Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine

Denys Svyrydenko

Doctor of Philosophical Sciences, Professor,
Guangdong University of Petrochemical Technology (Maoming, China)
E-mail: denis_sviridenko@ukr.net
https://orcid.org/0000-0001-6126-1747

Wiktor Możgin

Jagiellonian University in Kraków (Kraków, Poland)
E-mail: wiktor.mozgin@gmail.com
https://orcid.org/0000-0001-5744-8103

Svyrydenko, Denys, and Wiktor Możgin (2022) Hacktivism of the Anonymous Group as a Fighting Tool in the Context of Russia's War against Ukraine. *Future Human Image,* Volume 17, 39-46. https://doi.org/10.29202/fhi/17/6

The Russian invasion of the territory of the Ukrainian state in February 2022 disturbed the existing order in the world. The hybrid nature of this war resulted in the involvement of hacktivists from the Anonymous group. Therefore, the aim of this article is to analyze the legitimacy and legality of the hacking activities undertaken by members of the Anonymous group against the Russian state. Assuming that hacking activities are illegal in the light of the law, the author proves that during the war, this type of activity in cyberspace becomes justified and is one of the tools to fight the aggressor. At the same time, this fits in with the modern concept of hybrid wars because today's conflicts do not have the pure form of conventional actions, but are a mix of various fighting methods.

Keywords: hacktivism, war, Anonymous, Russian military aggression, cyberspace, law.

Received: 12 March 2022 / Accepted: 22 April 2022 / Published: 29 May 2022

Introduction

In the modern world, warfare is not limited to conventional battlefield operations. The economic sphere, and above all – the information sphere, is also becoming such a field. War takes the form of a hybrid rivalry between two sides (the term "side" is legitimate, as they can be both individual states as well as blocks of states). We can certainly speak of the phenomenon of hybridization since 2006, when the term was first used by Frank Hoffman in relation to the armed conflict between Israel and Hezbollah (Hoffman, 2007: 23-24). The hybrid character was synonymous with a new quality of armed conflict in the post-Cold War period. The attention was paid primarily to the asymmetry of conflicts, which has become a regularity implemented in the discourse of contemporary conflicts (Arrequin-Toft, 2001: 94-95). It is important that armed conflicts, being a part of social life, transform as it changes. Today, changes at the level of the international system, identified with the processes of globalization and the virtualization of social life, seem to be of particular importance for their evolution.

The departure from the traditional formula of conflicts, characteristic of the Westphalian system, meant that, primarily in Europe, at the turn of the 20th and 21st centuries, a new type of fighting was developed, taking into account the use of various methods. This has been referred to as a new, unconventional war, postmodern conflict, or low-intensity conflict (Kaldor, 1999: 2-3). An important feature of these conflicts is the extraordinary complexity and blurring of the differences between hostilities and justifying them from the point of view of the rule of law and general accepted rules for players on the international arena.

In the face of such a complicated phenomenon as modern war, it is necessary to analyze the activities in the virtual sphere, which is certainly one of the basic pillars of unconventional combat. Therefore, the author of this article pays special attention to the involvement of the Anonymous group in the war between Russia and Ukraine, which in fact, began in 2014 after the so-called the Revolution of Dignity. At that time, the Crimean Peninsula was annexed, which was considered by the Russians as the Cape so-called "Ruthenian mir" in Ukraine, and a military invasion of some territories in the Donetsk and Lugansk regions. As a result, Russia took control of the Crimean peninsula and created self-proclaimed separatist republics within the Donetsk and Luhansk oblasts – the so-called LNR and DNR. Thus, the virtualization of war is another step on the way to emphasize the hybrid nature of contemporary conflicts. The author hypothesizes that the actions of the Anonymous group in the context of the war in Ukraine are an effective combat tool implemented into the information sphere of this rivalry. It is therefore justified to analyze the issue of the legality of the actions of the Anonymous group, involved in the war between Russia and Ukraine. So, is the involvement of a team of hackers in hostilities on one side in line with the norms of the law, and what effect does such activity have in the context of hostilities? The purpose of this article is to analyze the legitimacy and legality of hacking activities undertaken by members of the Anonymous group against the Russian state.

In order to verify the hypothesis and answer the above questions, the authors used a number of research methods appropriate for social sciences. Therefore, the following research methods were used: content analysis, comparative method, historical method, decision-making method and the method of individual cases. Due to the fact that the work concerns the virtual sphere, the netscouting method, which is one of the qualitative methods based on the analysis of content on the Internet, was also used. It was primarily site-centric, i.e., the subject of the research was a website with specific content and message.

However, before analyzing the specific activities of the Anonymous group that constitute the narrative content of this article, it is necessary to consider the phenomenon of hacktivism as a space for hackers around the world.

Virtualization of social disobedience – the phenomenon of hacktivism

In the late 1990s, access to the Internet was so widespread that it allowed mass participation in online political demonstrations, which became one of the earliest forms of electronic protest. Information about this type of activity then penetrated the web, implying offline activity – that is, direct social activities on a mass scale. At that time, dissatisfaction on the Internet was caused primarily by restrictions on the freedom of expression, monopolization of media sources, manipulation of information, or lobbying (Lakomy, 2013: 182-183). In this context, the concept of electronic civil disobedience has developed, which can otherwise be presented as a form of non-violent electronic protest against institutions or persons undertaking unethical or illegal activities (Wray, 1999: 108). It is worth noting that in this context, the destruction of other people's resources in a direct, physical manner is not allowed, because the protest actions are to be carried out in such a way that the attacked suffer from a detriment consisting in impeding the normal functioning or completely preventing it.

Hacktivism is, therefore, a phenomenon that usually consists in a symbiosis of anonymous political and technological activity in order to manifest opposition to actions in the sphere of broadly understood politics (Lakomy, 2013: 183). Hacktivism is the use of computers and computer networks as a means of protest and manifestation of specific political demands. In this narrative convention, Alexander Samuel from Harvard University argues that hacktivism is a peaceful, non-military, use of illegal or legally ambiguous digital tools to achieve specific political goals (Lakomy, 2015: 124-125). Nevertheless, it is worth noting that the term hacktivism was used already in 1995 by Jason Sack, but it came into wider use a year later due to the actions of the hacker group Cult of the Dead Cow. Thus, hacktivism came to mean being active on the Internet by using hacking methods to achieve political or social goals. The targets of attacks by hacktivists are usually e-mail accounts, websites related to the opposed worldview or social group. Hacktivists often use an attack method called DoS (Denial of Service), the purpose of which is to block a network service or computer system by overloading servers or an application that handles specific data. Attacks of this type are based on the assumption that each server can handle a certain number of network queries at a time. When the hacktivist sends a very large amount of data in a short time, the server will not be able to function properly, and therefore the service will be denied, and the website will be unavailable. A variant of the DoS attack, which is also often used by groups of hackers, is DDoS (Distributed Denial of Service). A DDoS attack is carried out simultaneously from many computers in order to seize all free resources. To carry out an attack, zombie computers are often used, i.e., computers over which control has been taken (often without the knowledge of their owners) with the help of special software. On the perpetrator's signal, infected computers start attacking the victim's computer system by sending a large number of inquiries that the victim's system is unable to handle. This method was used by hackers attacking government portals in Estonia in 2007. What's more, there is also a method called DRDoS (Distributed Reflected Denial of Service), which is a variant of the DoS attack. This attack generates special SYN packets that flood the victim with large numbers of packets from multiple hosts, making it very difficult to detect the actual source of the attack (Worona, 2020: 332-333).

An important element of the hacktivist movement on which their activity is based is specific ethics relating to the idea of freedom of speech. Its canon is the unfettered right to information, even when it is stored on someone else's computers. Therefore, it is not ethically reprehensible for hacktivists to enter and "crack" a foreign computer, as well as download programs or data. Hence, accepting data from computers of governmental or corporate institutions in order to make them public is a moral duty of hacktivists. Moreover, the hacktivists established a specific ethos of behavior and radical, rebel spirit, a sense of fighting in a just cause and fulfilling in it (Lakomy, 2013: 185). However, it should be clearly stated that, according to the authors, hacktivism is not one of the forms of cyberterrorism. There are opinions that the actions of hacktivists can be classified as one of the three forms of cyberterrorism; they refer primarily to the work of D. E. Denning, *Activism, Hactivism and Cyberterrorism: The Interest as a Tool for Influencing Foreign Policy*. Nevertheless, according to Gen. Roman Polko, cyberterrorism is a new direction of destructive activity, which consists in using the information as a tool to fight (Polko, 2001: 9-11). There is no doubt, however, that the perception of hacktivists as cyberterrorists depends primarily on the point of view because, in this way, they are perceived by the governments of states and corporations against which the actions of hacktivist groups are directed.

An interesting fact is that hacktivists do not shy away from breaking into information systems in search of classified documents or creating "political" viruses. An example of this type of action was the 2001 *Injustice* program, the purpose of which was to disclose information about the killing of a 12-year-old Palestinian in the Gaza Strip (Leyden, 2001, et al.). One of the most important elements of hacktivism as a form of networked civil democracy are the so-called hacktivist collectives. We can include them, among others: the already mentioned Cult of the Dead Cow, Electronic Disturbance Theater, Chaos Computer Club, LulzSec and the most famous movement Anonymous. Anonymous's activity is known today primarily for its involvement in Russia's war against Ukraine. It is therefore worth considering how the actions of this group of hacktivists are perceived by international opinion and to what extent they are consistent with generally accepted norms of the rule of law.

Anonymous as one of the pillars of hybrid warfare

Following the spirit of the narrative convention adopted in this article, the group of hacktivists Anonymous can certainly be described as contemporary "fighters" opposing the violation of civil rights, restriction of freedom and, above all, the unfair and irrational war that Russia is waging against Ukraine.

The actions of the Anonymous group became widely known primarily as a result of their opposition to the adoption of the ACTA Act. In 2012, hacker attacks related to this act were carried out on government and corporate websites, including in countries such as the USA, Poland, Ireland, Slovenia, and France. Hacktivists associated with the Anonymous movement disclosed the e-mail addresses, logins, and passwords of some politicians, including many politicians in Poland, who supported the adoption of the law. Various types of information about the private life of these politicians were also disclosed, which was echoed in the media, being a "sensation" for many and opening eyes to the real state of political life in the country and abroad (Olson, 2013: 24-26). The activities of the Anonymous group were directed not only at specific politicians, but at entire information systems, moreover, often including government systems. The involvement of hacktivists from the Anonymous group achieved the

intended goal and drew public attention to the content of the ACTA Act, which significantly violated the freedom of access to information. As a result, the original draft of this law was rejected by the European Parliament. At that time, the demands of the protesting community were taken into account and a certain parity in access to information, corresponding to both parties, was maintained (Kewlani, 2021: 87-88).

The United States has also had problems with Anonymous due to its opposition to ACTA, as CIA sites have been attacked. In addition, a coded teleconference between the FBI and Scotland Yard regarding hacker attacks was made public (Kewlani, 2021: 90).

It is worth noting that hacktivism, including the Anonymous group's activities, is not a uniform form of activity in cyberspace. François Paget distinguished three groups of activists in cyberspace. Anonymous belongs to the group whose functioning includes breaking into websites, obtaining confidential information and blocking certain network services. Often this data is of significant value in the context of the ongoing public debate, be it at the regional, national and international levels (Paget, 2012: 14-16). It was François Paget who called the Anonymous group "cyber warriors." They act primarily to defend specific values or political attitudes specific to a given country. In this perspective, the activities of the "cyberarmy," which are currently constituted by the hacktivists from the Anonymous group, often have an international context or manifest themselves in the course of armed conflicts. Compared to conventional hacktivism, are not only its motivations different, but also the methods it uses (Paget, 2012: 18-21).

Hacktivism and the involvement of various hacker groups in political activities, and now also in the military, resulted in the need to introduce specific regulations, aimed primarily at protecting the individual in the virtual world. The basic instrument of such protection is the law, especially the norms regulating cyberspace. Such documents are created both in NATO, which recognized cyberspace as the fourth space for military activity of states (after land, air, and sea forces), as well as in other international institutions and individual states (Wrona, 2020: 45-46). The Council of Europe, which developed the Convention on Cybercrime, has the greatest influence on the harmonization of cybercrime regulations. Of course, one should not forget about numerous other legal acts that regulate the functioning of various entities in cyberspace. In this context, it is important to strengthen the cooperation of international law enforcement agencies – Interpol, Europol, and the European Cybercrime Center. The convention's purpose is to ensure the protection of cyberspace users and network security (Tarnogorski, 2009: 78-80).

This convention categorizes cybercrime acts as follows:

Category I – offenses against the confidentiality, integrity and availability of IT and system data: illegal access to the IT system; illegal data capture; breach of data integrity; violation of system integrity; improper use of devices.

Category II: computer crime: computer forgery; computer fraud.

Category III – offenses due to the nature of the information contained: offenses related to child pornography.

Category IV – offenses related to the infringement of copyright and related rights (Council of Europe Convention on Cybercrime: 2015, et al.).

On February 24, 2022, Russia invaded Ukraine. This act was immediately condemned by all European and world countries. The strong opposition to Russia's aggression is most visible through the sanctions imposed on both Russian leaders and goods and services imported or exported from and to the Russian state. One of the most painful ones is certainly the exclusion

of some Russian banks from the SWIFT system, as well as the closure of airspace to Russian planes in the European Union. Of course, it should be remembered that Ukraine is bravely left under the fire of Russian troops, while the Russians themselves do not know about the real reasons and actions (due to propaganda in the Russian media), or they keep such appearances.

The situation in Ukraine could not but attract the attention of the Anonymous group, which, as mentioned in previous considerations, is a hacking group associating members from all over the world. In the context of Russia's war against Ukraine, Anonymous's actions were directed primarily against official parties and governmental institutions of the Russian state. As a result of their actions, the functioning of Roscosmos, the institution controlling the activities of Russian satellites in space, was paralyzed, among others.

Of course, the question remains whether Anonymous is an altruistic group? Or maybe more of a terrorist character? According to Maciej Góra, an expert from the Kosciuszko Institute, the answer is not entirely clear, because it is very difficult to identify and track who is actually hiding under the characteristic and recognizable all over the world mask Anonymous. Some of the people operating under this banner may have an interest other than pro-social. However, most of their actions over the years were ideologically driven and related to the fight for freedom of speech and reacting to pathologies committed by large corporations or governments (Wysocka, 2022).

By engaging in Ukraine and essentially the entire Western world, the Anonymous Group even declares a state of war in relation to the Russian state. It is also very significant that the attack is not directed at the Russian society, which is actually calmed down by the members of the group, which could be found out via messages posted by Anonymous on social media, especially on Twitter: "*We want Russian citizens realized that we know very well how difficult it is to oppose a dictator for fear of reprisals*" (Polish Press Agency, 2022). On the same website, they also sent a message to Vladimir Putin: "*The Soviet Union fell many years ago, but the world has not forgotten the brutality of this regime. People from all over the world will resist you at every turn. This is not a war you will win*" (Polish Press Agency, 2022). On the day of Russia's invasion of Ukraine, Anonymous attacked the Russian media service RT by using DDoS. Moreover, government services were attacked, and the most severe ones were directed at the Ministry of Defence of the Russian Federation and Gazprom, the Russian resource giant.

Public television was also under pressure from the hackers' group, which as a result of these attacks on February 26, on the third day of Russia's attack on Ukraine, broadcast Ukrainian television broadcasts. The public opinion of Russia was thus informed about the actual actions of the Russian army on the territory of Ukraine. The background of the message was the national music of Ukraine and its national symbols. Russian military communications, which were completely unprepared for this type of action, were also intercepted. Anonymous gave the frequency as well as short recordings of Russian soldiers from the time of the hostilities.

Anonymous's actions also affected Belarus, which is the Kremlin's ally in this war. Access to the website of the Belarusian Ministry of Communications and Informatization has been blocked. It is worth mentioning that before this attack, the President of Belarus, Alexander Lukashenko, was informed about the plans and that the Anonymous attack would not take place when Russia resigned from aid.

The attack on the Russian media mentioned in the previous considerations was repeated on February 28, but this time it was preceded by an appeal on the website of the Russian TASS agency, in which it was announced that: "*Vladimir Putin forces you to lie and poses a threat to*

the whole world. This is not the Russian war, let's stop it!" (Piechocki & Gorzkowska, 2022). A similar cyber-attack affected the RBK TV station and the online edition of the newspaper "Izvestia." Nevertheless, the hackers in the group failed to take control of all parts of the affected system. The fact is that the group admitted to blocking the following sites: sovam.com, com2com.ru, ptt.ru, mail.ru, goverement.ru, kremlin.ru, and rt.com.

Russia's attack on Ukraine is the greatest tragedy since World War II. It is a war that came as a surprise to everyone – security experts as well as every single inhabitant of the Western democratic world. Nevertheless, the Ukrainian army is effectively resisting the Russian invaders, and the Anonymous group, as a cyber-military supporting Ukraine in this fight, is, as shown by the above considerations, an effective means of combat.

Conclusions

The involvement of hacktivists from the Anonymous group in Russia's war against Ukraine fulfilled two extremely important tasks. First, by breaking the security systems of Russian news channels, it was possible to provide information about the actual activities of the Russian army in Ukraine. This was in contradiction to the official propaganda narrative directed by mass media channels in Russia to ordinary citizens. Secondly, the actions of the Anonymous group favoured, on the one hand, the blocking of some strategically important internet domains and the websites of Russian government institutions.

This is an extraordinary feat because, as mentioned in the above considerations, Anonymous declared cyber war against the Russian state. Of course, this met with an immediate reaction from the Russian hacker community, which declared a fight against Anonymous. In this way, it can be concluded that the war is not only on the battlefield, but has also been transferred online, which is one of the hallmarks of modern hybrid conflicts. This is especially important in the context of information warfare, or a war of facts between the two sides of the conflict. The dissemination of fake news is becoming an increasingly effective tool. Today, an image of war is being created, which is presented not only to the internal but also to external recipients, who are various types of entities on the international arena. In this regard, the action taken by one of the parties is subject to evaluation by others, which is why an extremely skilful information structure is created, which is credible, but not always based on actual facts (Molina et al., 2019: 182-183).

It is also worth emphasizing that the widely discussed issue of the legality of Anonymous's actions in the context of this war boils down to an expert debate on this topic, because, in fact, each hacktivist attack that takes place is an unprecedented help in the fight against Russian aggression. Despite the existence of many legal regulations, especially those concluded between individual countries, the actions of the Anonymous group are an effective weapon of war. The authors of this article, referring to the Machiavellian term that the end justifies the means, believe that the Anonymous group acts in good faith and its actions, despite being treated as hackers, constitute a legitimate means of fighting.

Therefore, the hypothesis put forward by the author that the actions of the Anonymous group in the context of the war in Ukraine are an effective combat tool implemented in the information sphere of this rivalry has been fully confirmed.

🕮 References

Arrequin-Toft, Ivan (2001) How the Weak Win Wars? *International Security*. Vol. 26 (1), 93-102.

Council of Europe Convention on Cybercrime (2015) Available online: http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20150000728.

Hoffman, Frank (2007) *Conflict in the 21st Century. The Rise of the Hybrid Wars*. Arlington.

Kaldor, Mary (1999) *New and Old Wars. Organized Violence in a Global Era*. Cambridge.

Kewlani, Lena (2021) *Anonymous Method*. Morrisville.

Lakomy, Miroslaw (2013) *Democracy 2.0. Political Interaction in New Media*. Cracow.

Lakomy, Miron (2015) *Cyberspace as a New Dimension of Rivalry and Cooperation Between States*. Katowice.

Leyden, John (2001) *Pro-Palestinian Virus Raises Its Head*. The Register. Available online: https://www.theregister.com/2001/03/20/propalestinian_virus_raises_its_head/

Molina, Maria, Sundar, Shyam S., Le, Thai and Lee Dongwon (2019) "Fake News" Is Not Simply False Information: A Concept Explication and Taxonomy of Online Content. *American Behavioral Scientist*. Vol. 65, Issue 2: 180-212. https://doi.org/10.1177/0002764219878224

Olson, Parmy (2013) *We Are Anonymous. Inside the Hacker World of LulzSec, Anonymous, and the Global Cyber Insurgency*. New York.

Paget, François (2012) *Hacktivism: Cyberspace Has Become the New Medium for Political Voices*. McAfee Labs White Paper. Available online: https://www.mcafee.com/us/resources/white/papers/wp-hacktivism.pdf

Piechocki, Artur, and Katarzyna Gorzkowska (2022) *Anonymous Attacks Russia – Hackers on the Cyber War Front.* Available online: https://www.prawo.pl/prawo/wojna-cybernetyczna-z-rosja-aspekty-prawne,513867.html

Polish Press Agency (2022) Available online: https://www.pap.pl/aktualnosci/news%2C1105172%2Cukrainskie-media-grupa-anonymous-zhakowala-rosyjskie-panstwowe-kanaly

Polko, Roman (2001) *Terrorism as a Threat to the Civilization of the 21st Century*. Warsaw.

Tarnogorski, Roman (2009) Convention on Cybercrime – an International Response to Information Age Crime. In: *ICT Security of the State of Poland*. Edited by Marek Madej and Marcin Terlikowski. Warsaw, 72-96.

Wray, Stefan (1999) On Electronic Civil Disobedience. *Peace Review*, Vol. 11, 107-111. https://doi.org/10.1080/10402659908426237

Worona, Joanna (2020) *Cyberspace and international law*. Warsaw.

Wysocka, Kinga (2022) *Online War. Anonymous Hackers on the Side of Ukraine. They Just Attacked Russia's Spy Satellites*. Available online: https://www.euractiv.pl/section/gospodarka/news/ukraina-rosja-wojna-anonymous-atak-hakerzy-komputery-sankcje-atak-agresja-polska/