JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2023 Volume 13
https://doi.org/10.47459/jssi.2023.13.14

THE FACES OF HACKTIVISM BY THE ANONYMOUS COLLECTIVE IN THE CONTEXT OF RUSSIAN WAR AGAINST UKRAINE. COMPARISON BETWEEN 2014 AND 2022

Alina Betlej

Centre of Sociological Research on the Economy and the Internet, Department of Economic and Digital Sociology,
The Institute of Sociological Sciences, The John Paul II Catholic University of Lublin,
Al. Racławickie 14, 20-950 Lublin, Poland

E-mail: alina.betlej@kul.pl

Received 22 March 2023; accepted 25 June 2023; published 30 July 2023

Abstract. Hacktivism is a social phenomena which evokes different social assessments. The definitions of a term differ in many respects. This theoretical model of hacktivism has not yet been implemented into an empirical strategy for sociological research. The paper describes the the main initiatives taken by Anonymous collective during the 2014 conflict in Ukraine, which is considered by many researchers to be the first stage of preparation for the war triggered by Russia in 2022. Author analyses the collective's activity in 2022, after the war started, in order to identify similarities and differences in the creation of information messages about the situation. The comparative analysis covers information published in Anonymous' tweets and selected online news services. She asks the question about the possible consequences of Anonymous actions in the open cyber field for the social moods around the world. To what extent these media messages and their construction have reflected the social perception and/or social attitudes towards Russia's aggression? The theoretic explorations were embedded mainly on two methods: criticism of writing and the analytical and comparative one.
.

Keywords: Hacktivism; Anonymous; cyber war; cyberspace; new technologies

Reference to this paper should be made as follows: Betlej, A. 2023. The Faces of Hacktivism by the Anonymous Collective in the Context of Russian War Against Ukraine. Comparison between 2014 and 2022. *Journal of Security and Sustainability Issues*, 13, 143-152.
https://doi.org/10.47459/jssi.2023.13.14

JEL Classifications: F51

1. Introduction

The transformation of cyberspace is introducing new social phenomena into people's daily lives (Betlej, 2019; Aleksejeva et. al. 2021). In fact, this hybrid space is becoming a platform for the presentation of independent ideas, as well as a tool for collecting information databases about the citizens of contemporary surveillance societies. Hybrid space is largely virtually mediated. The information and communication technologies are tools of creative participation of social actors in shaping the shared narratives of everyday life and mediated production of interpretational schemes used by different categories of users embedded in a specific axionormative context (Bedianashvili, 2021; Chojnacki, 2023) Today, the Internet seems to play a special role in the process of constructing social reality. It is not only a tool, but also a self-referential world of sense sources. These two opposing tendencies become apparent in the activities of the emerging civil disobedience movement on the one hand and the rapid development of governmental and corporative agencies responsible for data gathering and processing on the other (Banks, 2017; Beck, 2016). Each has an impact on socio-economic change. The effects of these impacts are often ambivalent (Bodford et. al., 2018; Chojnacki, 2021; Katina et al., 2023). The social assessment of certain types of social action is highly controversial. The future may bring a more striking division amongst the Internet users into those who have been consciously or unconsciously subjected to surveillance and those who have escaped into the specific underground. The axiological aspects are also discussed to be changed. The right to privacy, to remain anonymous, to have freedom of communication are reappearing in a new context in the public debate.

The emergence of new social actors on the world's scene may disrupt the future social order (Betlej, 2019; Fuchs, 2014; Gondek, 2022). Nowadays, we can observe the transfer of civil disobedience to cyberspace (Coleman, 2013; 2014). It is perceived as an effective tool of the free expression of ideas and its popularization on a global scale. An interesting process is the emergence of new social movements calling for freedom and change in society and similar behaviour spreading like viruses according to the principles of self-organisation. Activities of different types of hacktivists on the Internet are often analyzed in terms of threats to the traditional agendas responsible for sustaining social order and new (Betlej, 2014; 2022; Gondek, 2020). The threats may be perceived as the opportunities for sustainable social development within the different analytical frames. Shadow Internet may breed new types of social activities related to forecasts about social networks' power of change. The scale of the permeation of the Internet into real space has long since exceeded critical mass. The growing importance of hacktivist movements illustrates the shift in societal expectations of citizens' privacy and freedom of expression. In this sense, the hacktivist movement represents the first of the above-mentioned phenomena. An interesting group active on the Internet and associated with civil disobedience is Anonymous. The undertaken actions have been attracting considerable social attention as well as media publicity since the beginning of Russia's aggression in Ukraine on 24 February 2022. Anonymous has distributed hacktivism of the specific kind related to its power of social impact. The collective has declared cyber war against Vladimir Putin's government following the Russian invasion of Ukraine. This was not the first time Anonymous had become involved in the Russian-Ukrainian conflict. The hacktivists had already become active during the initial conflict in Ukraine caused by the removal of Viktor Yanukovych from power and the Russian annexation of Crimea in 2014.

In this article, the author will describe the main initiatives taken by Anonymous during the 2014 conflict, which is considered by many researchers to be the first stage of preparation for the war triggered by Russia in Ukraine in 2022. She will analyse the collective's activity in 2022, after the war started, in order to identify similarities and differences in the creation of information messages about the situation. The comparative analysis will mainly cover information published in Anonymous' tweets and selected online news services. Considering social transformations evoked by technological development one might expect that war in Ukraine was bound to be reflected on the Internet and aggravated social tensions. The question is about the possible consequences of Anonymous actions in the open cyber field for the social moods around the world. To what extent these media messages and their construction have reflected the social perception and/or social attitudes towards Russia's aggression? The characterization of the ongoing information warfare on the Internet and elucidating the action strategies undertaken by pro-Ukrainian hacktivists will help to reveal the information warfare trends in networked societies as well as answer the question about how are Anonymous' strategies changing the way hacktivists' actions are assessed? The paper is structured as follows. Section 2 reviews the literature on conceptualizations of hacktivism. Section 3 describes the Anonymous pro-Ukrainians initiatives on the Internet undertaken in 2014. Section 4 analyzes the hacktivist activities in 2022 immediately after the outbreak of war. Finally, Section 5 indicates the research conclusions.

2. Hacktivism: Questions and Interpretations

To understand the birth of hacktivism and the global narration about new collectivities on the Internet and their social impact, it is necessary to understand the origins of the cyberculture generation in the early beginnings of networks (Sorell, 2015; Mitnick et. al., 2006; Goode, 2015). Hacktivism has its roots going back to the 1970s. The first actions of this kind, which today are combined with the term hacktivism, were, as it were, an expression of the idea of a new cyberculture fighting against any blocking of communication processes and networked knowledge exchange on the Internet (Holt et. al., 2017). Hacktivism is closely related to cyberactivism and initiatives with focus on capturing people's attention on perils of negatively assessed political decisions (Ireland, 2022). What is important, cyberactivism does not always draw from hacker cultures (Ireland, 2022). The interpretation line is therefore blurred. Widely available data, information and knowledge, quickly became symbols of a new, open society, defended by supporters of new social movements and hackers. Popular targets of first-generation hacker cyber-attacks were large corporations conducting advanced scientific research, protecting their most up-to-date knowledge from the public and competitors without large R&D funding. Access to electronic data was at this time almost equated with the category of the universal right to absolute truth. Cyberculture can be understood in this view as a new type of counterculture manifesting itself through the web. The idea of this new movement was expressed in the slogan 'Information wants to be free' (Sorell, 2015; Mitnick et. al., 2006). It was proclaimed in 1984 at the first hacker conference by Steward Brand and was combined with the demand for universal access to information.

The term hacktivism was first used by the group "Cult of the Dead Cow" (cDc) in 1996 (Betlej, 2014). The media popularised the term 'hacktivism' during the 1998-1999 Kosovo conflict, when activists from around the world launched DoS attacks and destroyed or took over many websites to protest against the war and the countries involved. Hacktivism, however, did not fully develop until the beginning of the 21st century, mainly through the activist and hacker collective "Anonymous", founded in 2003. Currently an interesting definition trend can be observed. Acts indicated a short while ago as examples of cyberterrorist activities are called– hacktivism. The word hacktivism is a relatively new construct, which was formed out of a combination of the words: *hacker* and *activist* (Fowler, 2022). Hacker is a person who gains access to a computer system without the owner's consent. This act of gaining access is sometimes associated in cyberculture with rebellion against the system, cyber-anarchism, the digital underground and the Shadow Internet (Betlej, 2014; Betlej 2019).

Sociological descriptions of this social phenomenon vary widely ambivalent (Bodford et. al., 2018; Chojnacki, 2021). Research on hacktivism suggests that a number of factors are significant for activism to take on the skill set of open and/or clandestine hacking in order to evolve into hacktivism (Banks, 2017; Betlej 2014). There is a need for a transdisciplinary approach in this case. Sociological complexities are often overlooked in media reports of events whose main protagonists were members of hacktivist collectives. Hacktivism is most often interpreted as a kind of combination of hacking and socio-political activity (Ireland, 2022). It is described as a manifestation of online self-organisation, a social mobilisation oriented towards achieving specific goals for the wider social good. These activities thus aim to bring about specific social changes. Nowadays, hacktivism is also defined as that cultural and civilisational movement which consists in combining political activism with technological achievements, in order to manifest opposition to actions in the space of widely understood politics (Coleman, 2013; 2014). In another view, the focus is on the second aspect of these initiatives, namely criminal activities in cyberspace (Banks, 2017; Beck, 2016). Hacktivists typically use illegal hacking methods. However, they are distinguished by their political and social motivation. They act with a specific idea to oppose negatively evaluated political decisions or global corporations. The originators of the term, the group 'Cult of the DeadCow', applied it to describe individuals or groups using their computer skills to publicise specific political demands (Betlej, 2014). To date, the aim of hacktivists has primarily been to promote certain attitudes or values in public spaces. The effects of hacktivists are often described as ambivalent. Many researchers draw attention to an important aspect that distinguishes hacktivists from cyber-terrorists. Hacktivists use hacking techniques against websites to temporarily disrupt their functioning. Cyber-terrorists aim to completely destroy websites or cause serious damage that is difficult to repair.

Understanding the place and significance of hacktivism in the contemporary socio-economic transformations of modern societies requires overcoming a specific epistemological obstacle and moving beyond analyses of the cult of personality, individualism and cyberculture heroes. Much of the research has focused on strategies to create a cultural pattern of the hacktivist by referring to well-known figures such as Julian Assange (Ireland, 2022). One of the world's most recognisable hacktivist collectives is Anonymous. In general, Anonymous opposes governments and corporations that they see as participating in censorship or promoting inequality. The group is decentralised, with no real structure or hierarchy (Ireland, 2022). Its participants often have internal debates about which ideas or causes to support. Anonymous members are often characterized as a working class of people who seek a better future for humanity. Its guiding principles are freedom of information, speech, accountability for companies and governments, privacy and anonymity for private citizens. Anonymous has many supporters and critics. It is often deemed to be a threat to national security in the USA. The actions of

Anonymous have been repeatedly described in the context of a war triggered by Russia in Ukraine in 2022. However, the collective has been involved in the conflict for much longer, since 2014. Their 2014 initiatives did not receive as much media publicity, often remaining unnoticed by the global public.

Hacktivism, regardless of its roots, still aims to intervene in existing dominant communication systems. A new aspect of activism is the new unrestricted realm of cyberspace and contestation techniques. However, the techniques of online hacktivism have some lines of continuity going back to established and well-described forms of media activism by social scientists. Indeed, the undermining of the intended meaning or message of advertising can be analysed within the framework of media activism. However, new issues are also emerging, such as the analysis of power relations in the digital world, the new faces of lobbying, the emergence of new reference groups, the entanglement of social activism in informal power structures, the loss of meaning of the longue durée structures, as well as propaganda and disinformation on Internet (Betlej, 2022; Gondek 2018; Gondek 2018). An interesting issue is the questions of how hacktivists mediate the process of global information exchange and the construction of narratives about certain events, social situations, problems and their interpretative schemes.

3. Here we are again. Anonymous actions in 2014

The analysis of hacktivists initiatives in this section refers to the situation of the conflict in Ukraine caused by removing Viktor Yanukovych from power and the annexation of Crimea by the Russians in 2014. On 17 March 2014, Russian President Vladimir Putin signed the treaty on the annexation of Crimea to Russia. As a result of the annexation of Crimea to Russia, economic sanctions were introduced by the European Union and the United States to put pressure on Russia and force it to return Crimea. Even before this decision, the internet had already become an arena for the activities of the Anonymous collective. At the time, three groups of hacktivists were active on the Internet, Anonymous, Caucasus Anonymous and Cyber Berkut. An analysis of the detailed calendar of events directs our attention to a number of significant actions undertaken in cyberspace by the hackers. On 2nd March 2014 the website of the Russian television "Russia Today" fell prey to a hacker attack. The content of the website has been changed. The word "Nazi" has been added to all the information published there:

> "Russian senators vote to use stabilizing Nazi forces on Ukrainian Territory.
> Putin: Nazi citizens, troops threatened in Ukraine, need armed forces' protection.
> Thousands rally against "illegitimate govt", raise Russian flags eastern Ukraine.
> Nazi nationalist leader calls on "most wanted" Nazi Umarov" to act against Russia".

After a somewhat longer break, on 14th March 2014 Russian servers were attacked by hackers related to Anonymous. The official website of the Russian President Vladimir Putin www.kremlin.ru did not operate for several hours. The website fell prey to the DDos type of attack. A similar attack was launched against other Russian websites of the Central Bank, the central Russian television, www.1tv.ru, kavkazpress.ru and of the esteq.net company. The attack was admitted by the Caucasus Anonymous. At the same time the following message was posted on the group's Facebook profile:

> "Here we are Again Russian Servers.
> http://frgk.economy.gov.ru/ TANGO DOWN!!!
> ftp.gov.ru/ TANGO DOWN!!!
> By#AnonymousCaucasus#PaybackforSochiAnd Go out from our lands".

What is interesting, in an official published statement the Anonymous claimed that the attacks should not be associated with the current situation in Ukraine:

> "Nothing to do with Ukraine, or all current events in this country,
> And we are not waiting for anyone.
> Wait for us Russian Pigs we will learn you soon> expect us."

The Kremlin did not confirm the hacking and explained the situation was an ordinary technical failure. The Central Bank of Russia acknowledged in a published statement that it had fallen prey to a cyber-attack[1]. The experts suggested that the attacks might have been linked to Putin's decision to block the following websites which published information on protests in Russia against sending troops to Ukraine[2]: Grani.ru, Kasparov.ru, Ej.ru, Navalny.livejournal.com. Among them was the website of well-known chess player and opposition politician Gary Kasparov and Alexei Navalny, known at that time as a blogger-oppositionist revealing corruption scandals in Russia.

On 30th April 2014 Ukrainian Anonymous defaced several Polish websites. These were rather of low significance levels[3].The hackers explained as the purpose of their actions the desire to warn Poland and Poles against the Ukrainian Nazis, who had risen to power and were soon to take over in Poland as well[4].

> "We are Anonymous Ukraine.
> Ukraine has suffered a coup and Nazis came to power. Yes,
> Nazis came to power in a European country in the 21 century!
> Europe has suffered Nazi terror in the past. Now it may happen again.
> We want to warn people of Poland that their country is in great danger.
> Poland will be the next country to be torn apart by fascist plague like it happened in Ukraine.
> Storm troopers from Ukrainian neo-Nazi movement "Right sector" who are responsible for all the
> violence in Ukraine are planning to seize territories of Eastern Poland that they think belong to them.
> Poland has forgotten its history. So we've made defacements of some Polish websites. We want Poland
> to understand that Volin tragedy may happen again if Poland continues to support Ukrainian Nazis".

In 2014, the attention of Internet researchers in the context of the political situation in Ukraine was drawn to the activities of yet another group of hackers describing themselves as members of the Cyber Berkut. On 15 March 2014 the hackers attacked several NATO Internet websites, like the Cooperative Cyber Defense Centre of Excellence in Tallinn and NATO mailboxes. The CyberBerkut announced that NATO Cooperative Cyber Defence Centre of Excellence has been employed by the *"*Kiev junta" to carry out "propaganda among the Ukrainian population through the media and social networking..[..] and helps "blocking objective sources of information and concealing criminal activities of those calling themselves the 'legitimate authority". Posts questioning NATO's ability to secure Ukraine's interests and protect Europeans have appeared on websites. As can be inferred from the messages, the attacks were aimed at expressing opposition to NATO's presence on Ukrainian territory[1].

A detailed analysis of the actions of Cyber Berkut hacktivists targeting NATO highlights several important points. The methods used by the hackers were primitive in terms of technical sophistication. All attacks consisted of paralysing access to servers (DDoS attacks)[2]. The question was raised about the origin of the Cyber Berkut hacktivists who call themselves Ukrainian hackers. Many experts suggested that they were from Russia. All posted information on the hacked sites was in Russian. The political motivation of the hackers also points to the Russians. Speaking out against Western interference in Ukraine's internal affairs, calling Maidan activists supporters of NATO may indicate a clearly pro-Russian orientation of the hacktivists. What is more, DDoS type operations have so far been typical patterns of behavior of the Russians in information warfare they carried out on the Internet. In 2007 the same attack was launched against Estonia, in 2008 against Georgia and in 2009 against Kyrgyzstan. It might be supposed that also this time it was the Russians who provoked attacks on the NATO Internet websites.

[1] http://cbr.ru/press/pr.aspx?file=14032014_14593303_03.htm [access: 2014]

[2] http://rkn.gov.ru/news/rsoc/news24447.htm [access: 2014]

[3] Author's note: The list of the attacked websites: -festiwal.cerkiew.pl; cegielka.cerkiew.pl; bacieczki.cerkiew.pl; bractwocim.cerkiew.pl; bialowieza.cerkiew.pl; bilgoraj.cerkiew.pl; cieplice.cerkiew.pl; dojlidy.cerkiew.pl; ckp.bialystok.pl; zielonirp.org.pl; playablog.pl; bonusmedicus.pl; www.gis.gov.pl; zwingik.szczecin.uw.gov.pl; www.gregorgonsior.com; alicjasaar.com; www.herzlichwillkommen.pl; burninglion.com; modapolka.com; djcrab.com; bartoszlipowski.com; annabinczyk.com; www.hakobo.art.pl; maua.pl; www.wunderteam.pl; www.hakobo.pl; bonusmedicus.pl; www.dommusic.pl.

[4] "…Nazis came to power in Ukraine and Poland is in danger because it is next."

4. Anonymous and cyber war in 2022

Cyber conflicts tend to take place in the shadows, without attracting the attention of global public opinion. In the case of Russia's invasion of Ukraine in 2022, this situation has changed. The hacktivist collective Anonymous has made the public declaration of war. Late on Thursday, hackers tweeted from an Anonymous-affiliated account, @YourAnonOne, that they had Vladimir Putin's regime in their sights.

> "The Anonymous collective is officially in cyber war against the Russian government. #Anonymous #Ukraine
> — Anonymous (@YourAnonOne) February 24, 2022"

From 24 February to 19 March 2022. Anonymous launched 8 major attacks against Russia. This chapter will mention a selection of them. On the third day of the war, Anonymous released a video in which they promised to respond to Russia's aggression against Ukraine with cyber warfare. They threatened to devastate the e-wallets of Russian bank card holders if they did not turn up to anti-war protests. Their funds were to be transferred to the Ukrainian armed forces. As predicted, this was just a bluff, which nevertheless caused panic among Russians. Hundreds of thousands of residents of major cities withdrew their assets from banks. These actions hit the Russian banking system. Since then, hacktivists have claimed responsibility for several cyber incidents, including distributed denial-of-service attacks. These allegedly led to the downing of government websites and the Russia Today news service which briefly outlined the bomb attacks on Ukrainian cities and other crimes committed by the Russians in Ukraine. Ukrainian music and national symbols were also featured during the incident.

> "JUST IN: #Russian state TV channels have been hacked by #Anonymous to broadcast the truth about what happens in #Ukraine. #OpRussia #OpKremlin #FckPutin #StandWithUkriane, February 26, 2022"

On 28 February, Anonymous attacked petrol stations in Russia. The hack resulted in the slogan "Glory to Ukraine, heroes glory" appearing on the screens of the docking stations. On 10 March, Anonymous hacked into the database of Roskomnadzor, the Federal Supervisory Service in the Sphere of Communications, Information Technologies and Mass Communications. This institution is responsible for blocking electronic resources and social networks in Russia. The activists placed 364,000 files in free access. On 11 March, they distributed 20 terabytes of files from the servers of the German subsidiary of state corporation Rosneft. Its chairman of the board was former chancellor Gerhard Schröder. Hackers also attacked Putin himself, changing the location of his yacht in the international AIS identification system. The status of the yacht suggested that it had crashed off the famous Snake Island.

Anonymous also demonstrated other aspects of hacktivism at the time. Their activities were not limited to providing information about hacking websites and other databases or making various data public. The collective began to highlight various other dimensions of the fight against the Russian invaders in their communications. On their Twitter account, hacktivists from Anonymous Operations posted the famous photo of strollers left at the Przemyśl train station by Polish mothers for Ukrainian mothers fleeing the war with their children. The extremely emotional message of the photo was widely reported around the world. Many international news outlets shared the photograph, drawing attention to Ukraine's problems.

To make it easier for the people of Russia to access real information, Anonymous hacked printers on 22 March. Across the country, thousands of devices began printing a message about Putin, on whose orders innocent people are being murdered. There were also incentives for other internet users to post online opinions against Russian restaurants, hotels and state institutions.

> "We hacked printers all across Russia and printed this PDF explaining that Putin/Kremlin/Russian media is lying and then we instructed how to install Tor and get around their censorship to access real media"

On March 23, Anonymous targeted companies who still did business in Russia. The collective successfully launched denial of service DDoS attacks on Auchan, Leroy Merlin, and Decathlon websites.

> "We are once again call on companies that continue operate in Russia: Immediately stop your activity in Russia if you feel sorry for the innocent people who are being massacred violently in Ukraine. Your time is running out. We do not forgive. We do not forget. #Anonymous #OpRussia"

Pro-Russian hacker groups have also been very active online during the 2022 Russian-Ukrainian war. One of these is the Killnet group known for its DDoS campaigns against countries supporting Ukraine, especially NATO countries. DDoS is a rudimentary type of cyber attack that can send thousands of connection requests and packets to a target server or website per minute, slowing or even stopping vulnerable systems. They formed sub-groups under the name 'Cyber Special Forces of the Russian Federation'. The group also established another hacking group called LEGION in April 2022 and continued DDoS attacks from there.

On 21 May 2022 the @YourAnonOne account announced a Twitter war with this organization.

> "The #Anonymous collective is officially in cyber war against the pro-Russian hacker group #Killnet."

The collective's initiative, which drew public attention worldwide, was also hacking the Yandex Taxi app which caused a massive traffic jam in Moscow on September 1st.

> "#Moscow had a stressful day yesterday. The largest taxi service in Russia 'Yandex Taxi' was hacked by the #Anonymous collective. A traffic jam took place in the center of Moscow when dozens of taxi were sent by the hackers to the address on Kutuzovsky Prospekt. #OpRussia"

Jeremiah Fowler listed many of the highly destructive methods and techniques used by Anonymous 2022 (Fowler, 2022):

- ✓ Hacking Printers
- ✓ Using Conti Ransomware Code
- ✓ Hijacking Russian Servers
- ✓ Hacking The News
- ✓ Attacking Exposed Data
- ✓ Targeting companies who still do business in Russia
- ✓ RoboDial, SMS, and Email Spam
- ✓ Hacks on key Russian holidays and important date Hacks

Anonymous used some distinctive hacking methods and techniques, but also some that can be attributed to social influence, like: hacking into databases, targeting companies that continue to do business in Russia, blocking websites, training new recruits, hijacking media and streaming services, directly reaching out to Russians and promotion of pro-Ukrainian social attitudes. This last aspect of the collective's activities seems particularly interesting from a sociological perspective in revealing the different faces of hacktivism.

5. Conclussions

Anonymous collective has created different faces of hacktivism in the times of comparison. The actions taken in 2014 did not attract so much public attention. The focus of analysts was mainly on types of techniques carried out by the hackers. Many of them concluded that the attacks cannot have been carried out by professionals. The effects of the collective's activities have been assessed differently. It was disputed whether the attacks could indeed be described as hacktivist or whether they should be assessed in terms of cyber crimes. The ambivalence stemmed from a certain ambiguity related to the online activity of pro-Ukrainian and pro-Russian hacker groups, which did not explicitly declare their ideological affiliation. It can be concluded that in 2014 we observed the beginning of a disinformation war on the Internet. In particular, the digital counteroffensive of hackers also using the name Anonymous publishing controversial slogans with a pro-Russian tinge influenced public attitudes towards this activity. Moreover, news of cyber attacks by hacking groups tagged as Anonymous did not appear in mainstream media headlines. Niche websites and local media covered these topics. However, the strength of the hacktivists' social influence or their effectiveness in the context of the ongoing conflict in Ukraine was not considered at the time.

In 2022, the methods Anonymous have used against Russia have been more disruptive. The effectiveness of the cyber attacks were also higher. The collective has changed the status quo of hacking by supporting and promoting the crowdsourced model of cyberwar. The techniques of cyber attacks were more sophisticated in many cases. What is most important for changing the social perception of hacktivism was the efforts of evoking emotional engagement in the war of people around the world by sharing with them dramatic pictures of war. During this time, Anonymous drew clear lines between pro-Ukrainian and pro-Russian activity. The ideological identity of the hackers did not elicit cognitive ambivalence. Experts estimate that more than 100 pro-Ukrainian hacking groups and more than 70 pro-Russian groups have become active during the ongoing Russian-Ukrainian war. However, not all of them have gained as much publicity as Anonymous, due to the different operating strategies and goals of the individual collectives. Anonymous has played a major role in shaping pro-Ukrainian public attitudes in various countries, especially among younger generations of internet users. Anonymous attacks have also revealed Russia's cybersecurity defenses weak points. Many Russian strategic assets were hijacked by hackers. Veiling Russia's cybersecurity practices has also indicated the process of global declining of the superpower image. Information collected from the hijacked database breaches has revealed criminal activity of the Russian government and elites.

The faces of hacktivism by the Anonymous collective in the context of Russian war actions against Ukraine in 2014 and 2022 are similar in many respects. The transformation is seen in something that could be called the axionormative load released during an evaluation based on humanistic values. Negatively evaluated hacker is perceived as a cyberculture hero when launching the values saturated tweet which touches the public opinion. Anonymous hacktivists seem to have been positively perceived in 2022 as fighting on the right side. They also tend to have highly impacted communication, cultural and symbolic aspects of social media functioning. It has been observed in the changes of power relations on the Internet. Their social engineering related to a crowdfunding model of cyberwar was less visible but more subtle and focused on symbolic transfer. Assigning meanings, constructing and disseminating interpretation schemes, coding communication, producing new semiotics are inseparable elements of the cyberwar. Anonymous collective seem to become an important social actor on the global scene of powers in that respect in 2022. The global social narrative for assessing hacktivism has reverted in this context to an 'end justifies the means' type of assessment (Gondek et. al., 2023; Fowler,2022; Chojnacki, 2005). The analysis of aspects of hacktivism draws attention in particular to the aspect of the production of information, knowledge and the social construction of interpretative schemes in the networked laboratory of power (Raudeliūnienė et. al., 2020; Wiltgen, 2022; Nussbaum, 2008). Internet warfare also encompasses the issue of image creation of leaders, soldiers, hackers and the information, propaganda, disinformation messages themselves. The *power of minds* is linked to the performativity of new technologies, as the normative, narrative and cultural conditions for the reproduction of social order are embedded in the technical context of the development of contemporary societies.

References

Aleksejeva, V. et. al. 2021. Analysis of disparities in the use of information and communication technology (ICT) in the EU countries. *Entrepreneurship and Sustainability Issues*, 9(2), 332- 345. http://doi.org/10.9770/jesi.2021.9.2(22)

Banks J. 2017. Radical criminology and the techno–security–capitalist complex. In: Steinmetz K, Nobles MR (eds) Technocrime and Criminological Theory. New York: Routledge, 102-115.

Beck C. 2016. Web of resistance: Deleuzian digital space and hacktivism. *Journal for Cultural Research*, 20(4): 334–349.

Bedianashvili, G. 2021. Globalization and modern challenges of economic uncertainty. Conference materials: Strategies, *Models and Technologies of Economic Systems Management (SMTESM-2021)*, Vol. 7, 45-48.

Betlej A. 2014. Hacktivists and War on Internet, [in:] S. Partycki (edited by.), Perspektywy rozwoju społeczeństwa sieciowego w Europie Środkowej I Wschodniej, Wydawnictwo KUL, Lublin.

Betlej A. 2019. Społeczeństwo sieciowe- potencjały zmian i ambiwalentne efekty. Wydawnictwo KUL, Lublin.

Betlej A. 2022. Power relations in the network society. A sociological approach. *Studia Gilsoniana*, 11/3, 425-443.

Bodford JE, Kwan VS. 2018. A game theoretical approach to hacktivism: is attack likelihood a product of risks and payoffs? *Cyberpsychology, Behavior, and Social Networking*, 21(2), 73-77.

Coleman, G. 2013. Anonymous in context: The politics and power behind the mask. Available at: https://www.cigionline.org/publications/anonymous-context-politics-and-power-behind-mask/

Coleman G. 2014. Hacker, Hoaxer, Whistleblower, Spy: The Many Faces of Anonymous. London: Verso Books.

Chojnacki, W. 2005. Socjologiczna analiza profesjonalizacji wybranych armii NATO i Wojska Polskiego. Wyd. Akademii Obrony Narodowej, Warszawa, p. 109.

Chojnacki, W. 2021. Elity polityczne w perspektywie logosu i etosu. Transformacje, 1(108), 116-137.

Chojnacki, W. 2023. Wielopoziomowe sieci struktur nieformalnych potencjałem ukrytym między zadaniami, działaniami i wynikami. *Transformacje*, 1 (116) 2023, 23-47.

Fowler J. Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks Against the Russian Government, available: Is Anonymous Rewriting the Rules of Cyberwarfare? Timeline of Their Attacks Against the Russian Government (websiteplanet.com) [access 12 May 2023]

Fuchs C. 2014. Anonymous: hacktivism and contemporary politics. In: Trottier D, Fuchs C (Trottier, D. and Fuchs, Christian (ed.) Social media, politics and the state: protests, revolutions, riots, crime and policing in the age of Facebook, Twitter and YouTube New York Routledge. pp. 88-106.

Gondek, M. J. 2017. *T*echniki doskonalenia krytycznego myślenia na przykładzie retorycznego ćwiczenia anaskeuē i kataskeuē. *Forum Artis Rhetoricae*, 4, 23–44.

Gondek, M. J., 2018. A Teleological Interpretation of the Applicability of Rhetoric in the Peripatetic Tradition. *Studia Gilsonian*, 7(2), (April- June), 181-199.

Gondek, M. J., Nowak, P. 2023. Emotional Rationality as an Indicator of Rhetoric Discourse in Polish Agricultural Texts, [in:] Routledge Handbook of Descriptive Rhetorical Studies and World Languages. Edited By Weixiao Wei, James Schnell, 403-420.

Gondek, M. J. 2022. On Foresight Functions of Rhetorical Invention in Acts of Counselling. *Roczniki Filozoficzne / Annales de Philosophie / Annals of Philosophy*, 70(3), 165-178.

Gondek, M. J. 2020. Partes Integrales jako podstawa tłumaczenia cnoty roztropności w tradycji perypatetyckiej. Zeszyty Naukowe Katolickiego Uniwersytetu Lubelskiego Jana Pawła II, 59(1), 41-57.

Goode, L. 2015. Anonymous and the Political Ethos of Hacktivism, *Popular Communication*, 13(1), 74-86, https://doi.org/10.1080/15405702.2014.978000

Holt TJ, Freilich JD, Chermak SM. 2017. Exploring the subculture of ideologically motivated cyber-attackers. *Journal of Contemporary Criminal Justice*, 33(3), 212-233.

Ireland, L. 2022. We are all (not) Anonymous: Individual- and country-level correlates of support for and opposition to hacktivism. New Media & Society, 0(0). https://doi.org/10.1177/14614448221122252

Katina, J., Plėta, T., Petkevičius, R., Lelešienė, L. 2023. Industrial Control Systems (ICS) cyber prediction model. *Insights into Regional Development,* 5(1), 86-96. https://doi.org/10.9770/IRD.2023.5.1(6)

Mitnick K. D., Simon W. L. 2006. Sztuka infiltracji, czyli jak włamywać się do sieci komputerowych. Biblia hakerów. Wydawnictwo Albatros, Warszawa.

Nussbaum, M. 2008. Upheavals of Thought: The intelligence of Emotions. Cambridge.

Raudeliūnienė, J., Tvaronavičienė, M., Blažytė, M. 2020. Knowledge Management Practice in General Education Schools as a Tool for Sustainable Development. *Sustainability*, *12,* 4034. https://doi.org/10.3390/su12104034

Sorell T. 2015. Human Rights and Hacktivism: The Cases of Wikileaks and Anonymous. *Journal of Human Rights Practice*, 7(3), 391-410, https://doi.org/10.1093/jhuman/huv012

Wiltgen, F. 2021. Challenge of balancing analog human (real life) with digital human (artificial life). *Transformacje*, 3(110), 17-33.

Alina BETLEJ is an assistant professor at the Institute of Sociological Sciences of the John Paul II Catholic University of Lublin (Poland). Her research interests: cybersociology, economic sociology, digital exclusion, sustainable development, ICT for ageing society, social innovations, cybersecurity, social transformations.
ORCID ID: https://orcid.org/0000-0002-2729-6564