УДК 316.422.44 URL: https://ptsj.bmstu.ru/catalog/hum/socio/1103.html

ХАКТИВИЗМ: ОТ АБСОЛЮТНОЙ ГЛАСНОСТИ ДО ЦИФРОВОЙ УГРОЗЫ

А.И. Близнякова bai22yu014@student.bmstu.ru

МГТУ им. Н.Э. Баумана, Москва, Российская Федерация

В статье представлено исследование, посвященное популярному социально-цифровому явлению, известному как хактивизм. Целью данной статьи является изучение его трансформации из цифрового хулиганства в сферу компетенции правоохранительных органов. Для создания этой работы мы использовали материалы хорошо зарекомендовавших себя исследователей в области кибербезопасности, а также онлайн-публикации из авторитетных источников, которые характеризуют понятие «хактивизм», раскрывая его основные цели, методы, используемые при организации атак, и предоставляя комментарии об эволюции этого явления — одном из самых распространенных, а также основные угрозы последних лет. Что касается методов, использованных в ходе этого исследования, были использованы методы сбора данных, критического анализа и обобщения научной и профессиональной литературы из общедоступных источников. Исторический и диахронический подход был использован для изучения эволюции хактивизма под влиянием социально-экономических и политических факторов. Метод тематических исследований позволил проанализировать конкретные примеры активности хактивистов и связанных с ними средств и техник. Для обобщения и интерпретации собранных данных, а также представления прогнозов и выводов, основанных на полученных результатах, был применен логический и интерпретирующий подход.

Ключевые слова: хактивизм, типы мотивации, индивиды или группы, похожие на хактивистов

Introduction. Nowadays a lot of cyber-attacks are conducted by individuals or groups that are pursuing mass awareness about various social situations: clearness of the elections, financial operations made by the government and so on. All these people call themselves hacktivists and believe that their online activities are devoted to improvements although means of uncovering the truth often lies under the law [1, p. 36]. However, in recent years the destructive effect of such activities has overbalanced the benefit. Do we still need such a “voice of truth”, and if not, is there a chance to silence it?

Definition: What is hacktivism? Coined in the mid-1990s by Cult of the Dead Cow, "hacktivism" initially described politically motivated cyberattacks that spread ideology without financial gain, with groups like Anonymous gaining notoriety in the 2010s through disruptive tactics such as DDoS campaigns against vul-

 ISSN 2541-8009

nerable targets, though improved cybersecurity and law enforcement eventually reduced its prominence [2, p. 280].

Motivation. Contrary to the past, modern hacktivists focus on advancing their political agendas, which vary in transparency [3]. Broadly, we classified their motivations into groups: ideological, political, nationalistic, and opportunistic. While some groups strictly align with one category, others pursue multiple agendas, often with a primary focus supplemented by secondary causes.

– Ideological motivations drive the most hacktivist activity. These groups target entities that challenge their worldviews, often focusing on religious beliefs or geopolitical conflicts.

As an example, pro-Russian group "NoName057(16)" often tries to target various Ukrainian agencies and governmental structures. GlorySec, possibly a Venezuelan group self-described as anarcho-capitalists, "believe in individual freedom and free markets" and therefore oppose countries like Russia and China as well as what they label "their proxy regimes" such as Cuba, Nicaragua, Houthi, Hezbollah, and Hamas [4].

– Some hacktivist groups seek to influence government policies or political outcomes, though such attacks are less common than ideological ones.

For example, "SiegedSec" targeted Project 2025, an initiative promoting conservative policies. They justified a hack and subsequent leak of a 200GB database by claiming that the project "threatens the right of abortion healthcare and LGBTQ+ communities in particular" [5]. Another similar case happened in August 2024. Following the arrest of Telegram's CEO, Pavel Durov, in France, several groups launched a #FreeDurov campaign, citing free speech infringements. As part of this effort, we saw People's CyberArmy initiating attacks against a French company, demanding Durov's release.

– Nationalistic hacktivist attacks are less common and often incorporate cultural symbols and patriotic rhetoric to justify their actions.

For instance, the Indian "Team UCC" group claims to "amplify Hindu voices" by "exposing false narratives that claim Hindus are safe in Bangladesh". They position themselves as defenders of Hindus worldwide, particularly in Bangladesh. They attack Pakistani government websites and organizations as an effort to "defend the Indian cyberspace".

– Some hacktivist groups act purely opportunistically, targeting organizations simply because they are easy to hack.

For example, SiegedSec hacked into a messaging application's website, citing that "it's not secure at all". The app being "made in China" might have compounded their motivation, but the group mentioned getting "access to their AWS S3 buckets", suggesting that the attack required minimal effort rather than a justification.

Methods and techniques. Presented diagram shows percentages of the various types of attacks carried out by the hacktivists (fig. 1). Some of them may be used in a combination to create a greater threat.

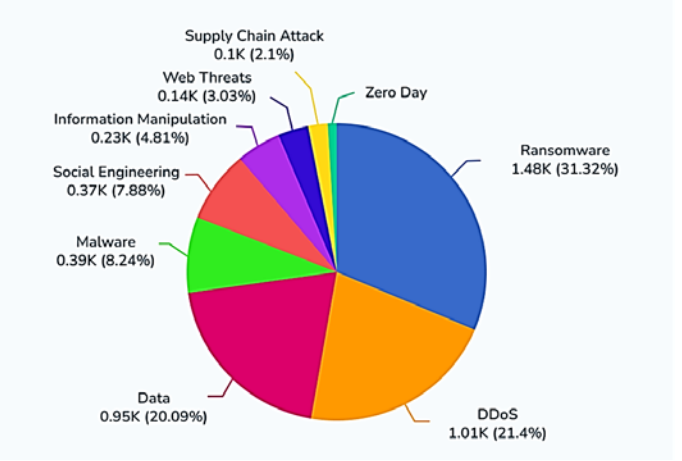

Fig. 1. Main hacktivists’ techniques used for attacking

The most frequently used technique is malicious software known as ransomware [6, p. 102].While traditionally being profit-driven, hacktivists have weaponized it to advance ideological goals. Some groups collaborate with cybercriminals to deploy ransomware, encrypting data to disrupt targets aligned with their political enemies (e. g., governments, corporations) [7, p. 54].

When hacktivism has dramatically changed. During the first quarter of 2022, there was a sharp increase in the number of cyberattacks, which was likely due to the start of a war between Russia and Ukraine. This was followed by retaliatory actions taken by various countries, leading to a particularly rapid rise in the number of threats posed by hacktivists. The end of the year saw a decrease in overall activity, although this was not as significant due to the ongoing anti-government protests in several Asian countries [7].

2023 started with another increase, particularly in NATO countries, before the activity level began to decline in the middle of the year due to the implementation of effective protection measures. However, the Israeli-Palestinian conflict that began at the end of that year led to an almost two-fold increase in attacks.

In 2024, activists formed various alliances more actively, which impacted their performance. Additionally, the escalation of tensions between China and Taiwan and the US elections at the end of that year also contributed to the overall number of attacks (fig. 2).

 ISSN 2541-8009

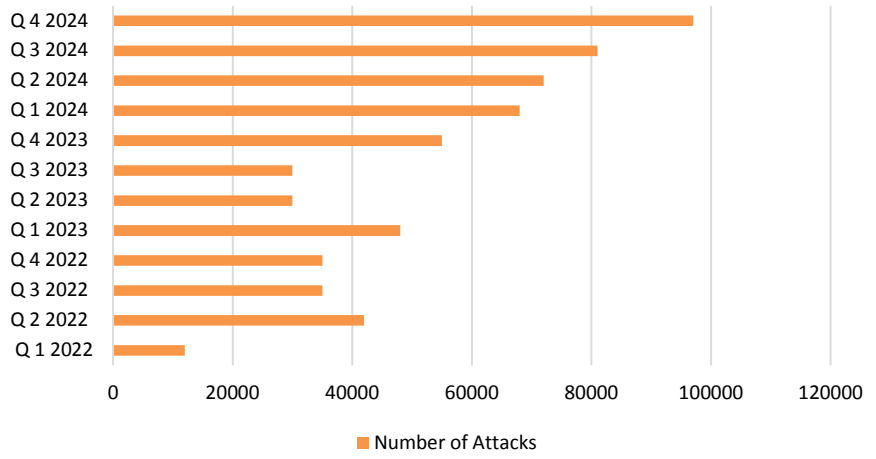

Fig. 2. Statistics of hacktivists’ attacks for the period from 2022 till 2024

Current situation. Hacktivist-like groups. After global political changes have occurred, hacktivism became a significant danger [8,178]. Some researchers call this new branch of hacktivism – hacktivist-like individuals or groups. They are characterized by their high level of coordination, large membership, and activities closely aligned with state interests [9]. The probability of government influence (direct or indirect) or support is high, as these groups often pursue specific political or ideological agendas, reflecting a more strategic and state-oriented approach to cyber operations. Given the substantial resources and support these groups receive, including significant technical and informational backing, they should be considered a high-level threat [10].

Ways of protecting from hacktivists. After analyzing the opinions of various experts, a general conclusion can be drawn that the current situation is likely to continue to deteriorate despite measures being taken to address the threat. In light of this, it is essential to adopt a more proactive approach to combat the escalating situation. The most effective strategy would be to establish a robust defense mechanism. This can be achieved through the application of the following approaches:

– Investing in DDoS protection. If uptime is crucial to operations, consider this as an insurance policy to maintain continuity.

– Securing web-facing assets. Document and fully patch external systems to reduce the risk of defacements and other attacks.

– Implementing attack surface risk management (ASRM). Deploy tools to monitor entry points, which helps minimize hacking attempts.

– Draw from industry expertise. Enhance preparedness against hacktivism and similar threats through resources that provide guidance for organizations during times of conflict.

As well as maintaining technical security companies should educate their employees about the potential risk of clicking on suspicious link sent by email. In case of fighting with malicious hacktivists the best strategy is to be proactive and prepared for the continuous process of creating a more secure network.

Conclusion. Hacktivism has undergone a crucial change in recent years. Previously it was considered as a way of civil disobediene and now it has evolved into a multifaceted threat that blurs the lines between activism, cybercrime, and state-sponsored aggression. While its roots in challenging power structures remain, the proliferation of advanced tools, geopolitical tensions, and alliances with cybercriminals have transformed hacktivism into a destabilizing force with global repercussions. Referring to prognostications, pro-government hacktivist-like groups will increasingly act as proxies in hybrid wars, targeting critical infrastructure (energy, healthcare) to sow chaos. Also, Generative AI tools like WormGPT will automate phishing, deepfake disinformation, and vulnerability discovery, enabling smaller groups to launch large-scale attacks and manipulate public opinion during elections, combining DDoS attacks on voting systems with social media disinformation. Moreover, ideologically motivated ransomware attacks will surge, with hacktivists encrypting data to paralyze adversaries rather than seeking profit.

References

[1] Jordan T., Taylor P.A. Hacktivism and Cyberwars: Rebels with a Cause? *Routledge*, 2008. https://doi.org/10.4324/9780203490037

[2] Himma K.E. *Internet Security: Hacking, Counterhacking, and Society*. Jones & Bartlett Learning, 2007.

[3] *The rising tide: A 2024 retrospective of hacktivism*. URL: https://www.silobreaker.com/blog/cyber-threats/hacktivism-ransomware-and-geopolitics-2024-in-review/ (accessed 15.06.2025).

[4] *Security Navigator 2025 reveals Europe as top target for hacktivism, with groups shifting focus to cognitive warfare*. URL: https://www.orangecyberdefense.com/uk/news/orange-cyberdefense/security-navigator-2025-reveals-europe-as-top-target-for-hacktivism (accessed 15.06.2025).

[5] *Hacktivism: Types, Goals, and Real-World Examples*. URL: https://www.investopedia.com/terms/h/hacktivism.asp (accessed 15.06.2025).

Sauter M. *The Coming Swarm: DDoS Actions, Hacktivism, and Civil Disobedience on the Internet*. Bloomsbury Academic, 2014. https://doi.org/10.5040/9781628926705

 ISSN 2541-8009

[6] *European Union Agency for Cybersecurity (ENISA)*. Understanding Cyber Threats from Hacktivism, 2020.

[7] Denning D.E. *Terrorism and Cyberterrorism: Threats and Responses*. Routledge, 2015.

[8] *Trend Micro. Understanding Hacktivists: The Overlap of Ideology and Cybercrime*. URL: https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/understanding-hacktivists-the-overlap-of-ideology-and-cybercrime (accessed 15.06.2025).

[9] *Forbes. Why Preparing For Hacktivism Should Be A Cybersecurity Priority*. URL: https://www.forbes.com/councils/forbestechcouncil/2023/04/14/why-preparing-for-hacktivism-should-be-a-cybersecurity-priority/ (accessed 15.06.2025).

Received 04.07.2025

Близнякова Анастасия Игоревна — студентка кафедры «Безопасность в цифровом мире», МГТУ им. Н.Э. Баумана, Москва, Российская Федерация.

Ссылку на эту статью просим оформлять следующим образом:
Близнякова А.И. Хактивизм: от абсолютной гласности до цифровой угрозы. *Политехнический молодежный журнал*, 2026, № 02 (103). URL: https://ptsj.bmstu.ru/catalog/hum/socio/1103.html

HACKTIVISM: FROM ENTIRE PUBLICITY TO DIGITAL THREATENING

A.I. Bliznyakova bai22yu014@student.bmstu.ru

Bauman Moscow State Technical University, Moscow, Russian Federation

The article presents a study on the well-established socio-digital phenomenon known as hacktivism. The goal of this research is to investigate its transformation from the realm of digital hooliganism into the purview of law enforcement authorities. To create this work, we have used materials from well-established researchers in the field of cybersecurity, as well as online publications from reputable sources that characterize the concept of "hacktivism", revealing its main objectives, methods employed in organizing attacks, and providing commentary on the evolution of this phenomenon into one of the major threats of recent years. Referring to the methods employed in the course of this research, methods of data collection, critical analysis, and synthesis of scientific and professional literature from publicly available sources were employed. The historical and diachronic approach was used to examine the evolution of hacktivism under the influence of socioeconomic and political factors. The case study method was utilized to analyze specific examples of hacktivist activity and their associated means and techniques. A logical and interpretive approach was applied to generalize and interpret the collected data, as well as to present forecasts and conclusions based on the findings.

Keywords: hacktivism, types of motivation, hacktivist-like individuals or groups

Received 04.07.2025

Bliznyakova A.I. — Student of Department of Computer Forensics, Bauman Moscow State Technical University, Moscow, Russian Federation.

Please cite this article in English as:
Bliznyakova A.I. Hacktivism: from entire publicity to digital threatening. *Politekhnicheskiy molodezhnyy zhurnal*, 2026, no. 02 (103). URL: https://ptsj.bmstu.ru/catalog/hum/socio/1103.html

 ISSN 2541-8009