© Laboratorium: Russian Review of Social Research. 2019. 11(3):46–70
DOI: 10.25285/2078-1938-2019-11-3-46-70

FROM CITIZEN INVESTIGATORS TO CYBER PATROLS: VOLUNTEER INTERNET REGULATION IN RUSSIA

Françoise Daucé, Benjamin Loveluck, Bella Ostromooukhova, Anna Zaytseva

Françoise Daucé, Centre for Russian, Caucasian and Central European Studies (CERCEC, EHESS–CNRS). Address for correspondence: EHESS, 54 Boulevard Raspail, 75006 Paris, France. francoise.dauce@ehess.fr.

Benjamin Loveluck, i3-SES, Télécom Paris. Address for correspondence: Télécom Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France. benjamin.loveluck@telecom-paris.fr.

Bella Ostromooukhova, Eur'Orbem, Sorbonne University. Address for correspondence: Sorbonne Université, 108 Boulevard Malesherbes, 75017 Paris, France. ostrob@gmail.com.

Anna Zaytseva, Laboratory LLA-CRÉATIS, University of Toulouse–Jean Jaurès. Address for correspondence: Université Toulouse–Jean Jaurès, Département des langues étrangères, 5 Allée Antonio Machado, 31100 Toulouse, France. anna.zaytseva@univ-tlse2.fr.

Research for this article was conducted within the ResisTIC ("Resistance on the Internet: Criticism and Circumvention of the Digital Borders in Russia") Research Program, with funding from the French National Research Agency (ANR).

State control over the Russian internet (Runet) has been enforced by dedicated administrations and private digital entrepreneurs since the early 2010s. Along with them, groups of digital vigilantes report on "negative" online content and claim to be fighting against activities considered to be criminal or contrary to social norms. However, their ideological convictions and moral supports are diverse and changing. This article analyses two nonprofits: Molodezhnaia Sluzhba Bezopasnosti (MSB, Youth Security Service) and Liga Bezopasnogo Interneta (LBI, Safe Internet League), which sponsors an emergent "cyber Cossack" movement. MSB, which can be referred to as "citizen investigators," has developed a high degree of technical and legal experience and cooperates actively with the police. LBI promotes a conservative vigilantism to ensure "virtuous browsing," with a strong focus on education. In March 2019 hearings at the Russian Civic Chamber on a bill addressing the activity of *kiberdruzhiny* (cyber patrols) revealed tensions between the "politically involved" (Duma members and *kiberdruzhiny*'s organizations) supporting the bill and the "experts" (representatives of internet companies and security specialists) opposed to it alleging the proposed law's inefficiency. A third group, the supporters of a free and democratic Runet, is absent from the official debates but speaks out on social networks and through independent media against the development of civil surveillance.

Keywords: Russia; Digital Vigilantism; Internet; Cyber Patrols; *Kiberdruzhiny*; State Control; Surveillance

In the fall of 2018 two United Russia deputies, Adalbi Shkhagoshev and Oleg Bykov, introduced into the State Duma a bill addressing the activity of *kiberdruzhiny* (cyber patrols), transferring to the digital world the law on *druzhiny* passed in 2014.[1] The background memorandum to the bill asserts that these patrols "will combat internet dissemination of information prohibited in Russia, particularly concerning war propaganda and incitement to national, racial, or religious hatred."[2] According to this text, the patrols would be performed by unpaid volunteers. The bill's two supporters claimed that a law was required to enable law-enforcement agencies to respond more effectively to crime-related information (*obrashcheniia*) provided by citizens. The proposal aroused some scepticism even within the Duma. Deputy Leonid Levin feared that "formalizing this movement on a legal basis would transform a popular initiative into an executive obligation, contradicting the very idea of voluntary participation."[3]

Why this sudden push to pass the law? Whereas the Russian internet developed fairly freely in the 2000s (Deibert and Rohozinski 2010), this bill was introduced in the wake of a considerable strengthening of state control over the internet since the early 2010s (Oates 2013; Soldatov and Borogan 2015; Tselikov 2014). Regulation has been entrusted to dedicated administrations (such as the Roskomnadzor agency for communication surveillance), private digital entrepreneurs (Vendil-Pallin 2017), as well as citizen initiatives from civil society. Networks of volunteers to regulate the Russian internet (often refered to as Runet[4]), which have existed in various forms since the early 2000s, have increased in number and taken on new shapes. These forms of digital surveillance involve ordinary citizens who report on criminal content online. They can therefore be associated with digital vigilantism (Loveluck 2016, 2019), which implies private practices of surveillance, deterrence, and online punishment. These are carried out in the name of justice, order, and security, in response to offences against civility or morality, crimes or perceived injustice.

---

[1] Federal Law No. 44-FZ of April 2, 2014, Concerning the Participation of Citizens in the Maintenance of Public Order supposes the existence of "people's volunteer squads" (*dobrovol'nye narodnye druzhiny*) and "voluntary associations specializing in the maintenance of public order" (*obshchestvennye ob"edineniia pravookhranitel'noi napravlennosti*). Citizens participate in maintaining public order in "cooperation with the police and other law-enforcement agencies, with the state authorities, and local self-government bodies," but the actions of voluntary patrols can in no case be substituted for the competence of the police and other law-enforcement agencies or the competence of the state authorities and local self-government bodies (Art. 4). Patrol members are not entitled to carry weapons and their use of physical force is strictly limited to situations where their life is in danger (legitimate self-defence). The state authorities and local self-government bodies, for their part, are required to "support citizens and their associations participating in the maintenance of public order" and "create favorable conditions for the activity of the people's patrols" (Art. 6).

[2] Using the categories specified in the Federal Law No. 149-FZ On Information, Information Technologies, and Information Protection.

[3] "Kiberdruzhiny ot 'Edinoi Rossii' budut iskat' v internete nelegal'nyi kontent," BBC News Russia, November 2, 2018. https://www.bbc.com/russian/news-46074279.

[4] For an analysis of the imaginaries of Runet, see Asmolov and Kolozaridi (2017).

These online surveillance groups are diverse and challenge the usual models of citizen participation in law enforcement. They all claim to be fighting against activities considered to be criminal or contrary to social norms (drug addiction, child pornography, "extremism," etc.) by bringing in volunteers prepared to track down this content and identify its authors. Through the media coverage they obtain for their chosen causes, particularly threats to children (child pornography, juvenile suicide, drugs), they contribute to highlighting the dangers of the Russian internet, arousing anxiety in public opinion and demands for regulation (Asmolov 2015; Nisbet 2015). They cooperate with state institutions (e.g., law-enforcement agencies and ministries), receive financial support via subsidised projects, and are officially registered as nonprofit organizations with the Ministry of Justice. They also cooperate with the major private Runet operators, particularly social media administrators. Most of them do not seek to publicly denounce offenders themselves or take vigilante action independent of police agencies, but rather aim to work closely or at a distance with the bodies that monitor Runet, namely Roskomnadzor, the Ministry of Internal Affairs (MVD), the Prosecutor General's Office, and the Federal Security Service (FSB). They present themselves therefore mainly as "auxiliaries" to these institutions and do not fundamentally challenge them, although they may sometimes operate on the edge of legality.[5]

However, these groups' conceptions of their actions do differ, which may lead to tensions between them. The surveys on vigilantism available in Russia reveal the offline existence of violent groups "closer to United States vigilantes than to neighborhood watches using social media and internet resources to name and shame" (Favarel-Garrigues 2018). Some researchers have examined their relationship with Soviet-era practices (Gabdulkhakov 2018), with some local situations reminiscent of citizen reporting and denunciation in the USSR (Nérard 2004) or of the maintenance of public order by people's volunteer squads embodied in the *druzhiny* (Matsui 2015). Online, our research reveals vigilante groups of varying origins. Although their cause is a common one, the conceptions they have of their actions differ and their range of actions, ideological convictions, and moral supports are diverse and changing. In 2018 we carried out a survey of two forms of online vigilantism, based on interviews with senior members of two officially registered nonprofits: Molodezhnaia Sluzhba Bezopasnosti (MSB, Youth Security Service) and Liga Bezopasnogo Interneta (LBI, Safe Internet League), which sponsors an emergent "cyber Cossack" movement in Moscow and the regions. These groups adopt either critical or complementary positions vis-à-vis each other. MSB, which we present in the first part of this article, can be referred to as "citizen investigators" and was set up in the early 2000s. Its participants have developed a high degree of technical and legal experience and focus on reporting and investigating in order to prevent crimes or to lead to criminal convictions. To that end they cooperate actively via well-established links with the police and legal system. LBI, which we analyse in the second part, was set up in 2011

[5] These illegal actions may also coincide with behavior by law-enforcement agencies, supporting the criticism made by various researchers of any definition of vigilantism that broadly separates it from the police (Fourchard 2018).

and promotes a conservative vigilantism to ensure "healthy, virtuous browsing." They provide extensive teaching activities for secondary-school pupils and students, with a strong focus on socialization and education. In addition, the cyber Cossacks, who emerged in the wake of LBI, use Cossack imagery to signal their loyalties and their aim to enforce order in terms of both security and morality. The moral causes they support as well as their relationship to the law are opposed to the liberal and libertarian ideologies of Runet.

These initiatives unfold in a context in which responsibility for several social and security issues is delegated to civil society under programs that fund volunteer and citizen projects (Daucé 2013). This delegated management favors the emergence of a market in low-intensity online surveillance as well as competition between volunteers for state support. Discussion of the cyber patrol bill, as observed in hearings of the Russian Civic Chamber in March 2019, revealed the contrasts between two types of loyalism among volunteers, split between an "expert model" and a "political model." In this world of citizen policing, the worried voices of activists for online freedom and human rights criticize new forms of surveillance delegated to the citizens themselves, but remain at the margins of public discourse, as we show in the third part of this article.

This article relies on interviews with senior officials of MSB, LBI, and the Cossack "cyber patrol" movement, conducted in Moscow and Saint Petersburg in 2018. We had no access to ordinary members and were not able to examine their demographics or the recruitment process. The data collected on these organizations is not exactly equivalent: the MSB officials gave us many details of the ways in which they cooperate with law-enforcement agencies and internet administrators, but the LBI officials were much less forthcoming on these matters. In addition, we had no respondents from the law-enforcement agencies involved in cooperation with these volunteers. These restrictions led us to focus on the ideological and organizational models underlying these initiatives rather than on a comparative analysis of their forms of action. The article also relies on public discourse (social media sites and pages, conferences, webinars) collected from the internet and on observation of the hearings concerning cyber patrols in the Civic Chamber on March 4, 2019.[6] Finally, interviews with defenders of online freedoms and rights of internet users provided material for analyzing the construction of an emic criticism of the volunteers for regulating Runet.

HELPING LAW ENFORCEMENT FOR A SAFER ONLINE SPACE: THE ONLINE "CITIZEN INVESTIGATORS" MODEL

The emergence of citizen investigators stems from the first attempts made within civil society in the early and mid-2000s to "cleanse" Runet of its abundant illicit content—drug dealing, pedophilia, child pornography, and, more recently, online suicide games—at a time when the government was adopting a relatively "laissez faire" approach. MSB was set up as a nonprofit organization in Saint Petersburg in 2000, but

[6] The official report of these hearings is available at the Civic Chamber's website (https://www.oprf.ru/press/news/2019/newsitem/48460).

until 2014 it was not officially registered. Its original purpose—fighting against heroin trafficking—was achieved through the innovative use of reporting via paging services and a toll-free phone number, and it then moved on to addressing internet-related topics. As social media took off in the late 2000s, raising new issues online (suicide games) and providing greater opportunities for criminals to contact victims (as in pedophilia), MSB developed a specific expertise. Child protection became central to their concerns and they have been working continuously with law-enforcement agencies, playing the role of independent experts.

These citizen investigators can be associated with other forms of citizen contribution to crime management and may be defined as a type of online "civilian policing" (Huey, Nhan, and Broll 2013; Myles, Millerand, and Benoit-Barné 2016), made up of citizens who do not take direct punitive action but help law enforcement by collecting "information about online crimes and potential crimes" and passing it on to the police, with whom they may also cooperate "during the stages of arrest and prosecution" (Myles et al. 2016:182). In some cases, MSB volunteers set traps by creating false profiles of young social-media users and actively track down suspects. They also claim to play a specific intermediary role between citizens and the police, with technical expertise in emerging offences because of their use of data-collection and surveillance tools on the VKontakte social media service (the Russian analogue of Facebook). They maintain a pragmatic relationship with legality within the lines of judicial practice.

EXPERTS IN EMERGENT CYBER OFFENCES AND INTERMEDIARIES BETWEEN CITIZENS AND POLICE

MSB[7] has been registered as a regional social organization since 2014 and emphasizes its "regular, permanent, and disinterested cooperation with law-enforcement agencies, in order to identify, document, and stop crimes of the following type"[8]: drug trafficking, organized crime and corruption, terrorism and extremism (racial and ethnic hatred, religious radicalism), online economic crime, child pornography, pedophilia, incitement to suicide. The organization receives no government subsidies, nor foreign funding, and its only resources are "members' subscriptions" and "grants from natural and legal persons domiciled in the Russian Federation."[9]

MSB monitors illicit online content (mainly on social media such as VKontakte), collects information, forwards it to the relevant police department (cybercrimes or sex crimes), and provides expertise to prosecutors regarding evidence that is hard to

[7] We interviewed two of MSB founders and leaders. S., aged 43, communications manager at the multimedia center in the Dzerzhinskii House of Culture (cultural center of the main directorate of the Ministry of Internal Affairs, Saint Petersburg), and R., aged 44, self-employed businessman (lubricant import) (interviewed by Zaytseva, Saint Petersburg, July 28, 2018). We also talked to a volunteer who had worked there since 2011: A., aged 26, administrator in the technical support department of a call center (interviewed by Zaytseva, Saint Petersburg, August 4, 2018).

[8] MSB website, "Istoriia organizatsii" (http://www.molbez.ru/novoe-history.html). See also MSB VKontakte page (https://vk.com/molbez).

[9] In particular, from those they have helped with their investigative work.

decipher (such as, for example, logs of closed discussion groups of suicide games on VKontakte passed on by VK admin to the police on CD-ROMs that require advanced interpretation skills). Its members sometimes take part in operational work on the ground (outside monitoring) and arrests (alongside police officers as "freelance police," *vneshtatnyi sotrudnik politsii*[10]) but do not attempt to punish the offenders directly: for them the case ends with the suspect's arrest. Their vision of the offender is expressed in terms taken from psychology and sociology: he is often considered to be a victim himself (of, say, earlier sexual or family violence). Videos are put online to publicize the work of MSB and law enforcement, emphasize its legitimacy, and aim at attracting new volunteers.[11] They also act as deterrents, showing offenders that they are under surveillance and cannot act with impunity; however, unlike the videos uploaded by "pedophile hunters" (Favarel-Garrigues 2018; Kasra 2017), they are not intended to shame the offenders: all faces are blurred out, confrontations do not contain verbal or physical violence, and chatroom names and profiles are redacted.

Just as MSB displays on the walls of its office and on its VK page[12] the decorations and acknowledgments it has received from the various local police authorities,[13] it has adopted a logo containing a sword and shield that is reminiscent of various law enforcement bodies, particularly the FSB and the Cybercrime department ("K" Department) of the Ministry of Internal Affairs. A red heart in the middle of the shield instead of the two-headed eagle symbolizes the MSB's role as a human intermediary between the people and the police, added to its loyal service to preserve the law.

Figure 1. From left to right: emblems of the MSB, FSB, and the MVD's "K" Department[14]

[10] The two founding members interviewed have that status, as defined by the Russian Ministry of Internal Affairs decree of January 10, 2012.

[11] See, for example, "MSB: Operatsiia 'straponshchik 3-go razriada," HelperSaver911, posted July 30, 2017. Video, 22:19. https://youtu.be/lAjnWiLAYqo.

[12] MSB VKontakte page, "Photo albums" (https://vk.com/albums-334471).

[13] Such as State Drug Control Service (Gosnarkokontrol'), Directorate of Federal Drug Control Service (UFSKN), Main Administration of the Ministry of Internal Affairs (GU MVD) in Saint Petersburg and in Moscow, and Prosecutor General's Office.

[14] MSB and FSB emblems come from the organizations' websites, while the "K" Department's is from a nongovernmental online database of Russian heraldic symbols (https://geraldika.ru/symbols/936).

The FSB is seen positively, as an authority able to control the police, "which people often trust more" than the police.[15] Criticism of law enforcement is not spontaneously expressed by these volunteers but is implied by their observations about the lack of practical or judicial procedures, which MSB members help to overcome by acting in new fields and gray areas, or even with the occasional illegality, if necessary.[16] The volunteers do not oppose these agencies but seek to complement them and fill the gaps.

MSB's primary mission, not specific to online activities, is to act as intermediary between law enforcement and citizens. Starting from the observation that "people are often afraid of the police and their methods,"[17] MSB aims to adapt police action and case investigation to individual situations. "It's all a matter of recommendations and personal contacts" in a "hands-on regime" (*v ruchnom rezhime*), they say; "first, the person shares their situation and fears with us, then that information is discussed anonymously with a trusted police employee, and together we consider various scenarios."[18]

MSB's second mission is to take action against emerging offences not yet covered by the law. So the volunteers began to warn the police about online suicide games as early as 2015–2016: "At that time, no one had ever heard of the Blue Whale Challenge,[19] and we were the ones that anxious parents turned to. Local police officers did not even understand what it was. There was no notion of 'assisting' suicide games (*kuratorstvo*), either in social media or in law."[20] MSB volunteers appear to have been the first to speak to the media about it, helping to feed what was later analyzed as "a moral panic of conspiratorial nature" (Yablokov 2017:55).[21] Given the police force's limited staff and resources, the volunteers believe that they are best armed for the time-consuming, painstaking work of monitoring suspicious profiles on social media (often setting up fictitious profiles of teenagers or children, in the case of suicide games and pedophilia): "Some things are more easily done by citizens themselves."[22]

Their technical expertise and methods of cooperation with law-enforcement agencies and social media administrators in investigation and reporting go together

---

[15] Interview with S. and R.

[16] For example, violating some procedural rules for getting information (when it comes to saving lives of potential suicides).

[17] Interview with S. and R.

[18] Interview with S. and R.

[19] Blue Whale (Sinii kit) is the name of one of the most notorious of the early suicide game groups. The "blue whale" thus became a worrying symbol for suicide games. See, for example, Artem Kondrashkin, Anastasiia Krys'ko, and Ekaterina Bianki, "Chto delat', elsi vash rebenok risuet 'sinikh kitov.' Instruktsiia." *Meduza*, February 22, 2017. https://meduza.io/feature/2017/02/22/chto-delat-esli-rebenok-risuet-sinih-kitov-instruktsiya.

[20] Interview with A.

[21] In 2017 Amendments 110.1 and 110.2 to Article 110 of the Penal Code were adopted, making it an offence to incite suicide and coordinate suicide games.

[22] Interview with A.

with a clear refusal to get involved in politics. Whereas "the prevention of extremism among the young" is one of their causes, the MSB volunteers make it clear that they have a more specific understanding of extremism than the Russian legislation: for them it means preparing for or carrying out violent actions (such as bombings) or physical attacks targeting a particular group of people. It does not mean tracking down nonviolent political opponents. This neutrality and their formal independence from state authorities have enabled them to transcend the political rifts between Russia and Ukraine since 2014 and act as intermediaries between Russian and Ukrainian cybercrime departments in tracking down suicide game coordinators on VKontakte (this social media platform is now officially banned in Ukraine but is still used by many Ukrainians via anonymizing proxies).

PRAGMATIC RELATIONS WITH LEGALITY: BROUGHT INTO LINE BY JUDICIAL EXPERIENCE?

In their investigative work, the MSB volunteers maintain a relationship with legality that treads a narrow path between the legal and the illegal. Rather than displaying the virulence of "lawless avengers" (Favarel-Garrigues and Gayer 2016), their behavior comes closer to the actions of the law enforcement agencies themselves. On the one hand, various discreet, accepted forms of illegality emerge, given the lack of regulation in a new field or via a particular balancing of good and evil (committing a minor infringement, such as skipping a judicial procedure, in order to avoid a much greater offence or crime). On the other hand, while a respectful attitude towards procedures is not an original part of their ethics, they learn it empirically, prosecution after prosecution. Ultimately, the respect for the law these volunteers claim is not merely lip service but gains its strength from the practical work they do alongside law-enforcement officers.

A whole arsenal of digital tools is used in a gray area of legislation: they pose a threat to users' right to the protection of personal data (covered by Russian Federal Law No. 152-FZ Concerning Personal Data), since no implementing legislation has been passed to punish the collection, collation, and cross-referencing of personal information that these tools enable. Over time MSB volunteers have become real experts in these new surveillance and digital tracking technologies. In the name of the causes they pursue they agree to use these technical possibilities without examining them critically as a danger to personal freedoms.

What then is the legal status of these digital surveillance tools? According to S., the usage of these databases and software does not constitute an offence, at least in Russia. Law-enforcement agencies are the only ones authorized to use them for what is called "information for investigation purposes." Thanks to its trusted relations with the police, MSB may still collect this information and forward it to law enforcement so that they can "carry out further verification on the ground," without going through the official channels (e.g., filing complaints through local police precincts' websites), which are "too troublesome for the police themselves" (S.). This activity in a gray area of legislation has not prompted any consideration of the illegal aspects of such investigations, as the online investigators wait for judicial practice and im-

plementing legislation to address the awkward question of personal information aggregators. Any caution and concern there has been about information collection methods have only emerged empirically in the wake of "precedents" that have altered legal practice.

For example, when the online suicide games affair came to light in 2016, MSB and others acting against the Blue Whale Challenge often used entrapment tactics with false teenagers' profiles: they would send to an identified "mentor" messages such as: "give me a task to do" and "when do we start playing?" Because the police cybercrime department now had quantified objectives to meet in this area, it would open cases on the basis of information obtained via these false profiles. The lawyer for one of the alleged mentors filed a counterclaim as a petitioner against the complainant, accusing the adults behind the false profiles of incitement to crime. Later the prosecution withrew this evidence and the case was closed. This set a legal precedent and other counterclaims of this type were filed by lawyers. Since then, precautionary measures for volunteers working online under false profiles have been laid down by the Investigative Committee and the "K" Department staff and are included in guides for volunteers written by MSB coordinators. This shift in legal procedures is not questioned but pragmatically integrated. For these actors, this is a normal evolution in the justice system that one must adapt to.

SURVEILLANCE WORK ON VKONTAKTE (VK)

Most of the work done by MSB volunteers and cyber patrols consists in monitoring content on social media, VKontakte in particular. How they operate is closely related to the history of this network, which at first asserted its autonomy under its founder Pavel Durov but since his forced departure has been more inclined to cooperate with the authorities. MSB volunteers have various applications at their disposal, created by anonymous programmers external to VK, that can extract hidden information from VK profiles and crosscheck open information between large numbers of profiles.[23] Identifying illegal content on VK raises the question of the responsibility of legal authorities and the social media platform for removing it.

MSB volunteers mention various cases when they strayed from procedures and attempted to shortcut long legal processes when discussing their actions against the drug Spice.[24] R. proudly tells the story of his struggle with the VK administrators

[23] For example, Yasiv.com/vk can be used to display as networks the connections between a vast number of VKontakte profiles; 220vk.com displays a VK profile's hidden friends and users who have concealed that profile among their friends, the date the profile was opened, friends and groups common to two VK users, home towns of a VK profile's friends, etc. Various integrated search systems are also mentioned, such as I-sphere.ru that analyzes connections between social media accounts, open bank data, documents, first and last names, telephone numbers, ad sites, etc. For more, see MLB's "Pamiatka: Kak sokhraniat' informatsiiu pri sbore materialov" (http://molbez.ru/rassledinet.html).

[24] A form of synthetic cannabinoid also called a "zombie" drug because of its possible violent effects.

(then headed by Pavel Durov) to get them to block pages linked to the sale of Spice and also vendors' profiles, even before Spice was officially listed as a controlled substance. R. then threatened to call in the Saint Petersburg prosecutor himself, who might well find some irregularities in VK operations. VK is entirely responsible for blocking pages, because the user licence stipulates that all user accounts are the property of the company. It is therefore VK representatives who decide whether or not to comply with a request to block, if this is not supported by a court decision. "They have dozens of moderators, some of whom, when hesitating between 'free speech' and 'perhaps we should block,' will opt for 'free speech.' And when we tell them, 'look, this is against such and such law,' they reply, 'go to the police or Roskomnadzor.'"[25]

When VK's management changed in April 2014, the network became much more cooperative. In the suicide games affair, "we are 95 percent sure that the VK administration adopts our point of view and will block illegal content, especially in emergencies, where the mentor sends his final task to the player. In those cases we ask VK to block both of them so that they cannot communicate any more."[26] Although this direct blocking mechanism, with no court decision, has become routine, it is still fragile because it depends on individual decisions by VK employees. One case that amazes R. and S. is that the current head of VKontakte's security service, according to them a former FSB man, is not making it any easier to block: "This former FSB officer knows the law and systematically asks for the court decision, even in emergencies. He's a legalist and won't accept informal agreements [*neformal'nye dogovorennosti*] made in the past." So, following the law too closely is seen as an excessive legalism: insistence on time-consuming procedures hampers action when dealing with emergencies that must be addressed in real time.

As for confidential personal information and discussions in VK chatrooms, the police (and thus MSB) may only access them with a court decision as part of a criminal investigation: "This is a very long, formal process: you get a court order, the MVD sends a letter to VK administration to obtain a record of the conversation. VK sends them this conversation on a CD, by mail." When MSB volunteers contribute their expertise to analyzing these masses of "service information" (*sluzhebnaia informatsia*), they sign a "nondisclosure agreement" (*podpiska o nerazglashenii)*. For localizing IP addresses, the legislation enables the police to obtain them from the ISP (internet service provider) via an "operational request" (*po operativnomu zaprosu)*. Because of their trusted relationship with the "K" Department, MSB volunteers can in this way easily localize the physical addresses of pedophiles and suicide game coordinators so as to track them down (together with the police or sometimes even ahead of them). Their long experience of cooperation with the authorities demonstrates their gradual professionalization both in elaborating cooperation procedures with the police and in using technical internet tools.

---

[25] Interview with S.

[26] Interview with S.

EDUCATING CITIZENS TO RESPECT MORALITY ONLINE: THE CYBER PATROL MODEL

Whereas MSB puts forward its expertise in online security based on the skills of its members, other civilian cybersecurity operators have developed a different model based on enrolling ordinary citizens in low-intensity surveillance of Runet. In the early 2010s, as internet usage became commonplace and social media developed, the appearance of the Safe Internet League (LBI) illustrated the involvement of private and public players to moralize Runet. At the time there was little regulation of the Russian internet, which had freely developed in the 2000s, so LBI lobbied politicians hard to adopt laws to moralize it (like the amendments to the 2010 Federal Law No. 436-FZ On Protecting Children from Information Harmful to Their Health and Development and particulary prohibiting the "propaganda of homosexuality among minors"[27]) in partnership with the conservative fringe of the Duma in the person of the well-known deputy Elena Mizulina. The League set up cyber patrols (*kiberdruzhiny*) claiming up to 20,000 members across the country, recruited via partnerships with administrations, educational establishments, and volunteer associations in many Russian regions. It helped form cyber Cossack groups in the mid-2010s. The cyber patrols operate intensely in three areas: training young people in online security, reporting illegal content, and producing "positive content." They do what they can to attract the media's attention. This "flagging" type of digital vigilantism (Loveluck 2019) is strongly focused on the political advancement of conservative values. These vigilante patriots belong to two traditions, Russian and international. On the one hand, the LBI executive director invokes the Middle Ages, when the *druzhina* was the "prince's personal retinue," particularly that of Grand Prince Vladimir (a barely concealed allusion to the current Russian president, Vladimir Putin). From the prerevolutionary period, the reference is to the Cossack patrols, loyal to the monarch and helping guard the borders of the Russian Empire. In the late Soviet period *druzhinniki* helped the police fight against minor delinquency and deviant behavior. Fully integrated into the law-enforcement system, they provide a legitimate model of symbiosis between the police and its volunteer helpers (Matsui 2015). On the other hand, LBI's website refers to the British and American practice of "neighborhood watch,"[28] whereby local residents help stop crimes such as burglary and vandalism by setting up hotlines to the local police and sometimes organizing patrols.

---

[27] Federal Law No. 135-FZ of June 29, 2013, Amendments to Article 5 of the Federal Law on The Protection of Children against Information Harmful to Their Health and Development and to Certain Legislative Acts of the Russian Federation Protecting Children from Information that Promotes the Rejection of Traditional Family Values. Chapter 6 of the Federal Law No. 436-FZ was supplemented by article 6.21. "Promotion of nontraditional sexual relations among minors."

[28] See the English-language page of the LBI website (http://www.ligainternet.ru/en/liga/activity-cyber.php).

PROMOTING A MORAL ORDER ONLINE: THE SAFE INTERNET LEAGUE (LBI)

From its beginnings in 2011, the Safe Internet League (LBI) has aimed to bring together various separate initiatives and Runet security patrollers (*kiberdruzhinniki*). It was founded by a number of public and private stakeholders at the initiative of the businessman Konstantin Malofeev, founder of the Marshall Capital investment fund, at that time a 10-percent shareholder in Rostelekom (Russia's largest telecommunications operator), together with four major internet service providers. Malofeev is openly linked to the Russian Orthodox Church, which for several years now has pursued a campaign to moralize Russian society and promote "family values" and "spiritual virtues" as a national standard. LBI's aim is to "eliminate dangerous content" by getting the professional community, online market traders, and ordinary users to organize. LBI is close to official circles and is reported to have contributed in 2011 to preparing the law blacklisting websites that threaten "children's health" and blocking websites banned by Roskomnadzor.[29] It has allegedly supported the adoption of a large number of laws restricting online freedoms since 2011. Its director, Denis Davydov, is said to have had political ambitions that ultimately came to nothing.

The *kiberdruzhinniki* movement initiated by LBI appears to have given rise to local organizations, each of which defines its field of action according to the type of offence that is targeted. These offences are similar to those monitored by MSB, except for organized crime and corruption. According to the LBI founders, its initial objectives were to fight against pedophilia, homosexuality (soon abandoned), extremism, and prostitution. However, the spectrum of "negative content" is actually broader: one member of the Civic Chamber even proposed to include videos of animal cruelty in the monitored content.[30] In May 2011 LBI and VKontakte signed a memorandum of cooperation allowing LBI volunteers to look for illegal content on that network and forward it to law-enforcement agencies.

Initially, like the MSB volunteers, the cyber patrols set up sting operations by creating false child profiles to attract paedophiles. In 2011 Davydov claimed that "the pedophiles tremble with fear" at the name of LBI. At that time, he asserted that "we do nothing illegal; the law does not stop anyone talking to pedophiles," who are supposed to be rehabilitated by these preventive interviews. This activity appears to have been stopped later, as a result of changes in judicial practice.[31] LBI volunteers report illegal content to the authorities. According to their figures, 1,500 criminal

---

[29] Federal Law No. 139-FZ of July 28, 2012, Amendment to the Law On the Protection of Children from Information Harmful to Their Health and Development and to other legislative acts of the Russian Federation (namely to Federal Law No. 149-FZ of July 27, 2006, On Information, Information Technologies, and Information Protection).

[30] "V novgorodskom internete budut borot'sia s shok-kontentom," Novgorod.ru, September 22, 2017. https://news.novgorod.ru/news/v-novgorodskom-internete-budut-borotsya-s-shok-kontentom-159491.html. In October 2019 the Russian government supported the bill on blocking sites displaying animal abuse, giving a legal form to previous isolated initiatives.

[31] Adelaida Sigida, "Druzhinniki berut pedofilov golymi rukami," Utro.ru, August 10, 2011. https://utro.ru/articles/2011/08/10/991465.shtml.

prosecutions were launched for child pornography, 1,000 websites selling drugs were blocked, and 10 cases of serial pedophilia were cleared up in the mid-2010s. After focusing on tracking down pedophiles, by 2018 they were concerned, like MSB, with "death groups" encouraging suicide and with "extremism."[32] The causes defended by the cyber patrols shift with the news at a given moment and with their own practices: according to activists in the Belgorod Oblast in 2017, their action no longer consists in "informing on people" but in "monitoring" them (*ne donosiat, a monitoriat)*.[33] This monitoring can also involve public denouncements, for example in the widely publicized operations in favor of a "white internet" carried out every year since 2013. These are raids, held with local organizations, on public spaces offering free wifi (mostly cafés) to check whether the underage have access to prohibited websites. If a participant in the "white internet action" clicks on a link given by LBI and is redirected to the blatantly named website Pornonarcosuicid.ru, it means that the wifi access is not secure. The owner of the premises is alerted, and if they do not quickly sort it out, they are reported to Roskomnadzor. During some actions, stickers saying "This place is dangerous for children" are handed out to the owners.[34] These visible stigmatizing marks are a form of shaming.[35]

LBI's action to clean up Runet is part of a harking back to the prerevolutionary heritage of Imperial Russia and a criticism of the Soviet past. Its director Davydov indicates his traditionalist political position: "The situation in Europe reminds me of Russia in 1917. A leftist international is preparing for global revolution. We have already had that in our country; I can see the horror of what is happening in the European Union and its bureaucracy. The EU is like the USSR in its time." Russian civilization is contrasted with Western, particularly European, decadence, which has given up the virtues of Christianity. Speaking of European leaders, the LBI official continues: "They act against traditional values, against the family, even in a Catholic, well, Christian, country like France. What is happening is horrible." But LBI is also critical of the political situation in Russia. As Davydov explains, "The problem is that we can't do everything. Our government has a liberal approach and doesn't want to annoy the major internet players (FB, Google, VK, etc.)."[36] He also denounces the destructive action of "anarchist, leftist, and antifascist groups."[37] This LBI official's critical conservatism appears to be gradually losing influence. In 2017 Davydov handed over his position as LBI president to Ekaterina Mizulina, the daughter of the

---

[32] "Kiberdruzhiny uzhe 'stuchat' po vsei strane," *Novye izvestiia*, December 7, 2017. https://newizv.ru/news/tech/07-12-2017/kiberdruzhiny-uzhe-stuchat-po-vsey-strane.

[33] Liga Bezopasnogo Interneta, Facebook post, June 6, 2017. https://www.facebook.com/ligainternet/posts/1357326550969666?__tn__=K-R.

[34] This happened in Ulyanovsk in 2015 ("Aktsiia belyi internet," IT v Ul'ianovske, March 26, 2015. http://it.ul-online.ru/news/?news_id=6669).

[35] For another example of such shaming in the Russian context, see article by Rashid Gabdulkhakov in this special issue of *Laboratorium* about shaming of bad drivers.

[36] Interview by Ostromooukhova and Daucé, Moscow, October 24, 2018.

[37] Anna Semenets, "Sotsseti stanoviatsia opasnymi," Rosbalt, November 5, 2018. http://www.rosbalt.ru/moscow/2018/11/05/1744165.html.

Duma deputy. Since 2018 LBI's activities appear to be dormant. Its website is not being updated.[38] However, some initiatives using the League's name are still emerging here and there, in particular within higher education institutions, evidence of an increasing political interest in cyber vigilantism from local authorities and educational supervisors. Groups of cyber patrollers, originally supported by LBI, are breaking free from its supervision.

ASSERTING ALLEGIANCE TO THE NATION ON THE INTERNET: THE COSSACK CYBER PATROLS

The Cossack cyber patrols were set up by the LBI and are a form of *kiberdruzhiny* characterized by their connection to the Cossack military regional organization system,[39] under the motto "Defend the digital borders." Their creation was sealed by an agreement on November 11, 2016, between LBI and K. G. Razumovsky Moscow State University of Technology and Management (MGUTU), named in 2014 as "the first Cossack university." This public institution recruits primarily but not exclusively students who identify as Cossacks and combines a technical education for agri-food careers with a "Cossack ethno-cultural component."[40] The latter is defined as learning the bases of Cossackness that are "patriotism, service to the state, historical memory, and the Russian Orthodox faith."[41] MGUTU has 18 campuses in the Russian regions, and, since a second agreement in January 2017,[42] Cossack cyber patrols have been set up in some 15 of them. The movement is tending to expand beyond higher education: an MGUTU webinar, broadcast in autumn 2018 to train new leaders for Cossack *kiberdruzhiny*, included alongside its students other young Cossacks wanting to organize their own patrols directly within the regional *druzhiny*. Russian social media groups

---

[38] According to some of our informants, the rise and apparent fall of LBI are due to the political fortunes of Igor' Shchegolev. As minister of communications in 2011, he encouraged telecom operators to support LBI financially. They stopped doing that six years later, when Shchegolev was given "honorary retirement" as presidential plenipotentiary to the Central Federal District.

[39] From the sixteenth century to the 1917 Revolution, the Cossacks were a community of border guards with their own culture and a special status enabling them to carry out various forms of service as state auxiliary forces. In present-day Russia, some Cossacks' descendants appeal to this heritage and are attempting to recreate a special culture and way of life. They are organized into regional "troops" (*obshchestva*) each with a "popular militia," *druzhiny*, called upon to support law-enforcement agencies. The *kiberdruzhiny* are actually a branch of these militias defined by their field of action, the internet.

[40] "Kazachii komponent v vysshem obrazovanii," K. G. Razumovsky Moscow State University of Technology and Management (MGUTU). Accessed January 22, 2019. http://www.mgutm.ru/kazachestvo/formation.php.

[41] "Kazachii komponent v vysshem obrazovanii," K. G. Razumovsky Moscow State University of Technology and Management (MGUTU). Accessed January 22, 2019. http://www.mgutm.ru/kazachestvo/formation.php.

[42] "Kazach'i kiberdruzhiny shagaiut v regiony," K. G. Razumovsky Moscow State University of Technology and Management (MGUTU), January 27, 2017. http://www.mgutm.ru/content/news/13559/.

(on VKontakte[43] and the Russian Orthodox network Elisty[44]) are evidence of groups claiming the name Cossack *kiberdruzhiny* but with a purely regional affiliation.

The Moscow cyber patrol is headed by a MGUTU marketing lecturer and comprises students who volunteer for this activity among the possible options of service to the state (*sluzhenie*). They attend weekly evening classes to learn a patrol member's two activities: holding workshops on cybersecurity in primary and secondary schools and monitoring information on drug sales. The first part, educational, involves cooperation with both "Cossack"[45] institutions and ordinary schools. The cyber patrol members teach pupils in the higher classes to give lessons to the younger ones, starting a chain of knowledge transmission. In these workshops, the child and the teenager are presented as vulnerable objects easily manipulated. The second part focuses on monitoring and consists in identifying messages concerning the sale of narcotics. Using a list of synonyms for the various drugs,[46] patrol members identify the websites and pages on social media that offer drugs for sale and report them to LBI or directly to Roskomnadzor, which blocks them. The monitoring is regularly repeated so that sales pages can be blocked as they (re)appear. This action is described as having modest aims: not to help law enforcement dismantle dealer networks but to make buyer-vendor communication more difficult. It is not presented as heroic, but rather as discreet but necessary grunt work.

In our interview with the Moscow cyber patrol leader,[47] he carefully avoided any ideological or identity-based component connected with the Cossacks. Dressed in civilian clothes (although in his recorded webinars he wears a Cossack uniform), he presented himself primarily as our "colleague," motivated by scholarly and educational interests, and said that his students, "some of whom identify as Cossacks," were basically no different from any other "active" students. The word "patriotism" was not used once, nor "moral" or "family values." When we asked him about the relationship between the cyber patrol and the Russian Orthodox Church, he distinguished between private faith and patrol work: "The Cossacks have always been close to the Church; some of our students are Russian Orthodox. But the patrol has no direct relationship with the Church.... The Church is interested in our activity, our classes. There are priests who would like to learn how to identify negative content. Our classes interest them; there are young priests who follow our seminars. But that does not mean that we cooperate directly." Attachment to Cossack values also

---

[43] For example, the Egorlykskii District Cossack *kiberdruzhina* group (https://vk.com/club154410182), which has 46 members.

[44] "Pravoslavnyi antitrolling," Pravoslavnaia sotsial'naia set' Elitsy, March 25, 2017. https://elitsy.ru/communities/112481/1155136/.

[45] To educate children and teenagers in Cossack traditions, there are "cadet" classes in secondary schools, including in Moscow. For example, in the Don region, densely populated with Cossacks, there are 147 Cossack educational establishments from primary to higher education.

[46] According to the cyber patrol leader, lists of these key words are freely available on the police website. Interview with V. (MGUTU cyber Kossak patrol official) by Ostromooukhova and Daucé, Moscow, October 26, 2018.

[47] Interview with V.

emerged in his hierarchical conception of subordination. The patrol leader emphasised his triple hierarchy—LBI, the university management, and the Cossack authorities—referring to them when he refused to answer any question that went beyond the rehearsed discourse used in his classes and seminars, and he absolutely refused the slightest criticism of the "authorities."[48] These values also surfaced, albeit in a nuanced form, in his discourse about the opposition between Russia and the United States (and "Western" countries in general). One recurring topic in the cybersecurity classes is the "big data" collected and monetized by "Anglo-Saxon" companies, against which Russian children and teenagers are warned. When the patrol leader is talking to the students in the webinar referred to above, he is slightly more explicit. He talks about a third activity of the Cossack *kiberdruzhiny* barely mentioned in the interview: the production of "positive content," the "creation of sites and communities with a patriotic inspiration" called upon to defend "Cossack values."[49] Cossack patrol members are asked to seek new supporters and to wield a discourse of patriotic propaganda.

BETWEEN EXPERTISE AND POLITICS: DISCUSSING THE VOLUNTEER REGULATION OF RUNET

The cases of MSB, LBI, and the cyber Cossacks demonstrate the diversity of surveillance groups gradually deploying in Russian cyberspace. They are a good illustration of the "protean" nature of the vigilante movements involved in a growing diversification of policing (Jobard and Maillard 2015:225) supported by new digital tools. However, these three examples do not give an exhaustive view of the entire range of citizen cyber surveillance, and other groups and movements could have been mentioned. These many initiatives remind us that the very notion of vigilantism is a malleable one and covers a variety of actions (Fourchard 2018; Moncada 2017); digital vigilantism blurs distinctions even more as surveillance becomes an everyday practice and as it becomes easier to slip from reporting activities seen as illegal, unfair, or immoral to punishing them (Loveluck 2016).

In Russia, as the digital world is increasingly restricted by attempts to achieve "sovereignty" over Runet, these initiatives raise questions about the competing vigilante models and political choices they imply. The debate concerning Shkhagoshev and Bykov's cyber patrol bill in 2018 and 2019 was an opportunity to observe current discussion of the delegation of online surveillance to civil society. It has given rise to a controversy that can be seen as a sociological "test" (Lemieux 2007), bringing to light two conceptions of vigilantism in tension. The controversy led to the identi-

[48] For example, when asked if he thought the police did not take enough interest in social media, he replied, "No, it's not right to say that, they are concerned not with media but with people. Their specific task is a different one, that's all. These media are Roskomnadzor's business." He would go so far as to criticize individual "dysfunctions" but only in a constructive way, in order to correct them.

[49] MGUTU webinar, October 16, 2018. These webinars were made available to registered members.

fication of two models of digital surveillance: the first can be understood as "political" and is supported by amateur citizens, while the second can be referred to as "professional" and is promoted by experts of the Russian internet.

These two models are based on two modes of justification, which show their anchoring in two conceptions of the common good, one based on domestic hierarchies, the other on technical efficiency, to use Luc Boltanski and Laurent Thévenot's ([1991] 2006) models. During the hearings held by the Civic Chamber in March 2019, the two groups were facing each other. On one side, the "politically involved" (Duma members, *kiberdruzhiny* association officials) supported the bill. On the other, the "experts" (representatives of internet companies and security specialists) were opposed to it. As one speaker said, "We can see the political nature of this initiative: it is linked not to combating illegal content but to political battles."[50] Finally, a third form of criticism and justification can also be identified: supporters of a free and democratic Runet who worry about the development of mass surveillance. They are absent from the official debates but express themselves on social networks and in independent media.

CYBER PATROLS AS A POLITICAL PROJECT

The "political" model of digital surveillance promotes the recruitment of Russian internet users for day-to-day low-intensity surveillance of their immediate digital environment. This "microparticipation" is based on simple, repetitive tasks that give the ordinary internet user no mission of analysis or achievement of surveillance objectives, but simply "a proper civic position." According to the cyber patrol bill mentioned above, digital patrol groups will be made up of citizens aged over 18 and will be registered as "social organizations." Deputy Anatolii Vybornyi says: "When we see people wearing the *narodnyi druzhinnik* armband in parks or at events, that is quite normal for us. This disciplines [*distsipliniruet*] the citizens and also the law-enforcement agencies they patrol with. And today, because we are spending more and more time on the internet, there is a demand for *narodnye druzhinniki* in that area."[51] The deputy calls for the establishment of an identification code for online patrol members. The sponsors of the bill want to see the many administrations in charge of surveilling Runet (Roskomnadzor, Rospotrebnadzor, Rosalkogolregulirovanie, Federal Tax Service, MVD, Prosecutor General's Office) respond more effectively to citizens' alerts.[52]

The bill would regularize the development of amateur citizen patrols on the Runet, which has been promoted in recent years by the LBI. Until 2018 there were no

---

[50] Authors' observations of the hearings, March 4, 2019.

[51] Evgeniia Filippova, "V 2019 godu dlia kiberdruzhinnikov napishut zakon," *Parlamentskaia gazeta*, December 29, 2018. https://www.pnp.ru/social/v-2019-godu-dlya-kiberdruzhinnikov-napishut-zakon.html.

[52] As they are known informally in the Prosecutor General's Office. See Denis Dmitriev and Aleksandr Borzenko, "V Rossii khotiat uzakonit' 'kiberdruzhinnikov.' Oni budut pomogat' sazhat' za memy?" *Meduza*, November 19, 2018. https://meduza.io/cards/v-rossii-hotyat-uzakonit-kiberdruzhinnikov-oni-budut-pomogat-sazhat-za-memy.

official regulations concerning the use of *kiberdruzhinniki* as law enforcement auxiliaries. Each region decided whether or not to make use of their services. Throughout the 2010s these online surveillance movements spread in the form of partnerships between citizen movements and local and federal authorities. Registered as voluntary organizations, the cyber vigilante groups signed agreements with city and regional administrations. LBI is a case in point. It gradually extended its activities over the entire country. It signed a cooperation agreement with the Kostroma Oblast administration in 2012 to combat "child pornography, fascism, drug propaganda, violence, and extremism on the internet." After that it made a number of agreements with regional authorities (particularly youth policy departments, as in Khanty-Mansi Autonomous Okrug in April 2017[53]) and local universities (MGUTU in Moscow, universities of Tver', Volgograd, Barnaul, Nizhnevartovsk,[54] Surgut, and in the Crimea). At the peak of its activity it claimed to be present in 38 of the 85 federal subjects of Russia. LBI sends trainers to universities (like Valerii Ponomarev, the LBI executive director's Cossack adviser[55]) and secondary schools. Cyber vigilante activities are extended by local voluntary associations and movements and higher education institutions[56] that set up their own brigades. By 2018 this surveillance activity had spread so far throughout the country that Radio Svoboda's website published an interactive map of regional seats of cyber patrols, entitled "Army of Informers."[57] Whether set up by LBI, the cyber Cossacks, or MediaGvardiia (a pro-Kremlin youth organization), these online citizen vigilantes receive state financial support. Given the extent of the phenomenon, the nonprofit Roskomsvoboda (a Russian nongovernmental organization that supports open self-regulatory networks and protection of digital rights of internet users) keeps a record of all these initiatives and the funding they receive.[58]

Grigorii Pashchenko, a former LBI member, is a representative of this "political" conception of digital surveillance. He had been in charge of the Tver' section of the LBI since 2015 and then became the head of all LBI internet patrol members. He has since broken with LBI and currently applies himself to avoid any association with it. In an interview, he stressed the respectable experience, some seven years, of his

---

[53] "V 11 organizatsiiakh KhMAO zapustili kiberdruzhiny dlia bor'by s 'gruppami smerti,'" TASS, March 29, 2017. https://tass.ru/v-strane/4137124.

[54] "Kiberdruzhiny za 'chistyi' internet," Official website of the municipal self-government of the city of Nizhnevartovsk, September 19, 2018. https://www.n-vartovsk.ru/news/citywide_news/bgorod/287605.html.

[55] "Nauchit' detei zashchite ot … Internet-ugroz," Internet poral of the Education Department of the administration of Odintsovo city district. Accessed November 21, 2019. http://odinedu.ru/upravlenie-obrazovaniya/novosti-upravleniya-obrazovaniya/74.

[56] Particularly law and "information security" faculties, as at Volgograd State University.

[57] "Armiia donoschikov: V Rossii rastet chislo kiberdruzhin," Radio Svoboda. Accessed February 19, 2019. https://www.svoboda.org/a/armiya-donoschikov-v-rossii-rastet-chislo-kiberdruzhin/29596085.html.

[58] "Iacheiki po kiberdonosam aktivno organizuiutsia v regionakh," Roskomsvoboda, November 20, 2018. https://roskomsvoboda.org/43120/.

kiberdruzhina. As for the organization's numbers, Pashchenko is deliberately vague on the topic, although he admits that one quoted figure of 20,000 is exaggerated. Not least, he rejects criticism of the cyber patrols as being incompetent first-year students or even school pupils looking for reposts on the internet and checking all sorts of VKontakte profiles for extremism. He claims their work is serious, targeted, and technically advanced. He says that an overwhelming majority (over 90 percent) of his *kiberdruzhina* are "technicians aged over 30": they are not "young guys sitting in front of their computers monitoring all sorts of stuff on VKontakte" but "genuine specialists" looking for online extremism, terrorism, drug sales, and so on.[59] Here, Pashchenko answers the critics of the "citizen investigators" model. At the same time, almost in passing, Pashchenko speaks quite naturally about the "information war waged against Russia by our Western partners" and insists at that point that in his *kiberdruzhina* they are "patriots" and "don't like people who badmouth Russia," thus referring to the "political model" of digital surveillance. One might well suppose that with the redistribution of power that would follow the passing of the cyber patrol bill, as head of *kiberdruzhina* he is attempting to play the field, relying on all the different models, targeting various types, sensitivities, and profiles of institutional sponsors and possible donors. During the Civil Chamber hearings Pashchenko was one of the most enthusiastic supporters of the new bill and main representative of the "political" model.

"EXPERT" OBJECTIONS AND CRITICISMS

The normalization of surveillance involving the enrolment of young internet users arouses criticism from expert "citizen investigators" who decry the amateurism and political use of these new cybersecurity agents. Those who think cyber vigilantism should be restricted to specific issues are sceptical about the patriotic mobilization of young people and attempts at teaching good morals.

One such is a founder of the Friendly Runet Foundation (Fond Druzhestvennyi Runet, established in 2008),[60] who helped set up LBI in 2011. Without directly criticizing the latter, he says that educational work, the "popularization of good behavior," does not interest him.[61] What mattered to him and his foundation was to focus on identifying and blocking online resources that spread child pornography. This was "the only topic on which there is an international consensus" for which the INHOPE hotline (International Association of Internet Hotlines)[62] was set up with Interpol support. At the local level, the Friendly Runet Foundation developed close links with the police cybercrime department and the VKontakte administration. Relationships of "friendly cooperation" with hosting services and internet providers in Russia were cultivated so

[59] Pavel Merzlikin, "Gosduma predlagaet sozdavat' kiberdruzhiny dlia poiska ekstremizma v internete. Glava kiberdruzhiny, kotoraia rabotaet uzhe 7 let, rasskazyvaet, kak eto vygliadit seichas i chto izmenit zakon," *Bumaga*, November 12, 2018. https://paperpaper.ru/gosduma-predlagaet-sozdavat-kiberd/.

[60] http://www.friendlyrunet.ru/.

[61] Interview by Ostromooukhova and Daucé, Moscow, October 2018.

[62] http://www.inhope.org.

as to be able to ask these "colleagues" to block content when they received complaints from other countries (e.g., France, the United States, the United Kingdom) via INHOPE. Although he took part in setting up LBI, he no longer works with them, believing that their mission (to remove child pornography from Runet) is completed. As for the cyber patrols that have emerged around LBI, he is "distrustful," because even if he supposes that their work is mainly educational he considers them analogous to other movements of Russian volunteer patrols (*druzhinniki*, with no "cyber"). Some of these "are armed with knives and axes" and "go hunting for pedophiles." The direct punishment dealt out by these amateur avengers is a provocation that is likely to lead to uncontrollable excesses. So, by extension, cyber patrols remind him of the street vigilantism of "pedophile hunters" (Favarel-Garrigues 2018, 2019; Kasra 2017) that are the bane of surveillance experts loyal to the institutions and police.

Another criticism, this time from the founder of MSB, is that the cyber patrols could be set up by people seeking immediate visibility and "a new slice of the budget" (*raspil biudzheta*). With no relationship of confidence with police structures, not realizing that "serious work on cybercrime requires experience, skills, knowledge of psychology, and time," they "do not take the time to get into the details of the situation" or to know the law. For example, "some did not even realize that it was prohibited to recruit underage volunteers to track down pedophiles and child pornography." Police officers close to MSB told them of their concerns about a bill seeking to make this sort of voluntary work official and force the police to work with them.[63] These criticisms of the cyber patrols from more senior actors in online surveillance appear, by reaction, to have shaped the discourse of those claiming leadership in this new field of virtuous Runet activism, who expect a rosy future if the cyber patrol bill is passed.

"LIBERAL" OBJECTIONS AND CRITICISMS

At the margins of the public space, online freedom activists are concerned about the ongoing discussions but cannot take part in them because they do not participate in official decision-making bodies. The 2018 cyber patrols bill aroused many criticisms from the defenders of online freedoms. These nonprofit activists, bloggers, and journalists were concerned about the civic and moral aspects of this online citizen enrolment. Their criticisms are based on the ideas of liberal, left- and right-libertarian movements. The nonprofit Roskomsvoboda, with members from the Pirate Party of Russia, is a central player in this controversy. Its director Artem Kozliuk says in his comments on the bill that many laws passed to regulate the Russian internet work poorly, however: "That doesn't mean that we needn't bother about them. Sooner or later, they're going to work one way or another. As time passes, this machinery will get more complex and we'll have the antiutopia of real totalitarianism. For the time being, we're at the shambolic stage, and on top of that there are people making money off digital blood [*na tsifrovoi krovi*]: some are building storage facilities [*khranilishcha*], others are developing SORM boxes (in association with the FSB)."[64]

---

[63] Interview with S.

[64] Interview with Kozliuk by Ostromooukhova, Moscow, October 24, 2018.

The defenders of a free internet are attempting to identify the many aspects of surveillance in this complex, distributed world of online security and are facing defenders of a moral order, greed for money, and commitments to security. Eva Merkacheva, chair of the Moscow Public Observation Commission (ONK), says that: "If these *druzhiny* are formed, I'll bet you that some of them will be former members of law-enforcement agencies or current agents."[65] The blogger El Murid considers that "it's about institutionalizing online snitching [*stukachestvo*]. That's classic for Putin's Russia: if the government gives these *druzhiny* financial support, the projects will be diverted and in a while there'll be 'fake structures' [*feikovye struktury*] like Nashi and MediaGvardiia, every sort of anti-Maidan groups that will be joined by the *kiberdruzhinniki*. In other words, they will exist formally but their utility will be nil."[66] El Murid says that the original model is LBI: "This sort of informant structure has been around since 2011, with the Safe Internet League." To understand the Russian situation comparisons are made with cases from abroad. For Mikhail Klimarev, executive director of the Internet Protection Society (Obshchestvo Zashchity Interneta) that advocates limiting internet regulation, the aim is to copy the principle of the Chinese *wu mao dan* "50-Cent Party,"[67] although these models of manipulation are no longer active because they are expensive and ineffective. These criticisms are based on knowledge of national and international developments on the internet, poorly covered in Russian public discourse. Activists for a free Runet are kept out of decision-making bodies in this field and are reduced to monitoring the "surveillers."

CONCLUSION

After a short period of relative government weakness in the 1990s, when policing functions were partly taken on by various private groups sometimes described as "violent entrepreneurs" (Volkov 2002), a new situation in the 2000s saw the state reclaim its monopoly on legitimate violence and the active management of various forms of "public-private" cooperation in many fields, of which the initiatives discussed here are only one aspect. Since the launch of MSB activities in the early 2000s, the organization's volunteers have come closer to local police forces and the Saint Petersburg Prosecutor General's Office and see this joint action with law enforcement as the sine qua non of their effectiveness. The organizations that set up LBI acted together from 2008 to block criminal content and also to report those uploading it to the police, with whom they formed close links. LBI itself, although a "private initia-

---

[65] "Za ideei sozdaniia kiberdruzhin mogut stoiat' siloviki, schitaet pravozashchitnik," RIA Novosti, November 2, 2018. https://ria.ru/20181102/1532019900.html.

[66] "'Legalizatsiia kiberstukachestva': RosKomSvoboda sobrala mneniia ekspertov o zakonoproekte, kotorym predpolagaetsia uzakonit' tak nazyvaemye kiberdruzhiny po vyiavleniiu v Seti zapreshchennoi informatsii," Roskomsvoboda, November 6, 2018. https://roskomsvoboda.org/42836/.

[67] The 50-Cent Party is the term used for internet commentators hired by Chinese authorities, at 0.5 yuan per post, to influence public opinion in ways beneficial to the Chinese Communist Party.

tive," was cited by the Ministry of Communications to all telecom operators in 2011 as a key institution, worthy of subsidy, although not actually a subdivision of the ministry.

These forms of cooperation with the institutions, already established in the 2000s, are now taking on new shapes as cyberspace in Russia rapidly changes. The adoption of coercive legislation, possibilities for blocking websites, deployment of surveillance technology via control boxes or access providers, and plans for "sovereignty" over Runet all raise the question of the place of citizen initiatives in the booming field of online security. The popularity of cyber vigilantism is part of the assertion of a political model seeking legitimacy through shared moral and patriotic references. Via online surveillance by the cyber patrols, the aim is to defend certain moral boundaries seen as fundamental to maintaining the community locally and nationally, and this includes an online decorum based on respect for morality and tradition. "We work with young people, students, public institutions. We call it internet public health," says Andrei Zlobin, head of *kiberdruzhinniki* in Vladimir Oblast.[68] Computer security courses in schools and universities are civic and moral education courses. These initiatives involve a form of normalization, which remains separate from the radical autonomous vigilantism that goes as far as physically hunting down offenders, doxxing and shaming them online. The cyber patrols' main weapon is the threat of blocking or closing down a website, a page, or a user account, after reporting it to the authorities. Cybersecurity experts are rather skeptical that these now-common practices could become massively adopted. To some extent, they are part of "security theater" where the important thing is to signal a strict attitude, even though this helps create distrust towards the digital world and a popular demand for greater online protection.

This research on Runet regulation volunteers since the 2000s shows the coexistence of several online citizen surveillance models, from the "expert" citizen investigators to the "political" cyber patrols. The tensions between them are fed by the competition in Russia between different supervisory agencies. These agencies compete for budget resources but also keep an eye on each other and, in addition, are ultimately monitored by a "loyalist" civil society. The large number of vigilante movements does not indicate a weakness of the state or its neoliberal privatization, so much as its constant reinvention (Fourchard 2018:177). "Cheap policing" is not just a way to add resources for the police but is also a way of monitoring it, in line with reforms that have followed frequent criticism of the police in Russian society since 2008–2009. Under the new bill there will be mutual vigilance between law-enforcement agencies and online surveillance volunteers, regulated by this legal framework. Russia is thus a test laboratory for plural forms of citizen participation in online security, at a time when legal and technical surveillance instruments are increasingly available to a host of public, private, and civilian operators; their relationships involve cooperation as well as tensions and competition.

---

[68] Ivan Medvedev, "Poluchat li kiberdruzhinniki ofitsial'nyi status?" BFM.ru, March 4, 2019. https://www.bfm.ru/news/408359.

REFERENCES

Asmolov, Gregory. 2015. "Welcoming the Dragon: The Role of Public Opinion in Russian Internet Regulation." Internet Policy Observatory, Center for Global Communication Studies at the Annenberg School for Communication at the University of Pennsylvania. https://pdfs.semanticscholar.org/ea61/880449ad50dcb5d025bdba80f15b44e14d7c.pdf.

Asmolov, Gregory, and Polina Kolozaridi. 2017. "The Imaginaries of RuNet: The Change of the Elites and the Construction of Online Space." *Russian Politics* 2(1): 54–79. doi:10.1163/2451-8921-00201004.

Boltanski, Luc, and Laurent Thévenot. [1991] 2006. *On Justification: Economies of Worth*. Princeton, NJ: Princeton University Press.

Daucé, Françoise. 2013. *Une paradoxale oppression: Le pouvoir et les associations en Russie*. Paris: CNRS Éditions.

Deibert, Ronald, and Rafal Rohozinski. 2010. "Control and Subversion in Russian Cyberspace." Pp. 15–34 in *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, ed. by Ronald Deibert, John Palfrey, Rafal Rohozinski, and Jonathan Zittrain. Cambridge, MA: MIT Press.

Favarel-Garrigues, Gilles. 2018. "Justiciers amateurs et croisades morales en Russie contemporaine." *Revue française de science politique* 68(4):651–667. doi:10.3917/rfsp.684.0651.

Favarel-Garrigues, Gilles. 2019. "Digital Vigilantism and Anti-Paedophile Activism in Russia: Between Civic Involvement in Law Enforcement, Moral Policing and Business Venture." *Global Crime*. doi:10.1080/17440572.2019.1676738.

Favarel-Garrigues, Gilles, and Laurent Gayer. 2016. "Violer la loi pour maintenir l'ordre: Le vigilantisme en débat." *Politix* 29(115):7–33. doi:10.3917/pox.115.0007.

Fourchard, Laurent. 2018. "Le vigilantisme contemporain: Violence et légitimité d'une activité policière bon marché." *Critique internationale* 78(1):169–186. doi:10.3917/crii.078.0169.

Gabdulhakov, Rashid. 2018. "Citizen-Led Justice in Post-Communist Russia: From Comrades' Courts to Dotcomrade Vigilantism." *Surveillance & Society* 16(3):314–331.

Huey, Laura, Johnny Nhan, and Ryan Broll. 2013. "'Uppity Civilians' and 'Cyber-Vigilantes': The Role of the General Public in Policing Cyber-Crime." *Criminology and Criminal Justice* 13(1):81–97. doi:10.1177/1748895812448086.

Jobard, Fabien, and Jacques de Maillard. 2015. *Sociologie de la police: Politiques, organisations, réformes*. Paris: Armand Colin.

Kasra, Mona. 2017. "Vigilantism, Public Shaming, and Social Media Hegemony: The Role of Digital-Networked Images in Humiliation and Sociopolitical Control." *The Communication Review* 20(3):172–188. doi:10.1080/10714421.2017.1343068.

Lemieux, Cyril. 2007. "À quoi sert l'analyse des controverses?" *Mil neuf cent: Revue d'histoire intellectuelle* 25(1):191–212.

Loveluck, Benjamin. 2016. "Le vigilantisme numérique, entre dénonciation et sanction: Auto-justice en ligne et agencements de la visibilité." *Politix* 115(3):127–153. doi:10.3917/pox.115.0127.

Loveluck, Benjamin. 2019. "The Many Shades of Digital Vigilantism: A Typology of Online Self-Justice." *Global Crime*. doi:10.1080/17440572.2019.1614444.

Matsui, Yasuhiro, ed. 2015. *Obshchestvennost' and Civic Agency in Late Imperial and Soviet Russia: Interface between State and Society*. New York: Palgrave Macmillan.

Moncada, Eduardo. 2017. "Varieties of Vigilantism: Conceptual Discord, Meaning and Strategies." *Global Crime* 18(4):403–423. doi:10.1080/17440572.2017.1374183.

Myles, David, Florence Millerand, and Chantal Benoit-Barné. 2016. "Résoudre des crimes en ligne: La contribution de citoyens au *Reddit Bureau of Investigation*." *Réseaux* 197–198(3):173–202. doi:10.3917/res.197.0173.

Nérard, François-Xavier. 2004. *Cinq pour cent de vérité: La dénonciation dans l'URSS de Staline*. Paris: Tallandier.

Nisbet, Erik. 2015. "Benchmarking Public Demand: Russia's Appetite for Internet Control." Internet Policy Observatory, Center for Global Communication Studies at the Annenberg School for Communication at the University of Pennsylvania. https://global.asc.upenn.edu/app/uploads/2015/02/Russia-Public-Opinion.pdf.

Oates, Sarah. 2013. *Revolution Stalled: The Political Limits of the Internet in the Post-Soviet Sphere*. Oxford: Oxford University Press.

Soldatov, Andrei, and Irina Borogan. 2015. *The Red Web: The Struggle between Russia's Digital Dictators and the New Online Revolutionaries*. New York: PublicAffairs.

Tselikov, Andrey. 2014. "The Tightening Web of Russian Internet Regulation." Berkman Center Research Publication no. 2014-15. doi:10.2139/ssrn.2527603.

Vendil Pallin, Carolina. 2017. "Internet Control through Ownership: The Case of Russia." *Post-Soviet Affairs* 33(1):16–33. doi:10.1080/1060586X.2015.1121712.

Volkov, Vadim. 2002. *Violent Entrepreneurs: The Use of Force in the Making of Russian Capitalism*. Ithaca, NY: Cornell University Press.

Yablokov, Ilya. 2017. "Social Networks of Death: Conspiracy Panics and Professional Journalistic Ethics in the Post-Soviet Russia." *Quaderni* 94(3):53–62. doi:10.4000/quaderni.1113.

ОТ ГРАЖДАНСКИХ СЛЕДОВАТЕЛЕЙ К КИБЕРПАТРУЛЯМ: ВОЛОНТЕРСКОЕ РЕГУЛИРОВАНИЕ ИНТЕРНЕТА В РОССИИ

Франсуаза Досэ, Бенжамен Ловлюк, Белла Остромоухова, Анна Зайцева

Франсуаза Досэ, Центр русских, кавказских и центрально-европейских исследований (CERCEC) при Высшей школе социальных наук (EHESS). Адрес для переписки: EHESS, 54 Boulevard Raspail, 75006 Paris, France. francoise.dauce@ehess.fr.

Бенжамен Ловлюк, i3-SES, Парижский институт телекоммуникаций (Télécom Paris), Парижский политехнический институт (IP Paris). Адрес для переписки: Télécom Paris, 19 Place Marguerite Perey, 91120 Palaiseau, France. benjamin.loveluck@telecom-paris.fr.

Белла Остромоухова, Eur'Orbet, Университет Сорбонны. Адрес для переписки: Sorbonne Université, 108 Boulevard Malesherbes, 75017 Paris, France. ostrob@gmail.com.

Анна Зайцева, LLA Créatis, Тулузский университет имени Жана Жореса. Адрес для переписки: Université Toulouse–Jean Jaurès, Département des langues étrangères, 5 Allée Antonio Machado, 31100 Toulouse, France. anna.zaytseva@univ-tlse2.fr.

Работа выполнена в рамках исследования ResisTIC («Les résistants du net: Critique et évasion face à la coercition numérique en Russie») при финансовой поддержке французского национального агентства по научным исследованиям (ANR).

Государственный контроль за рунетом в последние годы значительно усилился. Наряду со специализированными службами и частными компаниями появляются группы рядовых граждан, которые на добровольных началах занимаются отслеживанием «негативного контента» – информации об идущей в разрез с социальными нормами либо криминальной деятельности. Однако спектр действий этих групп, их идеологические убеждения и моральные установки сильно различаются между собой и меняются со временем. В статье анализируются две официально зарегистрированные некоммерческие организации: Молодежная служба безопасности (МСБ) и Лига безопасного интернета (ЛБИ), под эгидой которой были созданы бригады кибердружин. Члены МСБ, которых можно назвать «гражданскими следователями», приобрели в процессе работы многочисленные технические и юридические навыки и активно сотрудничают с правоохранительными органами. Волонтеры ЛБИ, со своей стороны, настроены более консервативно: они заботятся о сохранении «моральных устоев» и, развивая активную образовательную деятельность, желают оградить интернет-пользователей от потенциальных киберугроз. Состоявшиеся в марте 2019 года в Общественной палате слушания закона о киберпатрулях выявили конфликт между разными позициями. Те, кого мы называем «политиками» (депутаты Госдумы, руководители кибердружин), высказывались в пользу закона. Спикеры же, которых мы называем «экспертами» (представители IT-индустрии и специалисты по информационной безопасности), высказывались против, ссылаясь на неэффективность киберволонтеров. Что же касается третьей группы – защитников свободного и демократического рунета, – они не высказываются на официальных площадках, однако их голоса оказываются слышны в социальных сетях и независимых медиа.

Ключевые слова: Россия; цифровый вигилантизм; интернет; кибердружины; государственный контроль; надзор