DOI : 10.14746/pp.2020.25.4.8

Viktor Aleksandrovich SIDOROV
Saint Petersburg State University
ORCID ID: https://orcid.org/0000-0002-8819-6815

# The image of the "Russian hacker" and cyberphobia of the "digital environment"

**Abstract:** The "digital environment" is perceived as a new situation in the political consciousness of the society, as well as a source of xenophobia in politics. In the context of political uncertainty in the world, journalism is becoming a vehicle for spreading cyberphobia – a new type of social fear. Cyberphobia is understood as a natural reaction of public consciousness to the intensification of new types of crimes against the individual and society with the use of "digital" technologies. The new informational reality has predetermined cyberthreats that appeared in the media leading to the most dangerous social phobia. This, for instance, has been combined with the idea of the "Russian hacker" and his personification as the world Evil.

**Key words:** cyberphobia, "digital environment," political journalism, image of the enemy, Russian hackers

## 1. Introduction

Modern journalism has been accompanied by a continuous transformation of the society caused by the growing struggle of its strata, minorities and other communities for dominance in the setting of social values. Nowadays, the aggravation of the social situation results in a political turbulence experienced when "we go through a slow collapse of the old world order and the creation of a new one" (Karaganov, 2019, p. 19). A new world order in the economy, politics, and culture is not possible without the strengthening of new values and overthrowing of old ones in the public consciousness. An ideal space for social awareness of change is the public sphere dominated by the media and their diverse journalist products.

We are wary of the widespread belief that new media technologies and mobile communication will lead to the strengthening of democracy in the society, enhanced awareness of events in the world and in the country, as well as deepened knowledge about the essence of socio-political and cultural processes. According to Blokhin, in the contemporary "society of spectacle," there is a functional shift in journalism from informing to "representing," and at the same time, "the spectator becomes the main character of a performance created in his name, and he carries out mediation at the level of personal media behavior" (Blokhin, 2019, p. 18). In the "digital environment," "personal media behavior" becomes public. Therefore, one can share the anxiety of the Italian philosopher Gianni Vattimo about the "massed man," who has "reached the microphone" and who is intoxicated by the opportunity to enter the media sphere without any restraining actions by journalists, editors and other competent specialists authorized to select information. At the same time, the transition of mass communication to a higher level

of technology has an impact on journalism as a profession and as a means of political interaction in the world. The indefiniteness of ideas regarding the essence of journalism has tempted us to ease its application in social conflicts; many journalistic texts become vehicles for aggressive intentions and phobias of the mass society.

Mass communication technologies have changed their appearance: in the Internet, a recipient has mastered primary skills of informational response to a communicator’s message and often tries to become one himself. Therefore, the communicator is now changing his methods of influencing public consciousness. However, social shifts have failed to strengthen mutual understanding of people in the renewed media space, and they opened the way for the expression of aggressive emotions and opinions. Communicative aggression begins when the opponent/enemy inflicts a planned or spontaneously caused ideological-political and cultural-moral defeat through all media channels. The social elements of the early 21st century have their own distinctive features. And these traits cause a certain alarm. As the famous political scientist Bystritsky writes, “Firstly, protest activity occurs in a situation of incredible information and communication abundance. ... Secondly, it is a consequence of the new communication situation, too, but not only. ... Thirdly, protest borders get blurred. Again, the new information and communication environment plays its a role. Without a clear agenda, speeches turn out to be an element of general dissatisfaction with what is happening” (Bystritskiy, 2019, p. 3). In the dynamically growing mass of people involved in the network of conflicts in the media, there is usually a willingness to transfer aggression from a symbolic space to a physical space: “a significant number of pressure resources and network communities represent and aggregate radical and extremist views which are then articulated in the public political space” (Volodenkov, 2019, p. 119). This leads to a “dynamics of hatred,” which Huntington once described as a condition of “mutual fears, distrust and hatred who feed each other” (Smit, 2018, pp. 432–433).

## 2. Concept headings

Communicative aggression is a manifestation of social contradictions in the media (Nazarchuk, 2011, p. 157). The contexts of communicative aggression are politics, culture, sports, urban life, interpersonal relationships. They are permeated with media manifestations of hatred, violence, insults, threats against speakers of “other” languages, artistic tastes, and political views. Today, there is a high risk of excessive use by journalists and politicians of concepts with a sharply negative connotation, in view of their ability to cause aggressive reactions in the society during the aggravation of political conflicts. This is, in part, the conclusion of a research project by scientists of St. Petersburg State University, Russia, and the University Adam Mickiewicz, Poland. The results of the study (2017–2019) made it possible to determine the involvement, without exception, of all processes deployed on the vast field of mass communication disseminating aggressive “media behavior.”

The main feature of the political media discourse is the emphasis on the image of the enemy – as if repeating algorithms of information wars from the past, but in a new round of political history – the enemy portrayed in the media discourse acquired a particularly

sophisticated appearance, he appears as extremely insidious and almost elusive. The latter – the impunity of an imaginary adversary – should especially affect the mass audience of journalism and online communities. And the stronger the influence is, the higher is the degree of aggression in the “digital environment.” According to historian and culturologist Robert Myushemble, a well-known phenomenon, originating in the collective imagination, which “gives rise to the figure of Evil (or the Devil) in the society, is seeking to join the most active forces operating in this society” (Myushemble, 2005, pp. 46, 49). Since current media practice is primarily moving to the Internet, this face of the evil is moving there as well. Its new virtual appearance has been formed and it remains nothing more than a product of social reality rather than its repetition in the media.

Cyber fraud in a network environment, with credit cards and deposits, has become part of our everyday life and has formed the foundation for creating a new image of the enemy. Anyone can be a victim of fraud in the cyber environment, including shops, public funds, banks, and ordinary citizens. Moreover, such fraudulent operations very often stay unpunished which is why the vast majority of people consider themselves defenseless. This feeling is fueled by numerous media publications about hacking in one form or another. In the global media space, the hacker has become the most negative figure. From 01/01/2016 to 12/31/2019, on the InoSMI website, we found 985 publications referring to the image of a hacker, and in 645 cases these were Russian hackers. It was also found that over the same period the total number of publications in which the issue of information wars was raised, in one way or another, was 3,500. These publications were accompanied by references to such keywords as “hackers” and “Russian hackers.” Additionally, other keywords are also used in the political discourse: “hybrid wars” (1732) and “cyber warfare” (521).

Due to cyber fraud, the society rejects much of what is happening in the “digital world,” and it has become an environment which most citizens can no longer do without. Many events in the “digital world” cause distrust, especially since they are interpreted by politicians in the media, or by experts in the field of information security. In the eyes of the public, cyberbullying became a concept of denouncing any criminal acts against security of an individual, financial security included, as well as his democratic rights and freedoms. The hacker, most often a Russian hacker, personifies criminal acts in the cyberspace. InoSMI,[1] an informative and analytical portal, provides the best opportunity to analyze hacker’s representation in the media discourse. The portal publishes excerpts from leading world publications on relevant topics with the possibility of making a quick transition to the original full source text. This allows us to identify leading trends of the world press when covering events in politics, economics, culture, sports, etc. However, we should remember that the InoSMI site presents the RIA Novosti project. It means that the site is not free from a conceptual focus on researching world media materials about Russia. Nevertheless, for the purpose of our analysis, the selection of materials about Russia publicized at the website is representative: foreign publications on Russia’s involvement in the InoSMI include powerful layers of information on xenophobia, in all its diversity.

[1] InoSMI – a portal providing analytical reviews. It is owned to the Russian News Agency (RIA) News; financial support is provided by the Federal Press and Information Agency of Russia (Rospechat).

## 3. Discussion

The spread of social phobias, alongside private manifestations of crime in the digital world, has transformed them into cyberphobias. Today, a man is in a state of constant anticipation of troubles and inconveniences in the so-called virtual world. Our newspaper research on cyber warfare, hackers, and Russian hackers includes information on both financial and economic cyber fraud and political cyber fraud. In the first group of publications, samples have a common denominator in the form of a statement of information problems/cyber security, which everyone needs, including states, businesses, and ordinary people. In the second group, information about political offenses in the “digital” world is a reflection of not only actual events, but it is brought there by the effort of political propaganda. There is too much temptation to use the new type of xenophobia for utilitarian political purposes. The dividing line between the two clusters is fundamental: in the first case, cybercrime is cosmopolitan and knows no boundaries; in the second, on the contrary, borders between worlds and states are clearly drawn in newspaper publications by politicians and journalists.

Of the 645 articles that contain keywords of “Russian hackers,” 64 publications were selected by random sampling (10% of the total). The analysis of selected articles discovered that these publications reflect cybersecurity issues and social fears related to them. These phobias are represented in articles through statements that can instill strong anxiety among readers.

According to the number of references, the first place is taken by a cyber threat to the political system of a democratic society (44%), and the sinister image of the Russian origin hacker (37%). It is then followed by the threat of Russian hackers interfering in political processes of Western countries, including cyber espionage (25%). Authors of these publications are particularly interested in financial security issues – almost a quarter of articles (26%) analyze hackers’ criminal activity in the financial sector. Articles refer to a major damage suffered by banks. Additionally, the threat to the critical infrastructure may scare the reader since hackers can disrupt the operation of power supply and other utilities (12% of articles). The next stage of the study includes the analysis of 20 articles selected by a search engine due to the presence of a key concept of “Russian hackers.” Findings show the same results as the previous analysis based on random sampling. Therefore, there is reason to move on to an in-depth study of these 20 publications.

The authors of these articles, who evaluated cyber threats to the entire political system of a democratic society and hackers’ attacks in the West, operate with characteristic assertions that “Russian trolls and hackers have quieted down and stepped aside in anticipation of the midterm elections, having carried out large-scale cyberattacks and a disinformation campaign in the presidential election in USA in 2016” (Voli, Makmillan, 2018); and “with the help of Kaspersky products, the Russian state carried out attacks against foreign targets” (Rassel, 2017); that “a hacker from Russia allegedly hacked 272 million usernames and passwords on popular email sites Gmail, Yahoo and Hotmail and then began to trade them in the criminal Russian underground. ... This is not just one hacker, it is a whole organization – a Russian state controlled by Putin” (Limitoun, 2016).

However, the phraseology of articles on cybercrime in the areas of finance and the banking system fundamentally differs from the tone of publications on cyberthreats in

politics. If in the field of politics, mainly unproven or only potential threats (though quite ominous) are portrayed. Articles considering potential financial cyber fraud show optimism, because, as journalists put it, relevant US departments and leading European countries successfully counteract Russian criminals stealing millions of dollars. Optimism is fully reflected in the title of the article “How One German Revealed the Legendary Russian Hacker” (Neller, 2016). The article “Hunting for a Russian hacker” is similar and describes practically the same events as the previous one. It mainly elaborates on the American story. Although the anti-hero is the same hacker Bogachev. Although he cannot be brought to justice, damage from his cybercrimes is minimized. In 2015, the US government offered a US$3 million reward for the capture of Bogachev – the largest reward ever offered by the US government for a cybercriminal (Graff, 2017). Consequently, these articles are not about what might happen, but they are about what has already happened and issues that US departments have already resolved.

There are fewer publications describing cyberthreats to everyday life of ordinary citizens. Nevertheless, they emanate a sense of citizen’s powerlessness in front of a powerful criminal behind a computer monitor. It seems that a Russian hacker can do anything from power outage in Ukraine (Grinberg, 2019) and disruption of utility services, e.g. the supply of hot water to American homes. Criminal intentions are hatched to attack critical infrastructure in a number of countries, including the US (Smit, 2018).

Almost a half of publications analyzed (40%) attempt to outline Russian hackers’ main areas of criminal activity. The main area is the theft of money from banks in America and Europe. Hackers also include talented scammers, for example Roman Seleznev’s innovations transformed carding, a fraud involving the use of credit cards (Kozlovskiy, 2017). The Western media essentially try to prove hacker’s connections with the Russian special services (Graff, 2017). Such ties mean that they have the support of the Russian government. As a result, Russian hackers achieved an impressive success: “the Fancy Bear hacker group, which is supported by the Kremlin and blamed by the West for aggressive global cyberattacks on state and military targets in Europe, needs on average only 18 minutes and 49 seconds to crack a computer and access the operational system and other machines in the network of a hacked organization” (Bridzh, 2019).

This is an example how the media continuously describe the escalation of cyber threats in general, in particular caused by hackers from Russia actively supported by special services. Publications emphasize their unpredictability, sophistication of technologies used and their goal of stealing money from bank accounts of different organizations and ordinary citizens. All for the purpose of destabilization of political institutions and military facilities in the US and Europe (Bridzh, 2019). However, not all journalists adhere to this concept. For example, an Israeli journalist expresses his doubt when he analyzes hacker attacks on analytical centers and headquarters of political parties (Gurvits, 2016). Moreover, another publicist is convinced that one should investigate the activity of “hackers from the USA or Great Britain – ... they are even faster than well-known Russian hackers” (Boyt, 2019).

Results of the analysis indicate a widespread use of the image of a cyber threat that has a strong effect on ordinary people. An average citizen is primarily concerned about the safety of his modest means kept on a bank account, despite reassurance that law enforcement agencies are efficient in dealing with Russian hackers. As a Spanish journalist

puts it “the unpleasant aftertaste from mentioning the Russian threat remains, so the goal has been achieved” (Pointless, 2017). Fear remains because it is constantly reinforced by an increase in media phobias about cyber threat to civic rights and freedoms of a democratic society. Journalists, members of the same society, are also prone to phobias of cyber threats.

## 4. Conclusion

There has been a quantum leap in information technology, but it has not contributed to the modern media discourse. Nowadays, the consciousness of the society is struck by a new type of phobia – the fear of dangers that lurk in the depths of the “digital space” and are personified by the image of a hacker. At the same time, cyber threats are quite real. For example, losses from the criminal activity in the banking sector amount to hundreds of millions of dollars (in the analyzed period alone). Funds disappear from citizens’ credit cards, operation of power plants is violated, and secrets of governments, parties, and armies are stolen. The spread of cyber threat social phobias is a logical result of uneven cultural development and the use of technical capabilities of the new information environment. Under these conditions, a cyber threat turns into obsessive, irrational and basically uncontrollable fear, which is implied by the definition of phobia. Cyberphobia affects almost all social strata, including journalists and other media workers. The spread of a new phobia in the media is objectively predetermined and cannot be considered an intended result. Moreover, the new phobia, reinforced by cybercrime facts, has become an argument used by politicians and propaganda. The fact that the phobia is directed towards the “Russian hacker” allows lobby groups and politicians to keep voters in a state of tension and encourage them to vote for a particular political group. The emergence of a new type of phobia has predetermined political propaganda strategies for a long time to come.

## Bibligraphy

*Bessmyslennyy razgovor o russkikh khakerakh mezhdu Mariano Rakhoem i Karlosom Erreroy* [Pointless conversation about Russian hackers between Mariano Rajoy and Carlos Herrera] (2017), in: InoSMI, 17 November, https://inosmi.ru/politic/20171117/240790844.html, 05.01.2020 (in Russ.).

Blokhin I. N. (2019), *Zhurnalistika kak sotsiokul’turnyy fenomen* [Journalism as a sociocultural phenomenon], in: *Zhurnalistika i kul’tura obshchestva* [Journalism and society culture], Ucheb. posobie, ed. M. A. Voskresenskoy, SPb.: Izd-vo VVM, pp. 6–26 (in Russ.).

Boyt P. (2019), *Doklad CrowdStrike: russkie khakery samye bystrye* [Report by Bloods Strike: Russian hackers are the fastest], in: InoSMI, 20 fevr., https://inosmi.ru/social/20190220/244611908.html, 05.01.2020 (in Russ.).

Bridzh M. (2019), *Russkie khakery ostavili kitaytsev daleko pozadi* [Russian hackers left the Chinese far behind], in: InoSMI, 23 February, https://inosmi.ru/social/20190223/244630775.html, 05.01.2020 (in Russ.).

Bystritskiy A. (2019), *Vosstanie mass* [Uprising of the masses], in: Izvestiya, p. 3, 25 Dec., https://iz.ru/957667/andrei-bystritckii/vosstanie-mass, 05.01.2020 (in Russ.).

Graff G. (2017), *Okhota na russkogo khakera* [The hunt for Russian hacker], in: InoSMI, 22 marta, https://www.wired.com/2017/03/russian-hacker-spy-botnet/, 05.01.2020 (in Russ.).

Grinberg E. (2019), *Kak russkie khakery chut’ ne ostavili Ukrainu bez elektrichestva* [How Russian hackers almost left Ukraine without electricity], in: InoSMI, 13 sent., https://inosmi.ru/politic/20190913/245821827.html, 05.01.2020 (in Russ.).

Gurvits I. (2016), *Ne vsiakii khaker – russkii shpion* [Not every hacker is a Russian spy], in: InoSMI, 29 November, https://inosmi.ru/politic/20161129/238298756.html.

Karaganov S. A. (2019), *Ukhod voennogo prevoskhodstva Zapada i geoekonomika* [Western military superiority and geoeconomics], in: Polis. № 6, pp. 8–21, https://www.politstudies.ru/files/File/2019/6/Polis-6-2019-Karaganov.pdf, 05.01.2020 (in Russ.).

Khantington S. (2003), *Stolknovenie tsivilizatsiy* [Clash of civilizations], per. s angl. OOO «Izdatel’stvo AST», M., 603 p.

Kozlovskiy V. (2017), *Delo Selezneva: nechistoserdechnoe priznanie osuzhdennogo v SShA russkogo khakera* [The case of Seleznev: cruel confession of a Russian hacker convicted in the United States], in: InoSMI, 22 April, https://inosmi.ru/social/20170422/239199260.html, 05.01.2020 (in Russ.).

Limitoun Dzh. (2016), *Pochemu iz russkikh poluchayutsya khoroshie khakery?* [Why do Russians get good hackers?], in: InoSMI, 6 May, https://inosmi.ru/social/20160506/236443184.html, 05.01.2020 (in Russ.).

Myushemble R. (2005), *Ocherki po istorii d’yavola: XII–XX vv.* [Essays on the history of the devil: XII–XX centuries], per. s fr., Novoe literaturnoe obozrenie, M., 584 p. (in French).

Nazarchuk A. V. (2011), *Ideya kommunikatsii i novye filosofskie ponyatiya KhKh veka* [The idea of communication and new philosophical concepts of the twentieth century], in: Voprosy filosofii [Philosophy Issues], № 5, pp. 157–165 (in Russ.).

Neller M. (2016), *Kak odin nemets legendarnogo russkogo khakera razoblachil* [How a German of the legendary Russian hacker exposed], in: InoSMI, 8 May, https://inosmi.ru/multimedia/20160508/236453693.html.

Rassel B. (2017), *Russkie khakery ispol’zovali programmnoe obespechenie Kasperskogo dlya poiska nezashchishchennykh dokumentov ANB* [Russian hackers used Kaspersky software to search for unsecured NSA documents], in: InoSMI, 6 October, https://inosmi.ru/politic/20171006/240454058.html, 05.01.2020 (in Russ.).

Smit R. (2018), *Rossiyskie khakery mogut otklyuchit’ goryachuyu vodu v SShA* [Russian hackers can turn off hot water in the United States], in: InoSMI, 24 July, https://inosmi.ru/politic/20180724/242814221.html, 05.01.2020 (in Russ.).

Voli D., Makmillan R. (2018), *Nikto ne znaet, pochemu russkie khakery proignorirovali promezhutochnye vybory* [No one knows why Russian hackers ignored midterm elections], in: InoS.MI, 13 November, https://inosmi.ru/politic/20181113/243922440.html, 05.01.2020 (in Russ.).

Volodenkov S. V. (2015), *Internet-kommunikatsii v global’nom prostranstve sovremennogo politicheskogo upravleniya* [Internet communications in the global space of modern political governance], Izd-vo Mosk. un-ta, M., 272 p. (in Russ.).

---

**Wizerunek „rosyjskiego hakera” i cyberfobii „środowiska cyfrowego”**

**Streszczenie**

„Środowisko cyfrowe” postrzegane jest jako nowa sytuacja w świadomości politycznej społeczeństwa, a także źródło ksenofobii w polityce. W kontekście niepewności politycznej na świecie dziennikarstwo staje się narzędziem szerzenia cyberfobii – nowego rodzaju społecznego strachu. Cyberfo-

bia rozumiana jest jako naturalna reakcja świadomości społecznej na nasilenie się nowych rodzajów przestępstw przeciwko jednostce i społeczeństwu z wykorzystaniem technologii „cyfrowych.” Nowa rzeczywistość informacyjna z góry określiła cyberzagrożenia, które pojawiły się w mediach, prowadzące do najgroźniejszej fobii społecznej. To na przykład łączy się z ideą „rosyjskiego hakera” i jego personifikacją jako świata Zła.

**Słowa kluczowe:** cyberfobia, „środowisko cyfrowe”, publicystyka polityczna, wizerunek wroga, rosyjscy hakerzy

Article submitted: 12.08.2020; article accepted: 21.09.2020.