The Censorship of Extremist Content in the Russian Internet

Daria Korenyushkina 10394699

Sonia Kolasinska 10394605

University of Amsterdam

November 2012

The control of the Russian internet is not considered one of the prime examples of strict political censorship. Censoring problematic content online has not been legally introduced in Russia, and it usually is targeted at only selected materials online. As Ronald Deibert and Rafal Rohozinski claim, "In RUNET, control strategies tend to be more subtle and sophisticated and designed to shape and affect when and how information is received by users, rather than denying access outright." (206) However, on 1 November 2012 the Russian government passed the Law on the Protection of Children From Information Detrimental to Their Health and Development and published an official blacklist of blocked websites and internet addresses[1]. Organizations supporting freedom of information such as Reporters Without Borders fear that this law poses a threat to freedom of speech in Russia and would allow for censorship of content not necessarily violating the children protection law. Since the law has been passed just recently, a research of censorship related to this particular legislation would most probably not give any results yet.

Nonetheless, it is possible, and hopefully fruitful, to look into the past legislations introduced by Duma, and their execution in cyberspace. Federal Law on Counteraction of Extremist Activity introduced in 2002 is an interesting case. One of its aims is preventing, identifying and eliminating extremist activity, "including the disclosure and subsequent removal of the reasons and conditions promoting extremist activity"[2]. Thus, it provides the legislative basis for the disclosure and suppression of the extremist materials, including online content.

Even though the Russian government published a specific, official list of materials with extremist content (currently it consists of 1480 items), the representatives of the OpenNet Initiative fear that "under this law, effectively any Web site hosting a forum section is vulnerable. An individual needs only to post hate or extremist (or other objectionable) speech in a forum and report it to the authorities before a moderator notices it to kick off legal prosecution."[3] It is, therefore, interesting to investigate whether the 2002 law was executed effectively in cyberspace and if the government does in fact remove forbidden content thoroughly. The research will focus on the

[1] Internet Access Barred as Wave of New Legislation Threatens Freedom of Information"on *Reporters Without Borders* website.
[2] Federal Law No. 114 FZ On Counteraction of Extremist Activities.
[3] Country profile: Russia on *OpenNet Initiative* website.

extremist materials online: 62 out of 1480 materials on the federal list of extremist materials are websites and blogs[4]. The research investigates whether these 62 URLs are still available in Russia, and looks for the first-generation control in which access to certain websites is denied by directly blocking access to servers, domains, keywords, and IP addresses (Deibert, Rohozinski 212). If a website turns out not to be accessible, the type of error displayed is checked. This provides an insight into the way in which the forbidden content is being removed or blocked, as well as into the level of transparency of Russian internet censorship.

On the basis of the results, one can estimate the rigorousness with which the government implements its legislation regarding forbidden content online, and perhaps attempt to make predictions about the implementations of the November 2012 Law on the Protection of Children.

INTERNET CENSORSHIP IN RUNET

It is crucial to understand that in Russia censorship has not been legally introduced in the country, yet "the Russian government actively competes in Russian cyberspace employing second- and third-generation strategies as a means to shape the national information space and promote pro-government political messages and strategies."[5] The OpenNet Initiative identified only selective filtering of political and social content, with low transparency and low consistency of censorship. This means that the research of the censorship in Runet is quite challenging, since the practice of censoring content is usually disguised and there are no predictable, clear patterns of control.

One of the features of the Russian internet censorship, and the main focus of this research, is the fact that "the Russian judicial practice has accumulated substantial experience in the "war on Internet extremism." (Yudina) The Federal Law No. 114-FZ of July 25, 2002 On Counteraction of Extremist Activity defines extremist materials as "the documents intended for publication or information on other carriers which call for extremist activity or warranting or justifying the need for such activity, including the works by the leaders of the National-Socialist Worker's Party of Germany and the Fascist

[4] The Federal List if Extremist Material (Федеральный список экстремистских материалов) on the Ministry of Justice website (http://www.minjust.ru)
[5] Country profile: Russia on *OpenNet Initiative* website.

Party of Italy, publications substantiating or justifying national and/or racial superiority, or justifying the practice of committing military or other crimes aimed at the full or partial destruction of any ethnical, social, national or religious group."[6] The law states that any extremist activity of social and religious organizations, other organizations, or physical persons should be discovered and suppressed.

METHODS

This research aims at investigating the effectiveness of the Russian law enforcement in combating cyber hate. The implemented research strategy consisted of two major steps: building a list of the extremist websites in Runet and testing whether they are accessible in Russia and in the Netherlands.

For building the URL list the editorial approach was used; the federal list of extremist materials[7] was used as a source for the list. All of these websites should not, in theory, be available in Russia, since the Federal Law On Counteraction of Extremist Activity states that "materials included in the federal list of extremist materials shall not be distributed around the territory of the Russian Federation. Persons guilty of the illegal manufacture, spread and storage of the said materials with the aim of subsequent distribution shall be brought to book in administrative or criminal proceedings"[8]. This research aims at investigating whether this is really the case and the Russian government has effectively implemented this legislation in Runet.

The federal list of extremist materials also contained single items such as articles, texts, video, and audio files published on websites or social media platforms. These items were excluded from the sample, since the entire websites on which the forbidden content is published are not listed as extremist and, according to the law, can remain accessible. For example, the list mentions extremist content published on the largest social network in Runet www.vkontakte.ru (www.vk.com) 78 times. However, the platform itself is not blocked and only certain videos, audio files, photos and texts that were considered extremist had to be removed, following the court decision.

[6] Federal Law No. 114 FZ On Counteraction of Extremist Activities.
[7] The Federal List if Extremist Material (Федеральный список экстремистских материалов) on the Ministry of Justice website (http://www.minjust.ru)
[8] Ibid.

Therefore, only the websites that are fully considered extremist were included in the sample. The URL list for the analysis contains 62 URLs (Table 1). One should keep in minds that the biggest limitation of the research is the credibility of the web addresses given on the federal list of extremist materials. It is possible that some of them are misspelled on purpose, in order not to advertise the forbidden internet resources to the internet users. (Yudina) In further research it would be necessary to compare the list published on the official website of Russian Ministry of Justice with the archived issues of "Rossiyskaya Gazeta", the official newspaper of the Russian government.

Table 1. The URL list for Analysis.

URLs Retrieved	Number on the federal list of extremist materials
abuhurayra.wen.ru	851
fisadilillahi.com	848
http://abror.info/	1454
http://baboons.narod.ru	1459
http://djamagat.wordpress.com	1036
http://dobroslav.onestop.net/	717
http://guraba.info/	1473
http://haamash.wordpress.com/	1476
http://iepifanz.liveiournal.com/	776
http://infokavkaz.com	1035
http://ipvnews.org/	1072
http://jamagat.wordpress.com/	1476
http://kavkazanhaamash.com/meny.html	1038
http://kavkazinform.com/	1382
http://milleti-ibrahim.info/ru/	1408
http://mirtesen.ru/group/30405959426/blog/4322601982	415
http://soprotivlenie.marsho.net/	1474
http://tovbin.hoter.ru/wiki/1126/316	718
http://vdagestan.com	1428
http://vdagestan.info	1037
http://vilayatiu.co.cc	1039

http://www.doloyputinism.ru	1145
http://www.fank.ru/	365
http://www.ingushetia.org	709
http://www.islamdin.biz/	1377
http://www.islamdin.com/	704
http://www.national-socialist.tk/	432
http://www.newp.org/nazi/	432
http://www.rusigra.info	582
http://www.rusigra.livejournal.com	583
http://www.rusigra.org	581
http://www.sakh-88.nm.ru/	257
http://www.zhurnal.lib.ru/	381
http:/czeczenia-rus.blog.onet.pl/	1427
http:/Russia.bloodandhonour.net	626
http:/www.ichkeria.info	784
INGUSHETIYA.RU	276
kavkaz.org.uk	985
kavkaz.tv	985
kavkazcenter.info	985
kavkazcenter.net	985
kavkaznews.com	985
vik23.livejournal.com	264
www.3a_pycb.livejornal.com	586
www.44x2.com	871
www.barbos111.narod.ru	381
www.BelPar.org	624
www.chechentimes.net	462
www.djamaattakbir.com	1081
www.dpni-kirov.org	592
www.hunafa.com	663
www.kavkazcenter.com	985
www.KavkazChat.com	627
www.limonka.nbp-info.ru	1031
www.livainternet.ru	954
www.nbp-info.ru	969
www.pat-index.livejournal.com	614

www.resistance88.com	1048
www.rusinfo.org	587
www.sbl4.org	585
www.Sovinform.ru	719
www.TATARLAR.ru	955

For checking the accessibility of the websites the Censorship Explorer and ten proxies located in Russia were used. (Appendix 4) First, the URL of a Russian search engine www.yandex.ru, which is blocked neither in Russia nor in the Netherlands, was fed through the Censorship Explorer in order to check if the proxies work properly. Afterwards, each of the sites was run through the tool and the responses from at least three proxies were obtained. Each website that received the "200 OK" response code from at least one of the proxies was run for the second time with the use of "Also display the retrieved HTML" option. This was done in order to check whether the specific content of the website was also accessible. The websites that received error or "connection failed" response codes were categorized as inaccessible.

RESULTS AND ANALYSIS

In theory, according to the Law on Counteraction of Extremist Activity, all 62 websites listed by the government should be removed, because they disseminate extremist ideas. Yet, this research shows that not all investigated websites were deleted or blocked. It is possible to classify the results into three categories: *accessible*, *inaccessible*, and *mixed*.

Accessible

The websites that displayed the "200 OK" response code from at least one of the proxies located in Russia were classified as accessible. This research shows that 35 out of 62 forbidden websites are still accessible in Russia. (Appendix 2) The content of the accessible websites is both in Russian and in English.

Due to time limitations, the thorough content-analysis of the available sites could not be conducted. However, many of them seemed to contain calls for extremist activity, justifying national and/or racial superiority, or justifying the practice of committing

crimes aimed at any ethnical, social, national or religious group. Yet, they have not been deleted.

The sites that contained information clearly not connected to extremism were categorized as sites with unrelated content. Many of them contained information about the sale of a domain. Interestingly enough, the website www.dpni-kirov.org appears to be a corporate website of HR DEVELOPMENT ASSOCIATION "Alpha Resource Group". None of the websites containing unrelated content seemed to contain information about politics or government. Yet, they are still included on the blacklist of the extremist material.

Inaccessible

The websites that received a response code different than "200 OK", which were usually error response codes, were classified as inaccessible. The research shows that 26 out of 62 forbidden websites are inaccessible in Russia. (Appendix 3) Surprisingly, 19 of them are also inaccessible in the Netherlands. (Appendix 1)

The fact that the majority of the websites not accessible in Russia is also not accessible in the Netherlands indicates that this is not an instance of first generation censorship. Rather, the websites were probably taken down or deleted entirely. Also, none of the websites received the 403 Forbidden response code from a Russian proxy that would clearly identify blocking. The possibilities of finding the ways in which these websites were made inaccessible are limited, since the response codes from different proxies differ from one another. To nevertheless gain an insight into different possibilities, the received HTTP status codes and their definitions are listed below[9].

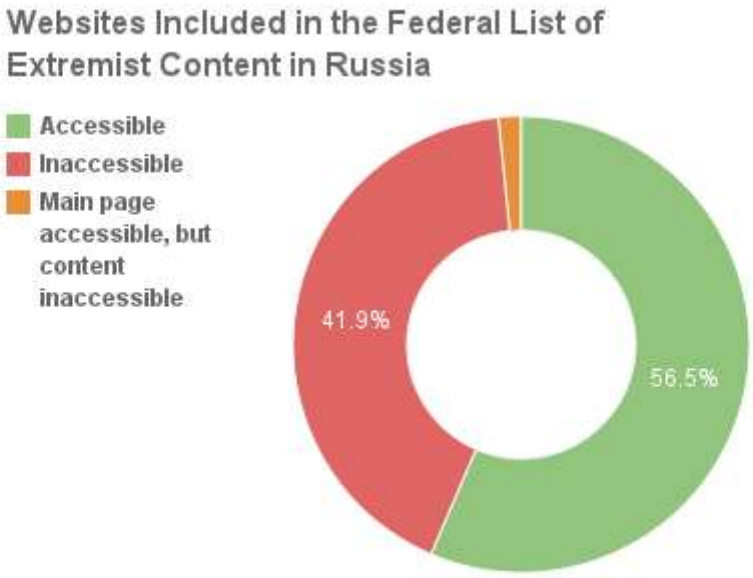
200 Server down by HAVP	HAVP is an antivirus proxy server. The proxy may be down.
200 DNS error by HAVP	HAVP is an antivirus proxy server. The proxy may be down.
302 Found	This is an example of industry practice contradicting the standard. The HTTP/1.0 specification (RFC 1945) required the client to perform a temporary redirect (the original describing phrase was "Moved Temporarily")
301 Moved Permanently	This and all future requests should be directed to the given URL.

[9] Descriptions taken from the Wikipedia page *List of HTTP status codes* and from mybroadband forum.

400 Bad Request	The request cannot be fulfilled due to bad syntax.
404 Not Found	The requested resource could not be found but may be available again in the future.
410 Gone	Indicates that the resource requested is no longer available and will not be available again. This should be used when a resource has been intentionally removed and the resource should be purged. Upon receiving a 410 status code, the client should not request the resource again in the future. Clients such as search engines should remove the resource from their indices.
503 ERROR	The server is currently unavailable (because it is overloaded or down for maintenance). Generally, this is a temporary state.
504 DNS Name Not Found	*(Definition not found)*
504 Gateway Timeout	The server was acting as a gateway or proxy and did not receive a timely response from the upstream server.
connection failed (60)	Internet connection problem
connection failed (61)	Internet connection problem

Mixed

The website www.kavkazcenter.com is the only website that might have been blocked. However, not by usual means. The website itself seems to be accessible; the main page and five pages in five different languages that the main page links to received 200 OK responses from Russian proxies. However, the retrieved HTML through Russian proxies showed that all the internal links of the website go to the web pages with the following text: “Not Found. The requested URL /.../... was not found on this server” whereas the HTML retrieved through proxies in the Netherlands showed that all the same links worked well and directed to the web pages with rather rich content that seems to be connected with extremism. Besides, the website has five mirror sites (www.kavkaznews.com, www.kavkaz.tv, www.kavkaz.org.uk, www.kavkazcenter.net, www.kavkazcenter.info) which are not accessible in Russia but accessible in the Netherlands. (Appendix 1)



Special Cases

Among the results there was one website that redirects the user to a different website, in this case to the official site of the Ministry of Justice. The www.zhurnal.lib.ru was a website of Maxim Moshkov's Library, one the largest online libraries in Runet. It was included in the federal list of extremist materials because some texts found in the library were considered extremist. In consequence, Maxim Moshkov had to move the library to another domain. To express his discontent about the government's action, Moshkov made a redirect from the banned site to the official site of the Ministry of Justice. The ISP "Netbynet" which was to block www.zhurnal.lib.ru temporarily blocked the official site of the Ministry of Justice because of the redirect[10].

Another special case among the results is a website www.44x2.com. It is the only website in this sample which openly states that it was closed by court order. It displays a message "WE ARE CLOSED BY COURT ORDER. WE APOLOGIZE FOR THE INCONVENIENCE CAUSED" in several languages. The fact that only one out of 26 inaccessible sites openly gives a reason for being shut down is in line with the OpenNet Initiative's claim about the low transparency of the Russian internet censorship.

[10] "Провайдер Netbynet заблокировал сайт Минюста" on *Lenta.ru* website.

CONCLUSIONS

The research shows that the implementation of the Law on Counteracting Extremist Activity in Russian internet has not been done rigorously. Even though some websites display extremist content, they are still available online. The research also did not detect any instances of the first generation control. That means that online content, at least content officially listed as forbidden, is controlled in different ways. The majority of investigated websites was most probably taken down or deleted entirely, instead of blocked only on the territory of Russia. In addition, researchers and reporters wishing to monitor the instances of censorship in Russia, for example after the introduction of the Law on the Protection of Children, will face a challenge of very low transparency of the Russian internet control. It is not common to see a message clarifying the reason for a website being deleted. It is interesting that the blacklist of extremist content is official and publically available, whereas the execution of the law is not that transparent.

REFERENCES

Deibert, Ronald, Rohozinski, Rafal. "Control And Subversion in Russian Cyberspace," *Access Controlled*. Cambridge, MA: MIT Press, 2010. 15-34

"Federal Law No. 114 FZ on Counteraction of Extremist Activities*". Legoslationline.* 2002. Organization for Security and Co-operation in Europe. 5.11.2012. <http://www.legislationline.org/documents/id/4368>

"Internet Access Barred as Wave of New Legislation Threatens Freedom of Information". *Reporters Without Borders*. 2012. 3.11.2012. <http://en.rsf.org/russia-internet-access-barred-as-wave-of-01-11-2012,43627.html>

"List of HTTP status codes". *Wikipedia*. 8.11.2012. <http://en.wikipedia.org/wiki/List_of_HTTP_status_codes>

Mybroadband forum, thread: HAVP server down. *Mybroadband*. 8.11.2012. <http://mybroadband.co.za/vb/showthread.php/82113-HAVP-server-down>

OpenNet Initiative. The Citizen Lab at the Munk School of Global Affairs, University of Toronto; the Berkman Center for Internet & Society at Harvard University; the SecDev Group (Ottawa). 5.11.2012. <www.opennet.net>

Yudina, Natalia. "Virtual Anti-Extremism: Peculiarities of enforcing the anti-extremist law on the Internet in Russia (2007–2011)". *Sova Center for Information and Analysis*. Ed. Alexander Verkhovsky. 2012. Panorama Center for Information and Research and the Moscow Helsinki Group. 5.11.2012. <http://www.sova-center.ru/racism-xenophobia/publications/2012/09/d25322/>

"Провайдер Netbynet заблокировал сайт Минюста". *Lenta.ru*. 2012. 8.11.2012 <http://lenta.ru/news/2012/10/10/blockeverything/>

"Федеральный список экстремистских материалов". Официальный сайт Министерства Юстиции РФ. 2012. Министерство Юстиции РФ. 7.11. 2012. <http://www.minjust.ru/nko/fedspisok>