: Shutting down elements within social media.
Targeting certain elements within social media, such as a particular account or a group, such as the alleged request to shut down RosPil on VKontakte. In difference to the before mentioned total shut down this countermeasure likely aims to split a homogeneous oppositional group that has become “too big” in the eyes of it's antagonists. This method also has an element of threat, demonstrating one’s power over an entity within the seemingly uncontrolled Internet.

Countermeasure 3: Attacking media outlets.
Attacking other oppositional or seemingly neutral media is, similarly to the previously mentioned targeting of oppositional groups, a demonstration of power. When conducted against commercial entities it can lead to a significant loss of income, weakening and demoralizing its financial stakeholders.

Countermeasure 4: Automated spamming the Twitter feed.
During ongoing demonstrations automated spamming the Twitter feed using the topics and hashtags utilized by members of the protest to drown out information that is relevant for ad-hoc organization. In these cases opposition has no chance to fight the spamming process manually and will have to resort to using other means, for example a different hashtag.
Countermeasure 5: Manually spamming the Twitter feed.
This can for example be done during ongoing demonstrations. This countermeasure is deemed to be different from automated spamming simply because an automated bot can generate new tweets in a much higher speed and thus is easy to identify as a bot. In manually conducted spamming activities on the other hand humans compete with humans and success largely depends on the number of people in the group and the level of their motivation. This type of activity demonstrates commitment for a cause rather than willingness to use “brute force”.

Human counteraction can also amend the information rather than just drown out the relevant messages. For example it is possible to post misleading information about further plans for demonstration in order to split up groups on the streets.

Countermeasure 6: Trending other topics.
Popularizing other hashtags and topics than the ones used by opposition on Twitter as in case of the #Мяу (Meow) hashtag. This activity is similar to manually spamming the Twitter feed as it aims to demoralize the opposition by showing their “unpopularity”.

Countermeasure 7: Organized spamming of blogs.
Organized spamming of blogs with unrelated or hateful comments and thus drowning out the discussion as it has been done in Alexey Navalny's blog on several occasions. This activity also aims at disturbing the discussion. There was not enough evidence to conclude that automated spamming of media other than Twitter occurred, though it is technically possible. Thus no distinction between manually and automatically conducted spamming is being made at this point.

Countermeasure 8: Defame the opposition with facts.
Using the gathered information to defame the opposition, for example by pointing out that a large amount of people who agreed to take part in a demonstration in deed do not even have any connections with Russia.

Countermeasure 9: Defame the opposition with forged information.
Forging “facts” that defame the opposition and spreading them online. This can be exemplified using the case of the Facebook event “Белая площадь” where the high
number of participants was composed of persons with no obvious ties to Russia. Since there is no way to know who added these persons to the event there are two possible explanations: members of the opposition to create an illusion of massive support in the population might have added these people. Alternatively those who aim to defame the opposition might have added these participants only to accuse the opposition of “playing dirty” or exaggerating their popularity.

Countermeasure 10: Discussion.
Partaking in discussions in opposition’s groups or blogs as observed within various social media platforms aims at changing the member’s opinions or demoralizing the opposition.

Countermeasure 11: Blogs, groups etc.
Maintaining own presence within social media and lobbying for one’s own cause.

5.2. **Means of Power**
Having identified a variety of possible countermeasures the next step is to categorize them as means of soft or hard power in accordance with Nye’s definition, which was introduced in section 2a, and the application of the theory onto social media suggested in section 2c. An important observation is that it is not uncommon that certain actions employ elements of both, soft and hard power thus making a clear-cut categorization impossible. As noted in section 2 measures of hard power often also include elements of attraction making it difficult to classify them. Also, the very same type of action can lead to a variety of results depending on its focus during execution. Thus the same countermeasure can be an exercise of both, hard and soft power.

Following countermeasures were identified as measures that predominantly employ elements of coercion or payment and thus are categorized as tools of hard power in this step:

<table>
<thead>
<tr>
<th>Countermeasure (CM)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CM1: Shutting down or limiting access</td>
<td>Physical demonstration of power</td>
</tr>
<tr>
<td>CM2: Shutting down elements within social media</td>
<td>Physical demonstration of power</td>
</tr>
</tbody>
</table>
CM3: Attacking media outlets

Physical demonstration of power

CM4: Automated spamming the Twitter feed

Aims to disturb the opposition’s operations

CM5: Manually spamming the Twitter feed

If aims to disturb the opposition’s operations

CM6: Trending other topics

If aims to disturb the opposition’s operations

CM7: Organized spamming of blogs

Aims to disturb the opposition’s operations

Following countermeasures were identified as measures that predominantly seek to gain influence by attraction and thus are categorized as tools of soft power in this step:

CM5: Manually spamming the Twitter feed
If aims to demonstrate support for the government amongst the population

CM6: Trending other topics
If aims to demonstrate popularity of other subjects

CM8: Defaming the opposition with facts
Aims at raising support for own cause by discrediting the opposition.119

CM9: Defaming the opposition with forged information
Aims at raising support for own cause by discrediting the opposition.

CM10: Discussion
Aims to demonstrate support for the government and amending the discourse into a pro-government direction

119 “Exaggerated claims about the imminence of Saddam Hussein’s weapons of mass destruction and the strength of his ties to Al Qaeda may have helped mobilize domestic support for the Iraq war, but the subsequent disclosure of the exaggeration dealt a costly blow to British and American credibility. Under the new conditions more than ever, the soft sell may prove more effective than a hard sell.” In: Nye (2004) p. 8
CM11: Blogs, groups etc. Aims to demonstrate support for the government and amending the discourse into a pro-government direction

Following the reasoning that the distinction between hard and soft power can be ambiguous, the following step is to rank the identified countermeasures in a “continuum of power”.

Because there is no definitive method of measuring the “softness” or “hardness” of power such a ranking procedure is highly subjective, thus the following results are merely a suggestion. Applying a different approach some of the countermeasures could be deemed harder or softer. It is suggested that the main indicator for hardness of power is the amount of coercion that is included in the measure.

Countermeasures 1 and 2 are clearly examples of exercise of very hard power; these are the demonstration of the uttermost coercion possible within cyberspace. Countermeasure 3 attacks a third party and aims to hurt the opposition indirectly meaning that the opposition could continue operating. Thus this countermeasure is ranked slightly softer, however the financial aspect puts this mean clearly within the realm of very hard power.

Countermeasure 4 can actively interfere with the opposition’s activities and is thus deemed being exercise of hard power. The interference is near physical and includes a fairly high degree of coercion.

Countermeasures 5 and 6 are comprised of both - hard and soft power. Depending on how these methods are used they may be classified slightly harder or softer. These methods employ both, coercion by interference and attraction by demonstrating human commitment.

Countermeasure 7 is similar to countermeasure 4. However it is not directed at the opposition’s operations in the same way and is thus deemed softer than countermeasure
4. As stated earlier blogs are not used to disseminate real-time information but are rather platforms for a political discourse. Thus only the opposition’s discussion is disturbed, not its operation.

Countermeasures 8 and 9 are very similar in their effects and in many cases it is hard for outsiders to say which one is which. These actions aim to defame the opposition and at the same time offer oneself as the trustworthy alternative. The latter places these countermeasures within exercise of soft power, however the element of attack against the opposition adds a coercive element.

Countermeasures 10 and 11 are also very similar and are by definition means of soft power. These categories represent the far most soft power that can be exercised within social media, as they do not seek to coerce.
6. Results and Discussion

6.1. How to exercise power in Social Media

“Shaping public opinion becomes even more important where authoritarian governments have been replaced by new democracies.”

*Joseph S. Nye Jr.* 120

This study has revealed a number of methods that were used to counter the opposition’s operation and coordination within social media. These countermeasures were ranked within a continuum of power depending on the amount of coercion they employ.

Shutting down access to the Internet or to parts of it as well as pressuring owners of social media platforms to delete oppositional groups were the methods of uttermost hard power that were identified in the course of the study. The use of these tools of hard power is however likely to result in strong reactions inside the country as well as from the international community. Exercise of power in this way conflicts with western ideas of freedom and democracy.

Automated spamming of Twitter feed is a method that applies much less hard power than the aforementioned. This method is very effective in disrupting ad-hoc organization. However it does not possess much soft power either, because it is an inconvenience and the automation is easily identified.

A number of methods use a combination of hard and soft power, depending on how these methods are used either hard or soft power will prevail. These methods are manual spamming or trending unrelated topics or contrary opinions on Twitter, manual spamming of blogs and other social media platforms. These methods can be regarded as fairly effective because they efficiently disrupt oppositional discussion or even ad-hoc organization and at the same time show the unpopularity of oppositional action.

Defamming the opposition with either facts or forged information, pro-government position in discussions and blogs are classified as use of soft power. As it is typical for

120 Nye (2004) p.6
means of soft power these methods aren’t immediately effective. They have no power to disrupt the oppositional discourse but can amend it in the long run. These methods rarely have immediate results and thus their success can only be verified or disproved after they have been applied over a longer period.

The suggested ranking is summarized and visualized in chart 3. In accordance with the analysis some of the measures are granted a range within the chart rather than a point. This ranking, however, is not absolute. Depending on the individual situation countermeasures can be “harder” or “softer”.

![Diagram of countermeasures in terms of hard and soft power]

Chart 3. Countermeasures in terms of hard and soft power

### 6.2. Discussion

Overall the study has resulted in a set of methods that can be used to oppose a movement growing within social media. The classification of the different means provides for an estimate of what reaction the actions might trigger. Knowing what can be done also raises awareness amongst those taking part in a movement, those trying to constrain it as well as outsiders wishing to receive a clear, more or less unbiased, picture of the events.

Campaigning within social media and exercising power within may seem very ambiguous. The near-anonymity delivers particularly a great potential for exercising
various types power. However there are a number of pitfalls to avoid. One of these pitfalls can be traceability or a lack of thereof. A lot of times it is difficult to trace a piece of information back to its source. A piece of information can quickly become popular, no matter whether it is true or not. Even if it is discredited at a later point, the damage to its subject's reputation will already be done, although we can assume that many people are aware that information on the Internet is often not very reliable.

At the same time one can be unaware of traceability: Information on the Internet is traceable in a way many users do not realize. It is simply a matter of effort and commitment whether a piece of information will be traced to its origin. For example a rumor that is traced back to its origin can boomerang and dishonor its starter.

The difference in cyberspace is that information, truthful or not, spreads much faster than through conventional media. Once posted online it might travel to different websites and platforms. At these different stations the information might be posted as-is or slightly amended resulting in a vast amount of data concerning one single subject. The results sometimes are similar to the popular childhood game of “Chinese whispers”: A whispered message is passed by a line of people and the longer the line the more the message becomes modified. Often the message received by the last person in line has little to do with the original message. Even if the information is discredited afterwards, traces of it will persist in different forms accessible to anyone who can use a search engine such as Google.

A similar issue exists for vulnerability of systems such as e-mail servers. With enough technical know-how e-mail servers can be hacked and their revealing content may be published for everybody to see. On the other hand it's likewise possible to forge e-mail conversations and present them as originals.

Exercising hard power online can also be problematic, partly because the Internet is sometimes thought of as a universally free zone compared to open seas in naval terminology. Restricting access to the Internet or to parts of it generally causes criticism by the international community, and can foster resentment and even riot within the parts of the population that were previously ambiguous towards political issues.
Similarly, the use of technically rather uncomplicated tools such as bots on Twitter can result in aggravation amongst the less tech-savvy users simply because they might experience this method as a large-scale and technically advanced attack. This would have a David facing Goliath effect that might be not desirable in a society that values democratic values.

### 6.3. Criticism

This study presents one of many possible ways to research exercise of power within social media. Depending on a scholar’s individual starting point and focus a study estimating to answer similar questions might be designed differently. For example, using a narrower definition of social media and relevant events would allow for a more in-depth analysis of exercise of power with social media. However it would also have disadvantages compared to the broader scope that were chosen for this study: The elements that affect social media directly but are conducted outside of it would have to have been neglected entirely. This would have presented an in-depth picture rather than an overall overview.

This study can also be criticized for leaving out more detailed descriptions of technical solutions that are used for exercising power within cyberspace. However the priority was to present a study written for a broader public rather than providing in-depth discussion of technical tools or solutions.

Another possible criticism is that the presented study focuses on a single case. While scrutinizing a single case allows for in-depth research it does not deliver any comparison to other comparable cases and thus allows for significantly less generalization.

### 6.4. Recommendation for Future Studies

This study can provide a foundation for further research as it provides an overall classification of methods that can be used to counteract the growth of an opposition online. As noted earlier, a single-case study is less generalizable than a comparative study and thus it is suggested to compare the results of this study with a number of other cases where social media was used to support a political struggle.
The results of this study can also be used to develop a comprehensive framework for observation of growth of political movements within social media. Such a framework would be useful when scrutinizing potential ways to democratization in technologically modern societies. This study can also be a starting point to research technical solutions lying behind the different means or to scrutinize the human reactions to various methods that were observed in this study.
7. References

**Published books**


**Articles**


Lonkila, Markku (2012). "Russian protest on- and offline; the role of social media in the Moscow opposition demonstrations in December 2011”. Finnish Institute for Foreign Affairs.


Wagner, Christian (2005) "From Hard Power to Soft Power? Ideas, Interaction, Institutions, and Images in


News


Gazeta. "Вслед за «Коммерсантом» в день митинга DDoS-атаке подверглись «Эхо», «Дождь» и Slon.ru". ("Kommersant, Ekho, Dozhd and Slon.ru were subjects to a DDoS attack on the day of the protest")


Internet / Blogs


LinkedIn. (2011) “100 Million members and counting...” LinkedIn blog. Posted: 03/22-2011 Retrieved: 05/18-2012 (http://blog.linkedin.com/2011/03/22/linkedin-100-million/)


Official statements / speeches
Appendix

Scr1a - Web elections website that was streaming the live feed from poll booths: webvybory2012.ru/#=_=

Scr1b - A number of archived streams from polling stations during presidential elections can be requested here: epgu.gosuslugi.ru/pgu/service/-1000000413_418.html#_description

Scr2 - News outlet “Utro” reporting about the “attempted Twitter revolution”: www.utro.ru/articles/2011/12/05/1015089.shtml
Scr3 - Web users coined the term “network hamsters” on Twitter. The term was coined on Twitter and the search parameters were “сетевые хомячки” between 12/04-2011 and 05/10-2012, tweets only.

Scr4 - Example for a Twitter bot: twitter.com/#!/AlyssaVasquez6

Scr5a - Example for possibly manually conducted spamming: twitter.com/#!/limax_08
**Scr 5b - History of Jimax_08’s account**

**Scr6 - Pro-Kremlin tweets, examples, hashtag: #ЯэПутина**

**Scr7a – Hijacking the hashtag used by the opposition, hashtags: #маршмиллионов #6мая**
Scr7b - Example of unrelated spam, hashtag: #Маршмиллиона

Scr8a - Spamming with the #Мяу hashtag, user Wane Baryshev suggests that the hashtag was trended by those wishing to stop demonstrations.

Scr8b – Spamming with the #Мяу hashtag.
**Scr9** - Victory Day-related topics trending: “С Днем ПОБЕДЫ”

**Scr10** - Example: oppositional group on Facebook, “Belaya Lenta”: 
facebook.com/groups/161227823979387

**Scr11** - Example: oppositional group on Vkontakte called “Honest Elections”: 
vk.com/chestnye_vybory
Exercising Power in Social Media

Margarita Jaitner

Scr12 - Example: oppositional group on Vkontakte “White Ribbon”:
vk.com/belayalentagroup

Scr13a - Alexey Navalny’s RosPil on Vkontakte: vk.com/rospil

Scr 13b - History of Alexey Navalny’s RosPil on Vkontakte
Exercising Power in Social Media
Margarita Jaitner

**Scr14** - Alexey Navalny’s Facebook group
www.facebook.com/pages/Алексей-Навальный-Трансляция-из-ЖЖ/

**Scr15** - Example of how content sites are used in groups within social networking sites, owner of the group vk.com/cestnyi_vibor posts Youtube video

**Scr16** - The linked video:
www.youtube.com/watch?v=VlhHCV6MU9c “For Russia or for Putin”
Exercising Power in Social Media
Margarita Jaitner

Scr17a - Event “White Square” with 3.792 guests “going” and 504 users marked as possibly participating, also example of the guest list

Scr17b - One of the guests of the event in scr18, no obvious ties to Russia

Scr17c - Another guest of the event “White Square”, no obvious ties to Russia
Exercising Power in Social Media
Margarita Jaitner

Scr18a - News outlet Ridus discussing the guest list of the event “White Square”

Scr18b - Members of the event “White Square” discussing the guest list

Scr19 - Alexey Navalny shares a Youtube video: “Electoral fraud in Moscow, area 2501” navalny.livejournal.com/2011/12/04
Scr20 - Blog post “Navalny accused of buying supporters on Vkontakte” ru-compromat.livejournal.com /tag/"Единая20%Россия"

Scr21 - Example for use of media in blogs: Oppositional blogger Zhenya Chirikova’s blog post on police brutality during demonstrations. jenya-khimles.livejournal.com/tag/6%20мая

Scr22 - Example of vulgar comments in Navalny's blog navalny.livejournal.com /564810html?page=6#comments
**Scr23** - Example of opposition using the term “Yedroboty” in a blog called barrycada – the barricade.
barrycada.
livejournal.com/7966.html

**Scr24a** - Blogger Eduard Kot (edvvvard) post on organized spamming by “Nashi”
edvvvard.
livejournal.com/22068.html

**Scr24b** - Blogger Eduard Kot (edvvvard) post on organized spamming by “Nashi”
edvvvard.
livejournal.com/22068.html
Scr25a - Video from polling station indicating electoral fraud
www.youtube.com/watch?v=t7ZU0Rco3zs

Scr25b - Video from polling station indicating electoral fraud
www.youtube.com/watch?v=2mqRtSo41tw

Scr26 - Reportage on electoral fraud made by a private online news outlet:
www.youtube.com/watch?v=2EMyx00C9wU
Scr27a - Alleged police brutality during a demonstration on Pushkinskaya Square 03/05-2012: www.youtube.com/watch?v=tMMCzbAN5Ec

Scr27b - Alleged police brutality during a demonstration on Pushkinskaya Square on 03/05-2012 www.youtube.com/watch?v=RMDDWE1L7Is

Scr27c - Alleged police brutality during a demonstration, OMON on Tverskaya on 03/05-2012 www.youtube.com/watch?v=baTBCncYYmw
Exercising Power in Social Media

Margarita Jaitner

Scr28a - User riggamortis1 live stream from demonstrations in Moscow ustream.tv/channel/ reggamortis1

Scr28b - User riggamortis1 live stream from demonstrations in Moscow ustream.tv/channel/ reggamortis1

Scr29 - No popular Russian political vlogs found www.youtube.com/results?search_query= влог
Exercising Power in Social Media
Margarita Jaitner

**Scr30a** - Allegedly, e-mails from a number of pro-Kremlin activists’ accounts published online: slivmail.com/

**Scr30b** - Allegedly e-mails from Kristina Poputchik’s e-mail account published online: potupchik.com/

**Scr31a** - Op_Russia’s Twitter feed: twitter.com/op_russia
Exercising Power in Social Media

Margarita Jaitner

Scr31b - “5 min TANGO DOWN” for taking down Kremlin’s website and allegations regarding attack on Ekho Moskvy and Kommersant on OP_Russia’s Twitter feed

Scr32a – Web site offering resources and help for protesters: helpwall.info

Scr32b: Hashtag #help496 in use on Twitter