TARTU UNIVERSITY

Faculty of Social Sciences

Johan Skytte Institute of Political Studies

Simon Berner

TELEGRAM-BASED RUSSIAN HACKTIVSM AS A NEW PHENOMENON AND THE INFLUENCE OF MEDIA VISIBILITY ON TARGET SELECTION

MA thesis

Supervisor: Martin Mölder, PhD

Tartu 2025

Authorship declaration

I have prepared this thesis independently. All the views of other authors, as well as data from literary sources and elsewhere, have been cited.

Word count of the thesis: 25 240

Simon Berner, 19.05.2025

Abstract

Russia's full-scale invasion of Ukraine in February 2022 resulted in a rise in cyber threats and initiated a continuing surge of coordinated cyberattacks by Russian-speaking hacktivist groups targeting countries expressing solidarity with Ukraine. This thesis explores the emergence of Telegram-based Russian hacktivism following the full-scale invasion of Ukraine in 2022 and examines the extent to which domestic media coverage influences the frequency of cyberattacks claimed by these groups. While prior academic literature has focused on hacktivism as the use of the internet to promote or resist sociopolitical agendas due to ideological beliefs, often targeting cyberspace itself as a means to achieve social change, this thesis argues that a distinct new era of hacktivism has emerged. This Telegram-based Russian hacktivism is characterized by centralized, openly malicious collectives operating through Telegram, combining geopolitical motives with financial incentives and media-driven strategies. The thesis employs a mixed-methods research design consisting of a qualitative and quantitative analysis. The qualitative exploration of the phenomenon reveals that post-2022 Russian hacktivist groups operate in a reactive and opportunistic manner, frequently targeting civilian infrastructure with low-sophistication attacks such as DDoS, while seeking visibility and legitimacy through public announcements and propaganda. The quantitative component evaluates the relationship between media coverage and attack frequency using two original datasets: over 20,000 claimed cyberattacks and more than 5,500 media articles across 16 EU countries. The findings show a generally positive but inconsistent correlation between media visibility and cyberattacks, with clear evidence in some cases (e.g., Germany, Slovenia) that media attention precedes increased targeting. However, other cases suggest that strategic or geopolitical relevance may override visibility as the primary driver of attacks.

Keywords: hacktivism, Russian hacktivism, cyberattacks, Telegram, media visibility, DDoS, digital activism, geopolitical targeting

Table of Contents

Introduction 7

1. Theoretical considerations 11

1.1. Political Participation and Activism in the Digital Age 13

1.2 Three-era model for understanding hacktivism 16

1.2.1 Early hacktivism as non-malicious and symbolic digital activism 18

1.2.2 Mid-2000s hacktivism Embracing Disruption and Spectacle 24

1.2.3 Contemporary Age of Telegram-Based, Profit-Motivated Hacktivism 29

2. Methodology 31

2.1 Qualitative Analysis - Understanding Telegram-Based Russian Hacktivism 33

2.1.1 Case selection 33

2.1.2 Data collection and analysis 34

2.2 Quantitative Analysis - Media Visibility and Cyberattack Frequency 38

2.2.1 Case selection 38

2.2.2 Data collection and analysis 39

2.3 Limitations 42

3. Empirical Analysis – Part I 44

3.1 Target selection and grounds for justification 45

3.2 Types of cyber attacks 50

3.2.1 Distributed Denial of Service 50

3.2.2 Defacements 51

3.2.3 Data Leaks 53

3.2.4 Summary of Russian hacktivist cyber attack types and technical sophistication 55

3.3 Communication 55

3.3.1 Telegram 56

3.3.2. Cyber-attack announcements 57

3.3.3 Forming alliances 58

3.4 Advertising and selling services 59

3.4.1 Advertising non-malicious services 60

3.4.2 Malicious services 61

3.4.3 Asking for donations 62

3.4.4 Providing services 62

3.5 Recruitment 64
4. Empirical Analysis – Part II 70
4.1 Cross-National Patterns of Cyberattacks and Media Visibility 71
4.1.2 General Patterns and Correlation 73
4.2 Timing and Event-Driven Spikes in Media Attention 75
4.2.1 Use Case: Germany 76
4.2.2 Use Case: Poland 77
4.2.3 Use Case: Czechia 77
4.2.4 Use Case: Slovenia 78
4.2.5 Use Case: Luxembourg 79
4.2.6 Use Case: Estonia 80
5. Conclusion 82
References 86
Appendicies 91

List of abbreviations

APT - Advanced Persistent Threat

CDC - Cult of the Dead Cow

CF - Cloudflare

CIA - Central Intelligence Agency

CIRSS - Center for International Relations and Strategic Studies

CV - Curriculum Vitae

DDoS - Distributed Denial of Service

ECB - European Central Bank

EDT - Electronic Disturbance Theater

EU - European Union

HaaS - Hacking-as-a-Service

IRC - Internet Relay Chat

IS - Islamic State

NATO - North Atlantic Treaty Organization

OSINT - Open-Source Intelligence

TTP - Tactics, Techniques, and Procedures

VPN - Virtual Private Network

EU – European Union

Introduction

The full-scale invasion of Ukraine by Russia, starting on February 24th, 2022, significantly altered the geopolitical order, simultaneously reshaping the digital landscape, where cybersecurity risks became increasingly prevalent (Brunk & Hakimi, 2022; Varbanov et al. 2024, p. 2). The immediate aftermath marked the beginning of a surge in coordinated cyberattacks carried out by Russian-speaking hacktivist groups, a trend that continues to this day. Leveraging the communication platform Telegram, these actors directed their attacks against countries that expressed their support for Ukraine (Canevez et al., 2024, p. 169). These cyberattacks targeting critical national infrastructures, sensitive banking systems, and essential government ministries continue to exert a direct impact on the daily lives of citizens and the operations of state functions within the targeted countries (Guchua & Zedelashvili, 2023, p. 35). This evolving threat in the digital landscape calls for a renewed attention to the role of non-state actors, such as hacktivist groups, as the line between activism, cybercrime, and state-aligned operations becomes increasingly blurred.

Despite the growing visibility and operational impact of these Russian hacktivist groups targeting European countries, there is a gap in the academic literature on the conceptualization of this phenomenon. Scholarly discourse reveals dissent regarding the fundamental nature of hacktivism, with perspectives diverging on whether it is a specific tactic, a broader tool for activism, or even a distinct social movement (Farmer, 2022). This contestation regarding the definition is further underscored by internal disagreements within hacktivist communities concerning the ethical code and strategic approaches of their operations, particularly regarding the acceptable level of disruption and spectacle (Milan, 2015, p. 1). Furthermore, the ongoing hacktivist attacks by Russian groups that affect public life and challenge the resilience of critical infrastructure (Guchua & Zedelashvili, 2023, p. 35) underscore the need for developing effective countermeasures. To address the need for both academic understanding and the development of resilience against post-2022 Russian hacktivism, the primary objective of this thesis is twofold. First, it seeks to explore and characterize post-2022 Russian hacktivism as a unique phenomenon. Second, it sets out to examine the strategic role of media visibility in the targeting decisions of Russian hacktivist groups.

While superficially seeming to align with the conventional understanding of "hacktivism" – the use of unauthorized digital means to pursue political or social goals – through their stated political and patriotic declarations, post-2022 Russian hacktivist groups are notably different. These contemporary hacktivist groups frequently blend patriotic rhetoric with performative attacks and financial incentives, raising a central question for this thesis: in what ways does Telegram-based Russian hacktivism differ from earlier forms in terms of motivations, methods, and operational logic? To address this question, this thesis draws upon existing literature in political participation, digital activism, and hacktivism. It introduces a novel three-era model of hacktivism to establish criteria for understanding its evolution: (1) early symbolic and non-disruptive hacktivism, (2) the subsequent era of disruptive, spectacle-driven hacktivism, and (3) the current era, characterized by Russian Telegram-based groups integrating political messaging with profit-seeking objectives. This theoretical framework will serve as the basis for evaluating the distinctions between contemporary Russian hacktivism and its predecessors concerning motivation, methods, strategic objectives, and organizational structure. Assuming that visibility motivates the strategic operations of Russian hacktivists, the second research question of the thesis is: to what extent does domestic media coverage influence the frequency of cyberattacks claimed by Russian hacktivist groups?

To answer these two research questions, the thesis employs a mixed-method design that integrates both qualitative and quantitative approaches (Harbers & Ingram, 2020). The first part is qualitative and conceptual, based on systematic, first-hand monitoring of 48 Russian hacktivist Telegram channels over a 16-month period (November 2023 – February 2025). Through manual thematic coding, six dimensions of activity were analyzed: motivations, target selection, technical methods, communication, monetization strategies, and recruitment. The second part is quantitative and explanatory. It uses two original datasets - one containing over 20,000 cyberattacks, and another with more than 5,500 national media articles from 16 EU countries that are used to examine the relationship between media visibility and the frequency of hacktivist attacks. The hypothesis tested is whether increased domestic media coverage correlates with heightened targeting, suggesting that visibility acts as an incentive for further attacks.

The findings confirm that post-2022 Russian hacktivism differs from prior eras. Although hacktivism has long challenged the boundary between activism and crime (Denning, 2001), the emerging post-2022 Russian hacktivism extends this ambiguity further. While retaining the language of political ideology, these hacktivist groups function as quasi-criminal enterprises, actively recruiting, selling services, and competing for attention and legitimacy. Their platform of choice, Telegram, not only enables operational coordination but also serves as a stage for propaganda, monetization, and recruitment. Their methods are largely unsophisticated, with over 95% of attacks being basic DDoS campaigns, but their symbolic value is amplified through public proof (e.g., check-host links or defaced websites). Furthermore, their recruitment processes are unusually structured, involving public announcements, skill-based applications, and task-based vetting.

The quantitative analysis reveals a general but not universal correlation between national media coverage and hacktivist targeting. Countries such as Germany, Spain, and especially Italy, whose domestic media frequently covered Russian hacktivists, experienced disproportionately high attack volumes. Conversely, states with low media visibility, such as Estonia and Luxembourg, were rarely targeted despite their strong pro-Ukrainian stances. Timelines further support this relationship: in Germany and Slovenia, spikes in media attention often preceded or coincided with waves of cyberattacks. These findings suggest that visibility itself may function as a soft incentive, reinforcing the strategic logic of performative cyberattacks. While media attention does not fully explain hacktivist behavior, geopolitical alignment also matters and thus appears to significantly shape target selection in many cases.

This thesis makes three central contributions. First, it provides a detailed analysis of post-2022 Russian hacktivism, a topic that has received little academic attention despite its growing significance. The use of primary sources, including Telegram channels, recruitment messages, and attack announcements, fills a notable gap in the literature on political cyber activity. Second, the thesis offers a new three-era model of hacktivism that captures the evolution from symbolic protest to hybrid operations that integrate activism, propaganda, and financially motivated entrepreneurship. Third, by exploring how post-2022 Russian hacktivism operates and how it interacts with public visibility, this thesis offers insights into how states and societies might respond to a threat that is as much about narrative control as technical disruption. The practical contribution is that if hacktivist attacks are at least partially driven by media visibility, then reducing the volume or sensationalism of media coverage may serve as a soft deterrent.

The thesis consists of five chapters. Chapter one constitutes the theoretical framework. It situates hacktivism within the broader concept of political participation and digital activism. It then proposes a three-era model of hacktivism, conceptualizing the post-2022 Russian hacktivism as a unique phenomenon. Chapter two lays out the methodology, including the reasoning for choosing a mixed-methods design. It explains the case selection, data collection, and analysis for each part of the analysis – qualitative and quantitative. Furthermore, it outlines some limitations of the research. The following two chapters – chapters three and four – present the empirical analysis of the thesis. Chapter three focuses on the operations, recruitment systems, and monetization of the activities of Russian hacktivist groups. Chapter four delivers the quantitative analysis, assessing whether national media visibility correlates with cyberattack frequency across EU member states. Chapter five concludes the thesis by summarizing the main findings and discussing its theoretical and practical implications. It points out avenues for future research on the topic.

1. Theoretical considerations

Etymology suggests the term hacktivism derives from a combination of the words "activism" and "hacking" (Denning, 2001, p. 263). However, the definition of hacktivism is subject to significant debate as varying and conflicting ethical stances toward tactics and techniques within the hacktivist community exist (Milan, 2015, p. 1). Given hacktivism's adoption of computer techniques prevalent within the pre-existing hacker community, it becomes difficult to set a clear demarcation between hacking and hacktivism (Jordan & Taylor, 2004, p. 3). However, while all hacktivists use hacking techniques, not all hackers are hacktivists (Romagna, 2020, p. 758). Hacktivism inherently involves hacking, but hacking itself does not constitute hacktivism. Today, the term "hacker" refers to any individuals who use their technical computer skills to illegally gain access to sensitive systems or information for financial profit or other personal motives (Furnell, 2003). In contrast, hacktivists use hacking techniques to promote political causes for social change or ideological causes in distinct ways (Snyder, 2022). Thus, since hacktivism inherently involves unauthorized digital activity, all hacktivists belong to the subset within the general classification of hackers.[1] However, the reverse is not true, as hackers engage in such activities for a broader range of reasons that go beyond activism. Thus, this thesis understands hacktivism as the promotion of sociopolitical goals (ideological, theological, political, etc.) through the use of hacking techniques by disputing targeted digital infrastructure.

There is general scholarly consensus that hacktivism is a form of cybercrime (Farmer, 2022, p. 52). However, it is necessary to separate hacktivism from other forms of cybercrime (Furnell, 2003, p. 8). Hacktivists do not pursue direct economic value. They often target institutions, corporations, and organizations in the public or private sphere to protest the wrongdoing they observe through these institutions' behavior (Farmer, 2022, p. 70). Most other cybercriminals target organizations to obtain monetary gain using fraudulent, thieving, and extortion practices. While hacktivists generally work independently of government affiliation, strategy-based hackers, such as Advanced Persistent Threats (APTs), often have state sponsorship or support and purposefully act with political intention (Snyder, 2022, p. 11). APTs are a more sophisticated type of threat and can invest significant amounts of time using advanced techniques to engage in long-term espionage and strategic activities.

[1] Contrary to its current association with illegal computer activities, "hacking" initially described the practice of creatively operating with systems to achieve original or unintended functionalities (Holt, 2020, p. 726).

Cybercriminals driven by financial motivations will primarily engage in a phishing attack, deploy malware, or data theft to attack individual or business targets (Singer & Friedman, 2014, p. 84). Hacktivists, in contrast, are motivated by ideological commitments and political objectives. They may use similar technical methods (DDoS attacks or data breaches) as other cybercriminals. However, the divergence resides in their intention and motivation. Hacktivists aim for political protest or protest action, and other cybercriminals for personal gain (ibid.). This sets the basis for the difference between hacktivism and other forms of cybercrime related to digital civil disobedience (Manion & Goodrum, 2000, p. 17).

Originating in the late 1990s, the phenomenon of hacktivism has undergone different historical developments. Nevertheless, three fundamental elements have served as typical characterizations of the diverse expressions of hacktivism as a phenomenon. First, political or ideological motivation is often centered on issues such as anti-censorship, civil liberties, or resisting surveillance (Romagna, 2020, p. 746). Second, hacktivists employ various technical methods such as website defacement, virtual sit-ins, and information leaks. These methods are used as protest action, not as means for any person or entity to profit (Samuel, 2004, p. 123). Third, hacktivist operations often incorporate an array of public communications or symbolic messaging to create clear political narratives on the issues they raise awareness of and bring social change (Romagna, 2020, p. 746).

This thesis argues that immediately following Russia's full-scale invasion of Ukraine in February 2022, a new type of hacktivism that is distinct from previous understandings of the concept began to evolve. This era of hacktivism is unique in both the underlying intentions and motivations of hacktivists as well as the organizational structure of hacktivist groups. The central argument is that this era constitutes a unique evolution that features geopolitical motivations and the prominence of the social media platform Telegram as the core organizational venue. While these hacktivist groups may superficially align with the the characteristics of “classical hacktivism“ due to their proclamation of political and patriotic motives, there are several indicators that they differ from previous hacktivist groups due to deviations in their underlying motivations (e.g., financial gain) and operational logic (e.g. malicious targeting of civilian infrastructure). Therefore, post-2022 Russian hacktivism diverges significantly from the previously established understanding of hacktivism as a category of digital activism.

1.1. Political Participation and Activism in the Digital Age

To contextualize the phenomenon of hacktivism, it is necessary to explain its position within the broader framework of political activism, which itself can be understood as a specific subset of political participation. Political participation is a notion that has been used with varying connotations and goals (Voss, 2014, p. 9). Politicians have invoked it in discussions of electoral turnout, citizen groups as a call for increased engagement, and scholars across have engaged with the concept of political participation, whether in empirical fields like electoral studies or within normative frameworks such as democratic theory (Norris, 2009). The emergence of hacktivism as a form of activism, however, has challenged traditional understandings of political participation (Denning, 2001). This chapter aims to provide a comprehensive overview, mapping diverse understandings of political participation, focusing on its online modes and the subset of political activism.

Political participation lacks a singular definition and has various interpretations depending on the subjective perception of sociatal participation (Voss, 2014, p. 10). In the 1950s and early 1960s, scholars viewed voting and involvement in political organizations such as political parties as a key form of political participation, as the focus was primarily on citizens' direct influence on the political sphere (Gabriel, 2013, p. 383). This perspective limits the definition of political participation to legally binding forms and excludes non-institutionalized and extra-representational forms (Voss, 2014, p. 10). Despite the later recognition of non-institutionalized forms of political participation, research prior to the late 1980s primarily focused on structural resources and cultural attitudes, rather than studying the role of institutional factors in shaping political participation (Norris, 2009). Over time, scholarly focus shifted from analysing formal and established activities like voting, party work, and contacting politicians to extra-representational forms of political participation, including protest and other less visible dynamics to participate in political discourse (Jensen et al., 2012, p. 4).

Verba and Nie (1972) developed one of the foundational empirical models of political participation, focusing on individual-centered engagement and adopting a bottom-up approach (Norris, 2009; Verba & Nie, 1972, p. 3). The authors define political participation as "those activities by private citizens that are more or less directly aimed at influencing the selection of governmental personnel and/or the actions they take "(Verba & Nie, 1972, p. 2).

Thus, participation is understood as democratic participation and entails concrete activities of citizens intended to influence the government, including but not limited to voting and campaign activity (ibid., p. 3). To explain why citizens engage in political participation, Verba and Nie (1972) recognized structural resources such as income, ethnicity, sex, education, age, and cultural attitudes as key motivators. Beyond these individual-level factors, the authors also touched upon the significant impact of institutional factors, including voting registration processes and membership in organizations such as labor unions and parties (Norris, 2009).

A common understanding of political participation entails all voluntary activities by which citizens try to exert influence or directly engage with various levels of the political system (Gabriel, 2013, p. 383). However, the study of political participation, particularly within democratic political systems, does not focus solely on bottom-up dynamics of citizen influence on policy-makers and government but also encompasses a top-down perspective.[2] The latter approach focuses on participation processes initiated by government administrations. Kubicek et al. (2009) analyse political participation from this perspective and understand it as citizen participation initiated by the administration. It includes varying forms of participation such as organizing national elections, distributing political information, enabling political communication, and consultation (ibid., p.19). A broad understanding of political participation reveals top-down and bottom-up perspectives as complementary aspects of the concept. State actors may organize participation, yet it also occurs through various informal channels through which citizens engage (Voss, 2014, p. 11).

Although the terms political participation and political engagement may overlap and even be used synonymously in certain instances concerning the involvement in civil society or political parties, it remains important to distinguish between these concepts (Voss, 2014, p. 11). For Jensen et al. (2012), political engagement serves as the general term, encompassing political participation as one of its three constituent dimensions, the other two being information consumption and attitudes. They define political participation as "actions taken

[2] It is important to note that the function of participation and the role of democracy are often intertwined, as participation can be viewed as a way to produce legitimation. In normative democratic theory, participation is often viewed as a fundamental component of democracy (Voss, 2014, p. 13). From the Schumpeterian view, limited public participation is seen as sufficient as long as electoral competition is provided. Theorists advocating for a participatory democracy, on the other hand, argue that extensive citizen involvement is vital and opportunities for grassroots participation and deliberation should be expanded upon (Norris, 2009, p. 630).

by citizens to influence political outcomes" (Jensen et al., 2012, p. 4). This is a broad definition and encompasses both representative and extra-representative activities, as well as vertical and horizontal directions of action. When political participation takes place outside of digital media, it can be divided into representative (e.g., elections) or extra-representative (e.g., protest) activities. Political participation online can be vertical (e.g., donations) or horizontal (e.g., political commentary on social media) (ibid.). Although certain forms of political participation, such as petitions, appear in both offline and online contexts, the widespread utilization of the Internet has led to the emergence of novel modes of political participation (Voss, 2014, p. 12).

The conceptualization of activism within political participation varies. While now a mainstream part of activism, late 1970s literature viewed direct citizen action like protests as a form of participation only activated when citizens were pushed to their limits and employed only when facing increasingly intolerable political alternatives (Budge, 1981, p. 221). Today, activism can be understood broadly as any political engagement highlighting citizens' roles and influence channels within democratic systems (Norris, 2009, p. 638). This understanding of activism includes citizen-oriented actions such as participating in elections and cause-oriented activities focusing on specific social or environmental issues and concrete policies, including activities such as protests and demonstrations (ibid., p. 640). Alternatively, a narrower definition positions it as a specific subset of political participation alongside activities like lobbying and petitioning (Kubicek et al., 2009, p. 19). Regardless of its scope, activism is overall viewed as a form of civic engagement initiated from a bottom-up perspective and includes a variety of activities (Voss, 2014, p. 11).

Digitalization and the concurrent expansion of internet access and social media usage have fundamentally reshaped the activism landscape, giving rise to digital activism. The prevalence of online campaigns, social movements emerging through hashtags, and the digital communication strategies of activist groups now represent a significant aspect of political engagement and have become normalized practices (Fielitz & Staemmler, 2020, p. 426). Denning (2001) refers to digital activism as a "normal, nondisruptive use of the Internet in support of an agenda or cause "(p. 241). From this perspective, the Internet is viewed as a tool for activism (ibid., p. 242). Contrary to the notion of digital activism as solely non-disruptive, Murdoch (2010, p. 137) points out its capacity to involve destructive and disruptive methods, thereby underscoring the potential negative dimensions of citizen

empowerment via digital tools. Within social movement studies, digital activism encompasses all activities undertaken by activists that utilize digital infrastructure (hardware and software) to promote social or political change (Fielitz & Staemmler, 2020, p. 427).

Fielitz and Staemmler (2020, p. 429) propose five categories of digital activism: click activism, hashtag activism, campaign activism, tech activism, and hacktivism. Although these categories are not strict ideal types and overlap to some degree, they offer a valuable framework for differentiating various forms of digital activism. Hacktivism, from this perspective, moves beyond a broad definition like "activism gone electronic "(Jordan & Taylor, 2004, p. 1) or a narrow understanding of hacktivism as an illegal protest practice (Baringhorst, 2014, p. 108). Instead, Fielitz and Staemmler (2020, p. 434) refer to hacktivism as a practice within a technologically skilled subculture where individuals collaboratively leverage internet infrastructures and employ manipulation techniques to generate public attention for political causes. This definition emphasizes that there is a collective of people with a shared interest in technology use that seeks to draw attention to a larger political or social issue (Milone 2003, p.77).

1.2 Three-era model for understanding hacktivism

To understand the diverse theoretical interpretations of hacktivism, scholars have historically traced its progression (Karagiannopoulos, 2018, p. 15; Milan, 2015, p. 2; Romagna, 2020, p. 758). While commonalities exist in categorizing its evolution from ethical, grassroots, and symbolic beginnings to more confrontational cause-based actions, scholars also offer different periodizations. Karagiannopoulos (2018, p. 15) breaks hacktivism into two eras, while Romagna (2020, p. 758) differentiates between three distinct phases. Building upon these existing frameworks, this thesis proposes that hacktivism can be historically separated into two distinct eras and that a perceived shift in the operational modalities, motivational factors, and recruitment strategies of hacktivism that has emerged since February 2022 constitutes a third, new era.[3]

[3] Although the three phases proposed by Romagna (2020) provide useful temporal structure, this thesis maintains that his second and third phases identified with Anonymous and the proliferation of cause-based cells can be understood as comparable occurrences in the same ideological and operational development. Both groups operate as decentralized, anti-authoritarian hacktivism engaged by ideologically fluid motives of media spectacle, and reactive campaigns that target unjust representations. The differences highlighted by Romagna - group platform choice, geographic contributions, and fragmented organization - are gradual moments of evolution in one model, rather than a decisive break warranting an entirely new phase.

The proposed periodization of hacktivism in this thesis is based not only on temporal markers but also on ideology, organizational logic, and strategic alignment. The first era included symbolic digital activism (Singer & Friedman, 2014, p. 87). The second phase included decentralized, confrontational hacktivist collectives like Anonymous, LulzSec, and TeaMp0isoN (Pendergrass & Morris, 2012). A defining feature of the third era of hacktivism is the prevalence of Telegram-based geopolitical hacktivism, with Russian groups like NoName057(16), KillNet, and CyberArmyOfRussia (Grossman et al., 2023, p. 20) The third phase is characterized by increased alignment with state interests, hyper-centralized propaganda, and hacktivism's shift from civil resistance to an instrument of hybrid conflict and monetary gain. While hacktivism in its first two eras constitutes a form of digital activism, the third era represents a departure from this, no longer aligning with the definition of digital activism.

Table 1. Comparative overview of the three eras of hacktivism based on key operational features.

Feature	First era	Second era	Third era
Motivation	Ideological/Ethical	Ideological/Protest	Geopolitical/Financial
Target Selection	Symbolic institutions (e.g., surveillance agencies)	Aligned with ideological causes (e.g., censorship, corruption, human rights violations)	Geopolitically aligned; often indiscriminate and aimed at civilian infrastructure
Tactics	Vulnerability disclosure, symbolic attacks	DDoS-attacks, Defacements, Data Leaks	DDoS-attacks, Defacements, Data Leaks
Monetization	None	None	Central feature: donations, HaaS, selling tools
Organizational Structure	Loosely affiliated, mostly non-anonymous collectives	Decentralized/anonymous	Semi-organized clusters with leadership, vetting, and public recruitment structures
Communication	Mailing lists, IRC	Social Media, IRC	Social Media

1.2.1 Early hacktivism as non-malicious and symbolic digital activism

The first phase of hacktivism from the early 1990s to the early 2000s was characterized by collectives with a tendency for left-wing ideologies that employed ethical methods for conveying a political message (Romagna, 2020, p. 758; Jordan & Taylor, 2004, p. 94). These hacktivist groups were either performative hacktivists, such as the Electronic Disturbance Theater (EDT), or hacktivists who started out as non-political hackers and technology enthusiasts and discovered a way to influence public policies, such as Cult of the Dead Cow (CDC) and L0pht (Samuel, 2004). These organized collectives were among the first to conjoin technical hacking and political and social advocacy (Goodrum & Manion, 2000, p. 14). Their actions were typically non-malicious and symbolic, building off the ideas promoted by those advocating for internet freedom, civil liberties, and resistance to censorship (Jordan & Taylor, 2004, p. 95). Rather than seeking disruption as an end in itself, these collectives strategically framed their online political activities as electronic civil disobedience, advocating for digital rights, or conducting ethical security research (Goodrum & Manion, 2000). Collectives such as the EDT, CDC, and L0pht were motivated by a shared moral commitment to transparency, free speech, and being able to resist and stand up against new forms of surveillance and censorship. The methods applied by these collectives ranged from commemorative, symbolic "virtual sit-ins" to developing privacy-enhancing tools to the responsible disclosure of software vulnerabilities (Samuel, 2004, p. 124). Another distinction between these collectives and later forms of hacktivism is that these groups often embraced public accountability and transparency. Compared to hacktivist movements that appeared later, the collectives from the early 1990s, such as the Electronic Disturbance Theater (EDT), intentionally chose not to be anonymous (Dominguez, 2016, p. 111). Other groups operated under pseudonyms; however, their real names were often not difficult to figure out (Samuel, 2004, p.131).

Some of the most prominent hacktivist groups from this era, such as the Cult of the Dead Cow (CDC), the Electronic Disturbance Theater (EDT), and L0pht, found their ideological roots in sociopolitical ideas characteristic of traditional left-wing and anti-globalization movements (Romagna, 2020, p. 760). They also advocated for causes such as digital rights and transparency in technology (Brooks et al., 2021, p. 46). The Cult of the Dead Cow was one of the first hacker collectives to establish the conceptual frameworks for modern

hacktivism that emphasized legal and ethical methods of making a point (Jordan & Taylor, 2004, p. 95). Founded in 1984 in Texas, the CDC's core ideological framework embraced and endorsed the right to privacy and the right of access to information as an inherent human right (Samuel, 2004, p. 131). The collective's philosophy, as stated by one of the CDC's founders, Bill Brown, stressed that "telecom is a means to an end, not an end to a means" (Menn, 2019, p. 15) to focus on human communication, not technology. Additionally, the CDC endorsed the “Declaration of Independence for Cyberspace” written by John Perry Barlow in 1996 which asserted that cyberspace as a new realm should be independent form the control and sovereignity of governments and instead be a space which every individual can access and express their beliefs (Hearn et al., 2009, p. 3).

L0pht, a 1990s hacker community dedicated to raising awareness of computer security vulnerabilities and advocating for technological transparency, was also driven by ethical motivations (Brooks et al., 2021, p. 46). Their philosophy was in line with the hacker ethic that takes a stance of active access to information, improving a system, and not destroying it (Best, 2003, p. 269). The ethical principles underpinning the L0pht collective's operations were underscored by their public denunciation of destructive cyberattacks carried out by several other prominent hacker groups, notably including the Legion of the Underground's declaration of cyberwar against China and Iraq (Best, 2003).

The Electronic Disturbance Theater (EDT), a collective formed following the Acteal Massacre in Chiapas in 1997, whereby paramilitary groups killed forty-five indigenous people, also portrayed their activities as part of digital activism (Dominguez, 2009; p. 1806). The group consisted of what Samuel (2004) refers to as “performative hacktivists“ (p. 129) - people with a background in both hacking and artistic activism. The EDT operated in accordance with a general anti-authoritarian ideology as they stressed that certain populations are disadvantaged by global norms and lack the same access as others who are more integrated into the global system (Dominguez, 2009; p. 1809). Compared to L0pht and the CDC, the Electronic Disturbance Theater was more focused on sociopolitical causes (Romagna, 2020, p. 760) and practiced “transnational activism” (Sauter, 2014, p. 51) or “mass action hacktivism” (Jordan & Taylor, 2004, p. 85). It was a group consisting of cyberactivists and artists who put the Electronic Civil Disobedience theory that arose in the early 1990s as a response to the changing landscape of capital and power in the digital world into practice (Dominguez, 2009). The Critical Art Ensemble first thought of the Electronic

Civil Disobedience as a theoretical base in 1994, arguing that while capital moved from centered urban locales to decentralized cyberspace, activist movements followed suit (Dominguez, 2016, p. 109).

Besides having ideological underpinnings and ethical stances, the legitimacy of hacktivist groups from that era was supported by their rather transparent approach to activism (Manion & Goodrum, 2000, p. 15). The Cult of the Dead Cow collective took part in various popular political campaigns, including protesting Internet censorship in China (Hearn et al, 2009, p. 4). They worked with other hacktivist groups, such as Hong Kong Blondes, where the Cult of the Dead Cow helped hack into computer networks in China to get around Internet censorship blocks in the 1990s (Singer & Friedman, 2014, p. 77). In fact, they progressed from that initial effort with the Hong Kong Blondes to their "Goolag" campaign against Google, when Google cooperated with Chinese censorship demands (Menn, 2019, p. 87). Constantly progressing their aim to promote any human rights causes, they launched the satellite organization Hacktivismo, a software project aiming to dismantle online censorship in authotarian regimes (Samuel, 2004, p. 124).

Rather than relying on destructive practices, hacktivist groups from that era, such as the Cult of the Dead Cow, the Electronic Disturbance Theater and L0pht sought to distinguish themselves from cybercriminals or terrorists by emphasizing non-violent methods and focusing on raising awareness rather than causing destruction (Jordan & Taylor, 2004, p. 95). The Cult of the Dead Cow categorically rejected destructive practices when they aligned with other leading hacker groups in condemning any attempts aimed at the destruction of national information infrastructures (Sauter, 2014, p. 47). The L0pht group prioritized the advocacy of active information access by deploying non-destructive tools as they focused on modeling technical analysis and responsible disclosure instead of destruction. The team gained notoriety for a product they produced called L0phtCrack, which demonstrated the flaws in security for Windows NT (Best, 2003, p. 269). The L0pht team's technical credibility was so strong that, in 1998, during congressional testimony, member Mudge stated they could turn off the whole Internet in 30 minutes, although they never specified how (Brooks et al, 2021, p. 47). The actions of the Electronic Disturbance Theater were planned not merely for disruption but to enhance widespread and media awareness of salient international issues, as their primary aim was to help marginalized communities stand up to institutional power

(Grindal, 2022, p. 35). This model of digital activism has influenced later movements and provided a template for blending artistic practice and political resistance.

The intent behind using their hacking techniques of the hacktivist collectives of that era was mostly non-malicious. The Cult of the Dead Cow collective chose to create and deploy privacy and security tools, free to the general public (Hearn et al, 2009). Their most notable technical contribution was Back Orifice, a remote administration tool that granted users access to controls of Windows or Unix-based PCs (Jordan & Taylor, 2004, p. 110). The L0pht group focused on making information available about software defects, especially given corporations like Microsoft were reluctant to accept any of these issues (McGraw, 2016, p. 10). Their focus was not on individual security vulnerabilities, but systemic security vulnerabilities, and they more often targeted specifically large technology organizations like Microsoft for their perceived inaction on securing systems (Özçelik & Brooks, 2020, p. 52). L0pht took their technical ability and converted it into public advocacy for a new voice in the cybersecurity practice of professional development, allowing them to be influencers and not be pegged as malicious hackers (McGraw, 2016). Ultimately, L0pht's work spawned principles of responsible vulnerability disclosures, which ultimately laid the basis for formal standards and protocols (for example, specific to bugs in software) that are in place today (Mollick, 2005).

While also staying mostly non-malicious, the Electronic Disturbance Theater's FloodNet, a browser-based application intended for virtual sit-ins, slowed government and corporate servers but left ordinary users and data intact (Grindal, 2022). Floodnet was a browser-based tool written in Java that was used for digital protest. Participants would visit a website hosting the tool, select a target, and it would bombard the target's webpages severs with rapid reload requests (Sauter, 2014, p. 110). The tool also allowed participants to send messages by requesting specific files from the server that was under attack. A request for "justice" or "human rights" generated a “404_file not found” message in the server’s logs (ibid., p. 111). It can be argued that the groups' "404_file not found" requests underscored the purely symbolic nature of the disruption, Floodnets purpose was to make “visible what was invisible“ (Dominguez, 2009, p. 1807) meaning the absence of certain issues or groups within the system of power represented either by the government or by powerful corporate actors. In the EDT's first significant actions were 13 pro-Zapatista Floodnet actions in 1998, which focused on protesting government involvement in the Acteal Massacre. They targeted the

websites of ex-Mexican President Zedillo, Clinton's White House, and the Frankfurt Stock Exchange, which epitomized emerging global capital (Sauter, 2014, p. 111).

The organizational structure of the hacktivist collectives of the first era had non-hierarchical tendencies and undertook mostly open operations. The organization of the Cult of the Dead Cow evolved over time. It started out as a text-file group, a community sharing rants, stories, and tech ideas on Fidonet, which was a bulletin board-based computer communication system (Jordan & Taylor, 2004, p. 95). Over time, they evolved into a well-known hacking and then hacktivist group as they created new hacking tools and openly discussed their opinions and ethical codes for hacktivism (ibid.). The group communicated with their audience through their electronic publication (in essence, an underground ezine) that focused on a variety of topics, and included anything from how-to guides to cultural and social commentary (Müller & Ulrich, 2015). The media coverage they received helped the group shape their public image as a real 'organization' in the hacker community with a balance of being activist and technical (Dautaj, 2018). The CDC claims to be the first group to come up with the term “hacktivism” which is to be understood as a form of protest that is legally questionable but non-violent and serves to advance or hinder political or societal change (Singer & Friedman, 2014, p. 77).

In terms of structure and organization, the EDT operated in a transparent leadership structure as opposed to anonymity. They had a core leadership group comprised of the artist-researchers Ricardo Dominguez, Carmin Karasic, Brett Stalbaum, and Stefan Wray (Dominguez, 2009). Using their real names was significant at the time, and they accepted the responsibility that came with it. Transparency was a deliberate choice made by the group to distance themselves from traditional hacker culture and connect their online actions to real-life life lived civil disobedience as citizens (Dominguez, 2016). The EDT also engaged with the public discussion and media attention based on transparency concerns as a key component of its mission. The group would put an action on the Internet with the date, time, and reason for the action (Dominguez, 2009). The group's stance on media is pedagogical. They see themselves as educating the public about social justice issues and illustrating how digital tools may be used for civil disobedience (Grindal, 2022).

The L0pht collective emerged as a physical space for people with a collective interest in computers as well as security problems that come with it (Brooks et al., 2021, p. 46). What

started as an informal gathering place for technology enthusiasts evolved into one of the most influential hacker collectives, with Peiter Zatko (known as Mudge) playing a pivotal role in transforming the group's direction and focus (McGraw, 2016, p. 7). Although L0pht and the CDC shared many similarities and also had common members, in contrast to L0pht, the CDC had no physical space for their collective. This made it easier to link the CDC to the criminal underground (Menn, 2019, p. 38-39). Eventually, L0pht turned into a security consultancy called @stake. Similar to the CDC and the Electronic Disturbance Theater, L0pht had sophisticated media awareness, which allowed them to take control of their overall image, and ultimately helped to ensure their associated technical outputs could be taken seriously by the security community (McGraw, 2016). Unlike the other two collectives, they collaborated with governmental institutions, and they probably built their most significant public relations activity by providing their testimony to the Senate in 1998, which raised their profile and credibility (Brooks et al. 2021, p. 47).

In sum, the first era of hacktivism signified itself by a strong ethical foundation characterized by non-violent forms of citizen resistance or protest, technological transparency, and digital rights. It is what Denning (2001) describes as hacktivism: "operations that use hacking techniques against a target's Internet site with the intent of disrupting normal operations but not causing serious damage" (p. 241). Groups during the first era were generally ideologically aligned in cyberlibertarian or anti-authoritarian motivations, in their advocating for freedom of information, privacy, and a form of resistance against local or corporate states. Their tactical means, like either FloodNet's browser-based protests, L0pht's security disclosures, or the CDC's exchanges of software to privilege individuals' privacy, were all focused more on being aware and empowered. Organizationally, many operated openly, and actively sought to disavow criminal hackers. The legacy of those participating in the first era was their influence on later generations of hacktivists, and the conceptual and moral authority it established when hoisting upon the practice of hacking through political engagement expressed as social action. These hacktivists' symbolism was strong although their operational disruption was weak, leaders from this era were, along with others, were credited for legitimizing cyberspace as a space for activism and resistance, at least until their later citations became crime.

1.2.2 Mid-2000s hacktivism Embracing Disruption and Spectacle

The second era of hacktivism that emerged in the mid-2000s and peaked in the early 2010s marked a significant shift in both tone and tactics (Romagna, 2020, p. 762). Unlike the relatively ethical and transparent approach of earlier hacktivist collectives, this era was defined by decentralized, anonymous groups that embraced disruption, spectacle, and mass participation (Sauter, 2014, p. 67). Members of the hacktivist collectives of this phase such as Anonymous, LulzSec, and AntiSec remained at least initially anonymous (Pendergrass & Morris, 2012). These actors engaged in significantly more disruptive and sophisticated operations, including distributed denial of service (DDoS) attacks, leaks, defacements and other types of system compromises. Both the mandates and actions taken by these collectives were still mostly driven by ideological aims that were primarily reactively rather than proactively socio-political in intent, responding to perceived transgressions in politics, business, or global affairs (Yang, 2013, p. 55). This phase of hacktivism was also deeply engaged in internet culture, and blended political messaging with satire and trolling, and something followers called "the lulz" (Richards & Wood, 2018, p. 189). This form of hacktivism is what Murdoch (2010) refers to as "destructive digital activism" (p. 138).

Hacktivist collectives of this era such as Anonymous, LulzSec, and TeaMp0isoN operated with a fairly wide ideological framework and focused on opposing censorship, the state, and corporate power. Anonymous, a collective that emerged out of the message board 4chan.org, started in 2003 by Christopher Poole as a message board to talk about pop culture activities (Özçelik & Brooks, 2020, p. 61). It operates with fluid and heterogeneous political worldviews that reflect a blend of anarchism, liberalism, communism and libertarianism (Singer & Friedman, 2014, p. 84). The core tenets of the group are fighting for transparency and accountability, and the free flow of information. Anonymous is fundamentally against internet censorship and advocates for privacy rights, and promotes freedom of speech and access to information (Mejia, 2017). Their actions are seen as both activism and satire, with early actions centered around "the lulz," which was a type of transgressive humor meant to increase contradictions rather than intended to amuse (Alexopolou & Pauli, 2021, p. 242). The increased access to and use of social media, internet forums, and real- time communication tools was essential not only for the way these collectives operated, but also their motives. Anonymous was initially known for online pranks, but then underwent a transformation, shifting the focus towards political activism (Pendergrass & Morris, 2012).

LulzSec, a hacktivist collective formed in early May 2011 as a branch of the group Anonymous, similarly started with seemingly no political ramifications (Snyder, 2022). The name merged "Lulz" (internet-speak for "laughing out loud") and "Security," which indicates the group's intent to mock victims whilst revealing flaws in security systems (Murphy, 2011). LulzSec openly positioned itself as an antagonist to state repression, corporate elitism, and censorship whilst supporting WikiLeaks and Bradley Manning (Pendergrass & Morris, 2012, p. 135). After initially seemingly having no political intentions, the collective later participated in political activism through their joint efforts as part of Anonymous in "Operation AntiSec" (Yang, 2013, p. 51). LulzSec operated as a group with both political aims such as opposing government control, corporate power, and censorship as well as satirical intent to mock the online security scene and provide entertainment. While their methods weren't strictly defined by ideology, they presented themselves as fighting against oppression and for online freedom (Pendergrass & Morris, 2012). TeaMp0isoN had a political agenda, specifically concerning who they considered enemies of muslims, which played a role in deciding who they targeted. The collective presented itself as pro-Palestinian and pro-Kashmiri (Hamid, 2018). Junaid Hussain, the founder of TeaMp0isoN indicated that his political awareness stemmed from locating and watching videos of Muslim children being killed in Kashmir and Palestine (ibid.)

The rise of social media, internet forums, and real-time communication tools enabled hacktivist collectives of this era to coordinate large-scale digital protests, data leaks, and Distributed Denial of Service attacks (DDoS), with unprecedented speed and global reach (Sauter, 2014). LulzSec utilized many different technical methods, and their most frequent methods included DDoS, website defacements, and extraction and public release of data (Held, 2012). The collective used destructive methods while maintaining symbolic aspects of their operations by creating security breaches or ridiculous events with serious and satirical reactions (ibid.). Anonymous employs similar techniques such as DDoS attacks, website defacements, and data breaches, however, in a more politicizing context. Although many of their efforts may only be erecting brief disruptions, they blend performative and creative features of resisting and beginning (Mikhaylova, 2014). TeaMp0isoN staged varying levels of cyber attacks inside a sub culture- defacing websites, DDoS attacks and stealing personally identifiable information (Hamid, 2018).

The tactics of hacktivist collectives such as Anonymous, LulzSec, and TeaMp0isoN were often confrontational, theatrical, and provocative. LulzSec consistently sent out press releases and noted their operations on social media, adding taunts and jabs to its technical feats (Held, 2012). Although only active for a short period, LulzSec gained popularity quickly, hacking major corporations and government institutions (Pendergrass & Morris, 2012). The most common targets for LulzSec were government agencies, law enforcement, media, and big corporations (Held, 2012). Noteworthy targets included Sony Pictures Entertainment, the CIA's website, PBS, and various law enforcement databases (Yang, 2013). TeaMp0isoN was provocative and confrontational as exemplefied by their attack in April 2012 which was broadly publicized in the media. The group led a phone-based denial-of-service attack on the U.K. Counter Terrorism Command hotline (Hamid, 2018). TeaMp0isoN also stole data, including Tony Blair's personal contact data and launched a wide array of attacks against a variety of entities, including government agencies, corporations, and political organizations (Heffelfinger, 2013). They also coordinated with the ZCompany Hacking Crew in December 2010 to attack Facebook groups that were identified as Zionist, right-wing, and anti-Islamic (Hamid, 2018). Additionally, they attacked the English Defense League's website, which shows that they were primarily attacking organisations they deemed anti-Muslim.

Anonymous has targeted multiple entities and has often preferred pretext to governments and corporations as they face accusations of censorship and/or corruption (Machado, 2015). Some notable campaigns include: Operation Payback against financial institutions that blocked WikiLeaks to receive donations and operation against Tunisia releasing sensitive documents on the government and enhancing the flow of information internally and to the outside world (Gorham, 2015). They have faced-off against SCN (Church of Scientology), various state websites, and leading corporations (Mikhaylova, 2014). Anonymous selects targets reactively in response to perceived injustices rather than random selection (Coleman, 2013). Anonymous engages with the public perception of themselves through sophisticated means of media strategy. They construct technologically complex and professional videos to produce "small artworks" promoting their message. Within this "online art," is The Guy Fawkes mask which is an icon for Anonymous to not only serve the practical purpose of protecting their face but also enacting resistance to authority (Mikhaylova, 2014). They have a dual and complex public image as some people view them as "folk heroes" (Richards & Wood, 2018, p. 192) while other refer to them as "folk devils" (ibid., p.192). Anonymous embraces its complex public image, through spectacular actions and creative messaging (Mikhaylova,

2014). They seek out media attention as this allows their message to penetrate or go viral, but operate with necessary ambivalence so that they may retain some level of anonymity and unpredictability that foils categories or control (Alexopolou & Pauli, 2021).

As this era of hacktivism was deeply intertwined with internet culture, the hacktivist collectives blended political messaging with satire and trolling, and something followers called "the lulz." The hacktivist collective Anonymous emerged out of the message board 4chan.org, started in 2003 by Christopher Poole as a message board to talk about pop culture activities (Price, 2017). The name of the group was derived from the fact that 4chan's users were able to post anonymously, whereby 4chan assigned random numbers to users, instead of requesting registration with account information (Price, 2017). Anonymous attracted wide public attention in 2008 with their "Project Chanology," which signified the development of their political consciousness and their strategies for taking mass actions (Gorham 2015). LulzSecs campaigns typically centered on a certain theme, such as "Fuck FBI Friday" and "Operation AntiSec", which directed attention towards law enforcement and security bodies. As cheeky as they were, LulzSec described their activities to be "a duality: a lesson and some LOLs at the same time" (Murphy, 2011, p. 27). They framed it as exposing important security vulnerabilities while providing entertainment. Would people "rather have someone expose the hole and tell you your data was exploitable than have the criminals who already found the hole sit quietly and exploit your data?" (ibid., p. 26).

The organizational structure of hacktivist collectives of this era was mostly decentralized. Anonymous functions as leaderless, decentralized networks with no formal hierarchy or associations to specific geographic locations. They communicate on various channels including social networks, IRC channels and message boards (Mikhaylova, 2014). Coordination is in the form of a system where members propose operations, and they gain momentum when enough individuals agree with it. This free-flowing structure is intentionally loose, which members believe is critical for the group to function, or even survive (ibid.). Whereas Anonymous is decentralized, LulzSec was a more hierarchical organization, with six central members (Held, 2012). It was headed by an individual who went by the name of Sabu, and other notable members included Topiary (Public Relations), Kayla (botnets), T-Flow (website), Avunit, and Pwnsauce (Held, 2012). In many respects, LulzSec differed from their Anonymous origins in that they had a more structured approach to their organization, but LulzSec also maintained strong ties to the hacktivist community. LulzSec held a strong

Twitter presence (@LulzSec) and had their own website (lulzsecurity.com) protected by CloudFlare's security services (Held, 2012). Their structured brand of hacktivism came to a quick end when their leader was arrested and began cooperating with federal authorities (Held, 2012). The period of activity by LulzSec was short and intensive, but it changed the way that organizations think about cybersecurity within the new context of increasing digital activism and political resistance (Yang, 2013).

TeaMp0isoN, founded by Junaid Hussain when he was 15 years old (aka "TriCk"), consisted of eight hacktivists, most of whom were teenagers or young adults from the United Kingdom (Hamid, 2018). As Anonymous, TeaMp0isoN was decentralized, making tracking the individual members more difficult (Chopitea, 2012). The group body was assembled from members of several other hacking collectives and underground forums (Hamid, 2018). The timing of the group's activity is uncertain; the group was operational in some capacity between 2010 and 2012 (Heffelfinger, 2013). TeaMp0isoNs members were identified by pseudonyms such as MLT, Phantom~, C0RPS3, f0rsaken, aXioM, and ap0calypse (Hamid, 2018). The collective was public about its actions and engaged with the media. For example, when they attacked the EDL's website, they left messages acknowledging the attack and issues of extremism and terrorism, speaking to public about those issues. They had a high-profile presentation of their hacktivist work on social media when Hussain publicized their successful hacks of news agencies and political entities on Twitter (Hamid, 2018).

In sum, compared to the first era of hacktivism, the second era was significantly more visible and disruptive while also approaching these points from a different angle. Earlier forms of hacktivism were largely symbolic actions that attempted to retain ethical boundaries. In contrast, second-era hacktivists engaged in more confrontational actions with a larger reach. TeaMp0isoN, LulzSec, and Anonymous regularly designed their attacks to include data breaches and DDoS attacks or defacements that included an effective disruption of various government institutions, corporations, and law enforcement. Their motivations didn't stem from monetary gain or senseless destruction. Instead, these collectives were mostly motivated by political and ideological beliefs against censorship, for digital rights, and against institutional abuse. The hostility of their methods did not mean that they wanted to inflict permanent damage; in fact, in most cases, hacktivists were trying to organize embarrassment or coerced accountability from their respective targets and violent acts of their long list of targets. Even when performed as satire, trolling, or for "lulz", these hacktivist groups were

consistently opposed to centralized power, and specifics of their action were grounded in a politcally infused protest pattern. Money was never a concern as they sought public recognition for bedroom hacks. The decentralized and anonymous trait of these groups helped them be unpredictable, but they would also enable mass participation without formal recruitment. This era blurred the lines between protest and cybercrime; however, it was tied still to a form of digital resistance that, whilst increasingly disruptive, was based on a form of activist logic (Romagna, 2020).

1.2.3 Contemporary Age of Telegram-Based, Profit-Motivated Hacktivism

The digital landscape has been altered following recent geopolitical conflicts, such as Russia's full-scale invasion of Ukraine and the military tensions between Israel and Palestine, making it more vulnerable to cybersecurity threats (Varbanov et al. 2024, p. 2). Since the 24th of February 2022, Russian hacktivist groups like NoName057(16), Killnet, and CyberArmyOfRussia have carried out hacktivist operations, where the sense of digital disruption is targeted not simply from an ideological perspective, but a geopolitical one as well. The objective of these attacks is to exacerbate the uncertainty, psychological burdens, and stress on civilians in the countries supporting Ukraine (Tavakkoli et al., 2025, p. 13). These groups are centralized, have a nationalistic alignment, and position themselves strategically alongside Russian state narratives. They communicate and coordinate attacks mainly using the communication platform Telegram (Canevez et al. 2024, p. 169). Telegram's commitment to user privacy has positioned it as an attractive medium for individuals engaged in political dissent since it facilitates features such as end-to-end encryption and abstains from algorithmically mediated content (ibid.). The second era of hacktivism, as expained in the previous sub-chapter, represented a significant change in scale, visibility, and disruption. However, it was still fundamentally ideological resistance, distinct from state-based structures. This visible shift into platform-based hacktivism that is explicitly aligned with geopolitical maneuvers and is a form of quasi-governmental engagement since 2022 raises the following research question: In what ways does Telegram-based Russian hacktivism diverge from earlier forms of hacktivism in terms of motivations, methods, and operational logic?

While it remains true that some aspects of the third era are a continuation of second-era developments, as Romagna (2020) pointed out, the new type of hacktivism emerging after 2022 differs in terms of motivations and organizational basis. To deterimine if and how this new form of hacktivism is different from the two previous eras of the phenomenon, post-2022 Russian Telegram-based hacktivism will be compared to the predeccessors in terms of: first, the underlying motivation that drives hacktivist activity; second, target selection and malice; third, the type and technical sophistication of the cyber-attacks they employ and the degree of maliciousness, specifically, whether disruption is confined to institutional targets or also harms ordinary citizens; fourth, the channels and narrative strategies through which hacktivists communicate and legitimize their actions; fifth, the extent to which their operations are monetized through donations, services or other revenue streams; and sixth, the recruitment practices and organisational structures that bind participants into a collective. Understanding how this new form differs from more ideologically autonomous forms of hacktivism in each of the prior eras is critical to understanding the transformation of hacktivism and digital resistance in the current global landscape.

As this third era illustrates, Russian hacktivist groups on Telegram are not only geopolitically aligned, they are also highly performative. They are designed to create visibility, provoke a symbolic response, and amplify visibility, both in terms of the negative press they may generate domestically and abroad. They actively watch the representation of their actions in the press, and ascribe validity to media coverage as a measure of their own success. This media frame suggests visibility may become a driver of their strategic operations. If media attention is considered a form of legitimacy, or a product itself, then it is conceivable that countries that more strongly report on these groups will also increase their risk of becoming a target. The second research question guiding this thesis is, therefore, to what extent does domestic media coverage influence the frequency of cyberattacks claimed by Russian hacktivist groups?

2. Methodology

The starting point of this thesis lies in the growing challenge posed by Telegram-based hacktivism. Escalating geopolitical conflicts, notably Russia's full-scale invasion of Ukraine and tensions in the Middle East, have intensified cybersecurity risks across the digital landscape (Varbanov et al. 2024, p. 2). This thesis argues that immediately following Russia's full-scale invasion of Ukraine, a new type of hacktivism began to evolve. Hacktivist groups started to use platforms like Telegram to share information about their plans for cyberattacks or to announce when they've successfully carried one out (Canevez et al., 2024, p. 169). Using Telegram as the primary forum, these Russian hacktivist groups began to operate in a quasi-organized and semi-structured manner to launch major cyber campaigns against European countries that expressed support for Ukraine. These attacks directly affected public life and state operations in the targeted countries, leading to questions on the resilience of critical infrastructure and of the average citizen (Guchua & Zedelashvili, 2023, p. 35). Given the growing impact of cyberattacks on daily life, making their effects tangible even to the average citizen, there is a notable gap in the academic literature on Russian hacktivist groups.

The problem addressed in this thesis, therefore, is twofold: first, to understand the characteristics and dynamics of post-war Russian hacktivism as a distinct phenomenon; and second, to examine the strategic role of media visibility in the targeting decisions of contemporary Russian hacktivist groups. To address these objectives, the thesis employs a mixed-method design that integrates both qualitative and quantitative approaches to data collection and analysis (Maggetti, 2020, p. 194; Harbers & Ingram, 2020). The integration-based mixed-method design allows to explore the phenomenon of post-war hacktivism using qualitative methods by focusing on the organizational structure and operational logic of Russian hacktivist activities conducted via Telegram. Furthermore, it enables to test if media visibility affects the frequency of cyberattacks using a quantitative approach. This research design was chosen because it adds analytical depth to the thesis by capturing the phenomenon itself as well as the dimensions of post-2022 hacktivist behavior (Maggetti, 2020, p. 198).

The first part of the empirical analysis adopts a qualitative and exploratory approach. To understand the phenomenon of Telegram-based Russian hacktivism, it is first necessary to explain how these hacktivist groups operate, communicate, and select targets. This will be achieved by contrasting their characteristics from their predecessors, which scholars have often described as decentralized, with strong ideological underpinnings and anti-

establishment stances (Karagiannopoulos, 2018, p. 15). This first part of the empirical analysis does not aim to test causal relationships but to conceptually and empirically describe the patterns and logic that define Russian hacktivist activities on Telegram. The analysis is based on primary data collected firsthand. Using thematic coding and qualitative interpretation, it aims to identify recurring patterns in group communication, organizational structures, and target selection.

The second part of the empirical analysis adopts a quantitative and explanatory approach to assess the relationship between media visibility and the frequency of cyberattacks. Unlike the first part of the analysis, which focused on conceptualizing the phenomenon of Telegram-based Russian hacktivism, this part moves towards systematically analyzing the interaction between two observable variables: national media coverage (independent variable) and cyberattack frequency (dependent variable). The hypothesis is that higher levels of domestic media attention may increase a country's symbolic significance for Russian hacktivist groups, encouraging them to conduct more frequent attacks. This part of the analysis is thus oriented toward detecting whether patterns in media reporting correspond with variations in targeting intensity across different states and time periods. To test this, two original datasets were compiled. The first documents the cyberattacks claimed by Russian hacktivist groups, while the second records media mentions of these groups in national news outlets across most frequently attacked member states of the European Union. Each dataset was aggregated by country and by date, creating a unified structure that allows for cross-national and longitudinal analysis. While this approach cannot determine causality with certainty, it enables the identification of possible explanatory patterns. Through this method, the research aims to evaluate whether national visibility in media narratives plays a measurable role in shaping hacktivist targeting behavior. If being mentioned in national media attracts Russian hacktivists' attention, understanding this dynamic becomes crucial for mitigating future attacks.

Given the two distinct analytical objectives of the thesis - first, to explain and conceptualize the phenomenon, and second, to test whether media visibility correlates with attack frequency- the methodology is structured in two parts. Each part corresponds to one of these aims. Both parts make use of original, first-hand collected data. In the first part, the level of analysis is organizational, as it focuses on Russian Telegram-based hacktivist groups. In the second part, the level of analysis is state level as it focuses on variations in cyberattack frequency between states in relation to their national media visibility. This observation period

was chosen because November 2023 marked the beginning of the research, when the initial thesis idea was developed and systematic monitoring of Telegram-based hacktivist activity began. February 2025 was selected as the endpoint after a sufficient volume of data had been collected to support both the qualitative and quantitative components of the analysis.

2.1 Qualitative Analysis - Understanding Telegram-Based Russian Hacktivism

The first part of the thesis uses qualitative methods to explore the phenomenon of Telegram-based Russian hacktivism. This approach is appropriate given the study's aim to understand the internal logics, communication patterns, and organizational characteristics of these groups, which remain underexplored in existing literature. The purpose of this qualitative stage is both exploratory and conceptual. It seeks to describe, interpret, and categorize the key practices and organizational forms that define contemporary Russian hacktivist groups.

2.1.1 Case selection

Telegram-based Russian hacktivist groups that were notably active during the period of November 2023 to February 2025, the time period chosen in the empirical analysis, formed the basis for the case selection. These groups were treated as the empirical units of analysis. The selection was based on criteria such as public activity on Telegram, alignment with pro-Russian geopolitical narratives, and regular publication of cyberattack claims that are targeted against Ukraine and its allied countries. To monitor Russian hacktivist Telegram channels, a personal Telegram account was created and used to manually track the activity of relevant groups in real time. This gave continuous access to posts, announcements, and claims of attacks across the monitored channels. The hacktivist groups were selected using the non-probability form of the snowball sampling (Heckathorn, 2011, p. 356), which allows for the identification of affiliated actors. It is a suitable method for this thesis since the phenomenon of Russian hacktivism has limited publicly available information (Dosek, 2021, p. 651).

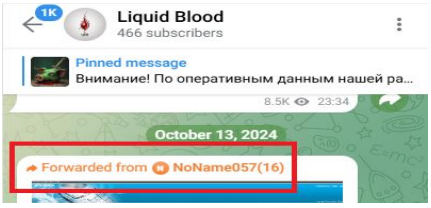

Figure 1. Example of channel discovery through forwarded Telegram posts. E.g, Russian hacktivist channel Liquid Blood forwards a message from NoName057(16). By clicking on the "Forwarded from" tag, the user is redirected to NoName057(16) Telegram channel.

The first step was to identify the most popular and widely recognized Russian hacktivist channels at the time, namely Killnet and NoName057(16), which were already known beyond the Telegram environment (Guchua & Zedelashvili, 2023). These channels served as the initial entry points for identifying further Russian-language hacktivist groups, using cross-posts, mentions, as illustrated in figure 1, and shared alliances to expand the list of monitored channels. The Russian hacktivist groups were continuously monitored for cyberattack-related activities from November 2023 to February 2025. The snowball sampling method applied over the 16-month period resulted in a final list of 48 Telegram-based Russian hacktivist groups: KillNet, CyberArmyofRussiaReborn, ZulikGroup, Server Killers, KREBS SPYEYE BOTNET, Passion Botnet, UserSec, Anonymous Russia, 62IX, DDoS Legion, Phoenix, CryptHades, Bluenet Russia, NoName057(16), Layer Legion, Passion Botnet V2, NashDDoS, CyberDragon, SkillNet, 22C, Ancient Dragon, Akesha, Digital Revolt, FastNet, KaliHunt/Russia, KillNet 2.0, Lionheart, Nightmare, Sapphire Rus Clan, Evil Empire, HackNet, Holy Order, BloodNet, High Society, Hunt3r Kill3rs, Matryoshka, Autodafe Internet, OverFlame, Russki Zadacha Sila, Virtual Barrier, EvilWeb, Hurricane-17, Liquid Blood, Russian Task Force, KyberVoiska, Z-Pentest, Re:Volix, TwoNet.

2.1.2 Data collection and analysis

Once relevant Russian hacktivist groups were identified, all of their posted content was read through manually and documented over the course of the chosen time period. This included announcements of cyberattacks, ideological statements, recruitment messages, advertisements, and posts containing propaganda, threats, or alliance declarations. The content was manually categorized using a personal Telegram account, allowing for real-time tracking of each group’s activities. The analysis followed a manual thematic coding process, designed to identify and interpret recurring patterns across the observed content. Codes were developed iteratively and grouped into a structured framework based on the following six categories: motivation, target selection and justification, attack type and technical sophistication, monetization, recruitment, and organizational structure. These categories, drawn from both theoretical considerations and inductive observations, served as the foundation for comparing Telegram-based Russian hacktivism with earlier generations of hacktivist activity:

For the ***motivation*** category, content was coded based on explicit statements of purpose or justification for attacks, including patriotic rhetoric, anti-Western or anti-NATO framing,

alignment with Russian state interests, ideological slogans, and references to defending the "Motherland" or retaliating against perceived enemies of Russia, as illustrated in figure 2.

Figure 2. Example of motivation framing by the hacktivist group WE ARE BLOODNET. In their Telegram channel, the group describes its mission as targeting "NATO | Europe Countries | Traitors to the country" and presents itself as a "pro-Russian pentester team working for the benefit of the Motherland."

For ***target selection and justification***, all posts in which a cyberattack was announced were systematically reviewed to analyze the types of targets selected by Russian hacktivist groups. Each claimed attack was logged in a structured Excel dataset that served both the qualitative analysis of target logic and the quantitative correlation study in the second part of the empirical analysis. Where groups provided justifications alongside their attack claims, such as retaliating for military aid to Ukraine or political statements like illustrated in figure 3, they were coded to trace how target selection was linked to specific geopolitical developments or perceived provocations.

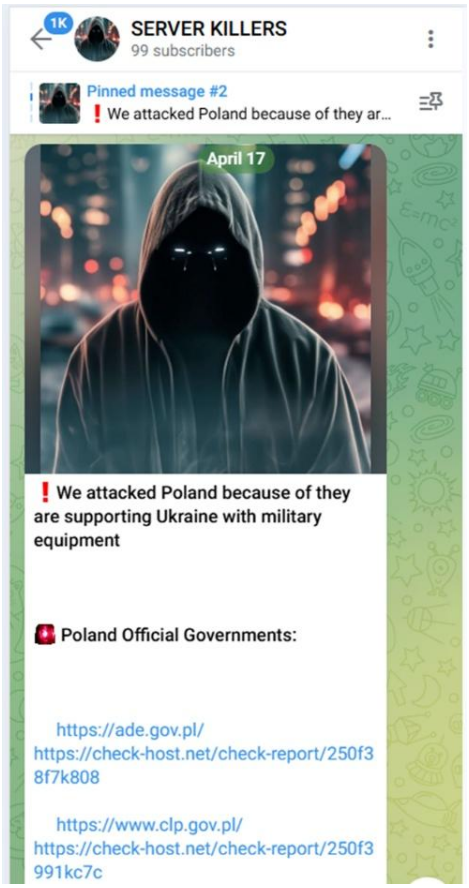

Figure 3. Example of a list of attacked targets posted by russian hacktivists, as well as justification for said attacks. The group SERVER KILLERS explains that its attack on Polish government websites was a direct response to Poland's military support for Ukraine.

In addition to tracking the types of targets selected and the justifications provided, the analysis also considered the overall presence of destructive intent behind the attacks. This was assessed by examining whether the cyberattacks were limited to governmental institutions such as ministries and conglomerates such as tech corporations or extended to civilian-facing infrastructure, including hospitals, banks, energy companies, transport systems, postal services, and media outlets. Attacks on essential services were coded as highly malicious, given their potential to disrupt everyday life and harm ordinary citizens, rather than solely targeting state functions. This dimension helped differentiate between symbolic targeting and more disruptive forms of cyber aggression.

For the ***attack type and technical sophistication***, each announced cyberattack was categorised based on the type of evidence attached to the post. Attacks were classified as DDoS when accompanied by links to external uptime monitoring services such as check-host.net, which showed the targeted websites as unavailable. Defacement attacks were identified through the inclusion of screenshots and direct links to visibly altered websites.

Data leaks were coded when posts contained leaked information or documents, along with a claim of access to the victim's system and a link to the breached source. These indicators provided a consistent method for categorizing the type of attack. The technical sophistication of each group's operations was then assessed by examining the proportion of each attack type. Since DDoS attacks require minimal technical skill, especially when using pre-configured botnets, they were considered the least sophisticated. In contrast, successful defacements or data breaches suggest a higher degree of skill, involving vulnerability exploitation or deeper system access. Therefore, the relative frequency of defacement and data leak posts compared to DDoS attacks served as a proxy for evaluating the groups' technical capabilities.

For the ***monetization*** category, content was coded whenever hacktivist groups engaged in financial activity through their Telegram channels. This included appeals for cryptocurrency donations, often framed as support for patriotic hacking efforts; advertisements for malicious services, such as DDoS-for-hire botnets or access to compromised systems; and promotion of tools, including botnets, exploit kits, or defacement utilities. These kinds of activities would reveal that Russian hacktivists are not solely driven by ideology but also by financial gain, blurring the lines between hacktivism and financially motivated cybercrime. Posts were reviewed for pricing information, wallet addresses, contact instructions, and transactional language to determine the presence and extent of monetization strategies.

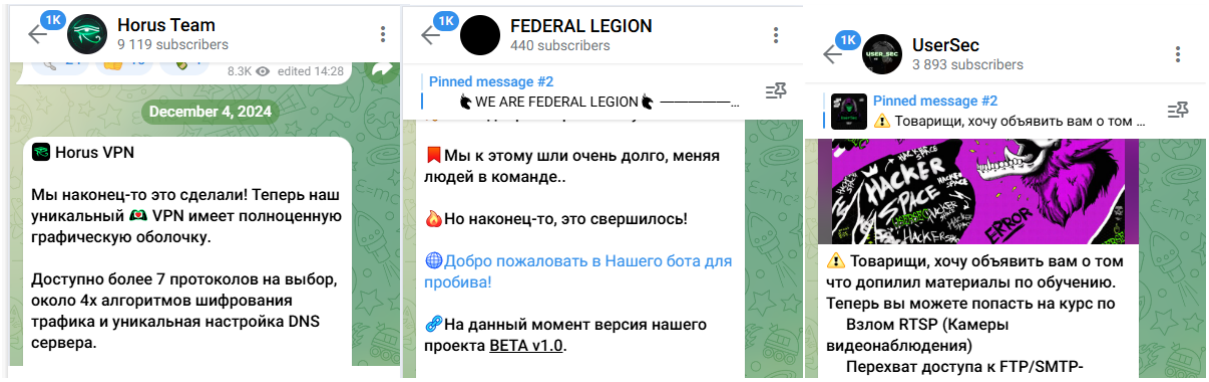

Figure 4. Examples of monetisation strategies by Russian hacktivist groups. Horus Team advertises a custom VPN service, Federal Legion promotes access to a data-extraction bot, and UserSec offers paid hacking courses.

For the ***recruitment and organizational structure*** category, content was coded when groups publicly advertised open positions, posted calls for volunteers, or described their internal organizational processes. The use of public Telegram channels for recruitment stands out, as

it differs from earlier hacktivist traditions, where entry was typically informal or assumed through ideological alignment. While anonymity remains preserved for individual members, the structured and open nature of these recruitment efforts may signal an evolution in how participation is formalised and roles are distributed within Telegram-based hacktivist collectives. This dimension was included to examine whether such practices reflect broader shifts in organisational strategy.

2.2 Quantitative Analysis - Media Visibility and Cyberattack Frequency

While the first part of the empirical analysis focuses on explaining Telegram-based Russian hacktivism as a phenomenon, the second part aims to investigate whether national media visibility plays a role in determining the frequency of cyberattacks by Russian hacktivist groups. Based on the assumption that these groups are highly performative and visibility-driven actors, it is expected that being mentioned in national media may serve as an incentive for attacks. This part of the analysis combines two original datasets: one documenting cyberattacks conducted by Russian hacktivist groups and another recording national media mentions of these groups across selected European Union countries. By comparing the level of media attention with the number of attacks each country faced during the selected time period, this part of the analysis seeks to determine whether there is a correlation between visibility and targeting.

2.2.1 Case selection

The selection of cases for this part of the analysis followed a step-by-step process designed to ensure both relevance and comparability. Importantly, the data used in the quantitative analysis was drawn directly from the cyberattack dataset compiled during the qualitative stage of the research. All cyberattacks were originally gathered through systematic monitoring of the same 48 Russian Telegram-based hacktivist groups analyzed in the first part of the empirical analysis. Therefore, the selection of targeted countries in this part is consistent with the qualitative methodology, ensuring methodological continuity between both parts of the study. First, the global dataset of recorded cyberattacks was created to identify the countries most frequently targeted by Russian hacktivist groups. From that, non-European Union countries were excluded, which resulted in the final list of the most attacked European Union member states.

This approach ensured that the analysis included countries relevant to Russian geopolitical narratives while also maintaining comparability through shared characteristics such as similar media environments and EU membership. Specifically, the analysis includes all EU countries that were among the most attacked overall, taking every country down the list until reaching Estonia, which was deliberately included as the final case. Estonia was retained not only because it fits within the ranking of frequently targeted EU countries, but also because it serves as a theoretically meaningful contrast case. Despite its geopolitical significance as a vocal supporter of Ukraine and its well-known role in cyber defense, Estonia appears to receive relatively limited media coverage of Russian hacktivist groups within its domestic media sphere. Its inclusion thus provides an opportunity to explore whether lower levels of visibility in national media may correspond with different patterns of targeting, without making assumptions about the outcome in advance. Ukraine, although the most frequently attacked country overall, was excluded from the analysis. Its exceptional status as the primary target of Russian aggression means that attacks against it are politically motivated by default, rather than influenced by variations in national media coverage. Including Ukraine would therefore risk distorting the hypothesis testing.

2.2.2 Data collection and analysis

This part of the empirical analysis makes use of two datasets. The first dataset is the ***cyberattack dataset,*** which was compiled during the first part of the empirical analysis. As explained in chapter 2.1, it is based on continuous, manual, first-hand monitoring of 48 Russian-language Telegram hacktivist groups. These groups were tracked daily between November 2023 and February 2025 using a personal Telegram account, allowing real-time observation of their activity. Every time a group publicly announced a cyberattack, the incident was manually recorded and entered into a structured Excel dataset. The following details were logged for every incident: the date when the cyberattack occurred, the targeted website, the type of cyberattack (DDoS, defacement, or data leak), and the country to which the targeted website belonged. Country attribution was determined based on the website's top-level domain (e.g., .de for Germany, .fr for France).

The most pertinent data points derived from the dataset for this section of the empirical analysis included the specific date of each cyberattack and the country attribution of the targeted website. These two data points served as the basis of the operationalization of the dependent variable: the daily count of cyberattacks per country. Country attribution was

determined using a two-step method: websites with country-code top-level domains (e.g., .pl, .de, .fr) were directly assigned to the respective countries, while websites with generic top-level domains (e.g., .com, .net) were attributed based on their hosting location. This was achieved using a custom-built script, which is shown in appendix 1, that identified the server's physical location.

The group NoName057(16) constitutes a notable exception within the cyberattack dataset. In contrast to other Russian hacktivist groups that routinely publish detailed attack claims on their Telegram channels, NoName057(16) only shares a small portion of their daily activity. This discrepancy is explained by their use of a custom-developed, crowdsourced DDoS infrastructure known as DDoSia, which enables a large number of voluntary participants to contribute computing power to execute attacks. The operational model involves a chain of command-and-control (C2) servers, through which a centralised list of daily targets is disseminated to all botnet members. Participants receive these target lists via a downloadable client that connects to the infrastructure and automatically initiates DDoS attacks against designated websites.\n\n> To account for this unique structure and avoid underrepresentation of NoName057(16)'s activity, access to the DDoSia system was obtained for passive observation. The client was configured in such a way that it retrieved the target list without launching any attacks, allowing for full daily logging of the group's intended targets while ensuring no direct engagement in malicious activity. This non-intrusive method allowed for a more accurate reflection of NoName057(16)'s targeting behaviour. The structure and flow of the botnet's task distribution process is illustrated in Figure 5, which demonstrates how target instructions are relayed from the group to the distributed network of botnet participants.

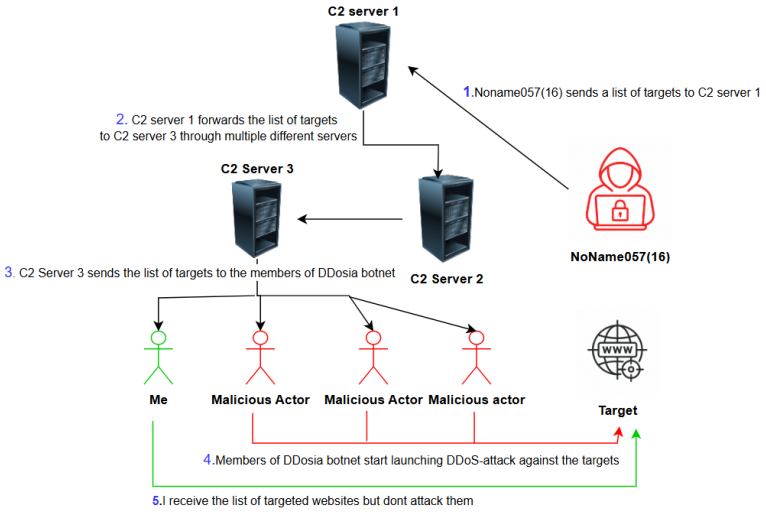

Figure 5. Illustration on how NoName057(16) group's crowdsourced botnet works

The result of this data collection and selection process was a comprehensive dataset showing the frequency of cyberattacks against each country on a daily basis. From this dataset, it was possible to identify how many times a specific country was targeted throughout the established time period of this thesis. First, countries with the highest number of cyberattacks were identified. As explained in the previous sub-chapter the list was narrowed to include only member states of the European Union (EU) member states by proceeding down the global ranking of most frequently attacked states until Estonia was reached.

The second dataset is the ***media-visibility dataset***. After identifying the most attacked EU member states up to and including Estonia based on the cyberattack dataset, the second dataset consisting of national media coverage on Russian hacktivist groups in each of those countries was compiled. For every selected country, a targeted search was conducted to identify media articles that mentioned Russian hacktivists. To ensure a consistent approach for the detection of relevant articles, four criteria had to be fulfilled. First, the article had to be published in the national language of the respective country or in a recognized minority language widely spoken within that country, for example, Russian in Estonia and Latvia, Catalan in Spain. Second, the article needed to explicitly mention Russian hacktivist groups, either by name (e.g., Killnet, NoName057(16)) or through general references (e.g., “Russian hackers”), regardless of whether the attack discussed was directed at the country in which the article was published. Third, only articles published on media websites using the national top-level domain (TLD) of the country were included (e.g., .pl for Poland, .lt for Lithuania). This restriction was applied to ensure that the articles reflected domestic media coverage, rather than syndicated or international reporting, and to allow for a more accurate comparison of national media ecosystems. Fourth, only articles published during the established time period of the thesis from November 2023 to February 2025 were considered for inclusion in the dataset.

To collect relevant media articles, a systematic keyword search was conducted for each of the selected countries. The search relied on a two-tiered keyword strategy. First, it included the names of all 48 Russian-language hacktivist groups that were monitored during the established time period. These included, among others: KillNet, CyberArmyofRussiaReborn, ZulikGroup, Server Killers, KREBS SPYEYE BOTNET, Passion Botnet, UserSec, Anonymous Russia, 62IX, DDoS Legion, Phoenix, CryptHades, Bluenet Russia, NoName057(16), Layer Legion, Passion Botnet V2, NashDDoS, CyberDragon, SkillNet, 22C, Ancient Dragon, Akesha, Digital Revolt, FastNet, KaliHunt/Russia, KillNet 2.0,

Lionheart, Nightmare, Sapphire Rus Clan, Evil Empire, HackNet, Holy Order, BloodNet, High Society, Hunt3r Kill3rs, Matryoshka, Autodafe Internet, OverFlame, Russki Zadacha Sila, Virtual Barrier, EvilWeb, Hurricane-17, Liquid Blood, Russian Task Force, KyberVoiska, Z-Pentest, Re:Volix, and TwoNet. Second, a set of generalized search terms was used, including the phrases “Russian hacktivists” and “Russian hacktivist” translated into both the national language and, where applicable, a relevant minority language (e.g. Russian in Estonia and Latvia; Catalan in Spain). These searches were performed using a combination of open-source media aggregators, country-specific search engines, and direct queries on national news websites.

Once relevant media articles were identified, they were logged in a separate Excel sheet to form the media-visibility dataset. For each article, the following attributes were recorded: the date of publication, the URL of the article, the source domain, the country in which the article was published, and the language in which it was written. In the context of the quantitative analysis, the most important attributes were the date and country of each article, as these were used to cross-reference the media dataset with the cyberattack dataset on a country-date basis, allowing for structured comparison and correlation analysis.

2.3 Limitations

A primary limitation of this research lies in the data collection process, impacting both the qualitative and quantitative components of the thesis. The thesis draws on comprehensive and systematically collected first-hand data. In relation to the qualitative analysis of Telegram-based Russian hacktivism, one important limitation concerns the volatility and instability of Telegram channels. Over the course of the time period from November 2023 to February 2025, many groups were banned, removed, or migrated to new channels, making long-term observation of some actors difficult. Although efforts were made to continuously track and archive content using threat intelligence tools and public repositories, it is likely that certain communications and developments were lost. The datasets in the quantitative analysis are also subject to some limitations. Although the datasets are comprehensive, certain media articles became unavailable during the study due to removals or paywalls. Although metadata was retained, gaps in full-text availability may have affected the precise measurement of media visibility in some cases.

While the application of a mixed-methods design, combining qualitative and quantitative approaches, enables the thesis to address both the both the nature of Russian Telegram-based

hacktivism and its relationship with media visibility, there are certain limitations that need to be addressed. As with all qualitative research, the analysis is interpretative in nature and therefore, influenced by researcher judgment (Denzin & Lincoln, 2018, p. 58). While coding and thematic interpretation were conducted systematically, and supported by first-hand recruitment experiences to enrich understanding, qualitative analysis inherently involves subjective decision-making and makes generalizability difficult. Regarding the quantitative approach, while correlation and pattern analysis were used to identify associations between media coverage and cyberattacks, the design does not allow for definitive claims about causality. Although temporal sequencing and cross-national patterns were explored, many other factors, such as geopolitical events or local political dynamics, may also have influenced targeting decisions by hacktivist groups. Finally, in the process of attributing attacks to specific countries, reliance on top-level domains and server hosting information introduces the potential for misclassification in ambiguous cases, although every effort was made to ensure consistent and reliable coding.

3. Empirical Analysis – Part I

This part of the empirical analysis explores if and to what degree Russian hacktivism after 2022 is a distinct manifestation of the third era of hacktivism. As elaborated in chapter 1.2.3, the third era is characterized by alignment to the state, performativity in the media, and greater financial motivation as an outcome of the liberalization of the underground marketplace. The findings of the qualitative analysis show that several post-2022 hacktivist groups employ similar stylistic and organizational aspects as hackivist collectives of the second era in terms of the use of social media platforms, the creation of a performative spectacle, similar hacking techniques and a loosly collectivist theme. However, the post-2022 Russian hacktivist groups differ from previous forms of hacktivism in their underlying motivations, form of operation and strategic alignment. While the second-era hacktivist groups of the mid 2000s to mid-2010s were ideologically driven and largely decentralized, contemporary Russian hacktivist collectives are auxiliary actors to Russia's information warfare capabilities.

The findings of the qualitative analysis show that post-2022 Russian hacktivism has a two-pronged nature meaning that the hacktivist groups are highly reactive to geopolitical events while acting as economically pragmatic opportunitists. They earn money through their public cyber attack activities with such methods as fundraising, selling malicious services through advertising, offering cyber attack for hire services or providing various hacking courses. This dual nature of the Russian hacktivist collective iterating patriotic or ideological rhetoric, with financial profit seeking behaviour makes it different from previous understandings of hacktivism. Despite differences in ethical codes and occasional internal fragmentation, hacktivist groups before 2022 tended to operate under the collective idea of rejecting financial means as motivation (Chopitea, 2012).

Post-2022 Russian hacktivism, emerging after the full-scale invasion of Ukraine, marks a shift from earlier earlier Russian aligned cyber actors who operated in a co-opted mode were ideologically or protest-driven. Prominent new groups like Killnet and CyberArmyOfRussia, while promoting Russian state narratives, also openly profit through donations, data sales, and DDoS'ing as a service. Their use of patriotic rhetoric, financial compensation, and public propaganda represent a departure from the earlier forms of hacktivism. Post-2022 Russian hacktivism is therefore best characterized as a hybrid. The rhetoric is ideologically based, but the methodology is strategically pragmatic and financially opportunistic. The analysis

confirms that its emergence represents an appreciable evolution in the hacktivism narrative: a combination of symbolic protest with cyber crime and embedded propaganda.

The qualitative analysis is structured as follows. First, it is examined how Russian hacktivists select their targets and the justifications they offer, showing how their reactive campaigns differ from ideologically consistent targeting seen in earlier hacktivist generations. Second, the main types of cyberattacks conducted - namely DDoS attacks, defacements, and data leaks are categorized and evaluated. An assessment of how their tactical use aligns with broader strategic and symbolic goals follows. Third, an exploration of how Russian hacktivist groups use Telegram to coordinate, publicize, and amplify their activities, highlighting the performative and communicative dimensions of their campaigns will be conducted. This is followed by, fourth, an analysis of how these groups monetize their activities, offering services for profit and blending political rhetoric with economic incentives . Finally, a detailed overview of the recruitment processes in how they are organized within these collectives, showing how structured entry requirements and task-based onboarding distinguish them from the more open and spontaneous models of earlier hacktivism, will be given.

3.1 Target selection and grounds for justification

One of the defining characteristics of post-2022 Russian hacktivism is the semi-random selection of targets and the narratives that justify their cyberattacks. As elaborated in subchapters 1.2.1 and 1.2.2, hacktivist groups selected targets based on specific ideological causes or reasons for protest, such as government transparency or digital freedom. Post-2022 Russian hacktivist groups directly select targets aligned with their country’s geopolitical aspirations, meaning that any country or an institution that criticizes Russian invasion in any way might become a taregt for their cyber attacks. Thus, Russian hacktivists target selection is aligned with a combination of political, economic and psychological warfare, where their intention is to hamper the adversary, spread propaganda, or divert attention from realities, reinforce the perception of Russia’s cyber capacity. This kind of target selection is in most cases reactionary - whereas state-agent sponsored cyber units will often have a multi-staged planning or approach and often set long-term strategic objectives, the Russian hacktivist groups mostly respond and select targets based on geopolitical developments. This reactionary element made their operational attacks very much reinvested and event driven, and the countries would suddenly become the high-scale targets when those countries made

their political, military aid, or diplomatic deeds against Russia.Russian hacktivist organizations closely follow major international news, and government statements and policy changes as triggers for attack campaigns. In most cases, their response cycle proceeds somewhat as follows, (an example is provided below of a timeline of an attack campaign).

1. **Trigger Event – Latvia Pledges Support to Ukraine**

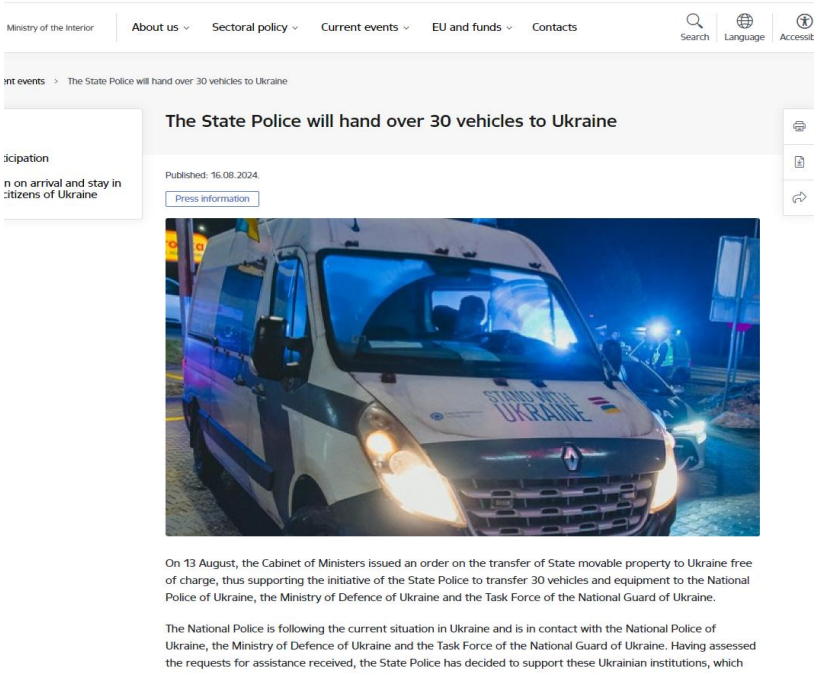

Figure 6. Latvia's Ministry Of Interior announcing their donation of 30 vehicles to Ukraine.

Figure 6. shows an official announcement from the Latvian Ministry of the Interior, stating that Latvia will donate 30 vehicles to Ukraine. This decision, made on August 13, 2024, aligns with ongoing Western support for Ukraine and represents a tangible contribution to Ukraine's law enforcement and defense efforts.

2. **News Reaches Russian Media**

Figure 7. Russian media outlet gazeta.ru article about Latvia donating vehicles to Ukraine

The second image, shown in figure 7, is from a Russian-language news outlet reporting on Latvia's decision. Once such news circulates in Russian media, it often serves as a catalyst for hacktivist groups to take action, portraying the support as a hostile move against Russia. The framing of the news report often aligns with Kremlin narratives, reinforcing the idea that

Latvia is aiding "Ukrainian terrorists" or engaging in anti-Russian activities.

3. Russian Hacktivist Group Picks Up the news and attacks the country

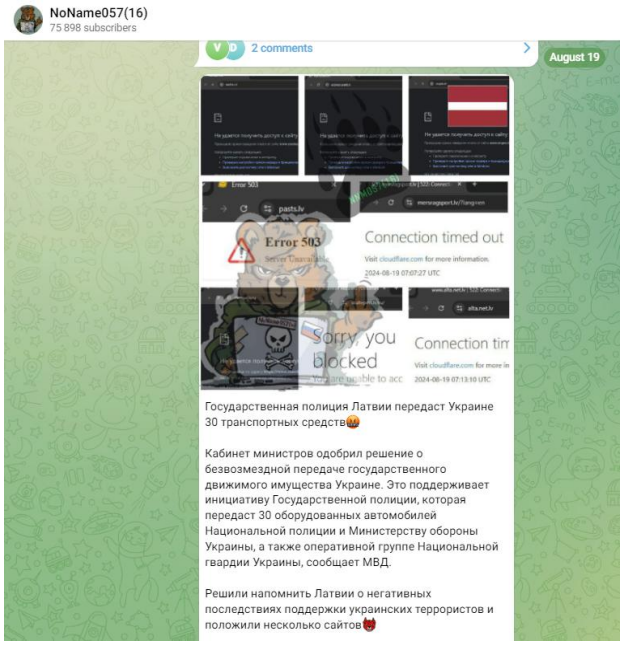

Figure 7. NoName057(16)" posting screenshots of Latvian sites that thye claim to have taken down, paired with a Russian-language message claiming the attacks are punishment for Latvia's decision to donate 30 police vehicles to Ukraine.

Figure 8 is a Telegram post from the Russian hacktivist group NoName057(16) about Latvia's donation of vehicles as a reason to begin launching attacks. The group clearly states that Latvia will be a target because Latvia is supporting Ukraine. They share, including sections of disrupted websites, proof of their cyberattacks on Latvia, including error messages, downtime indicators and offensive messages (figure 9).

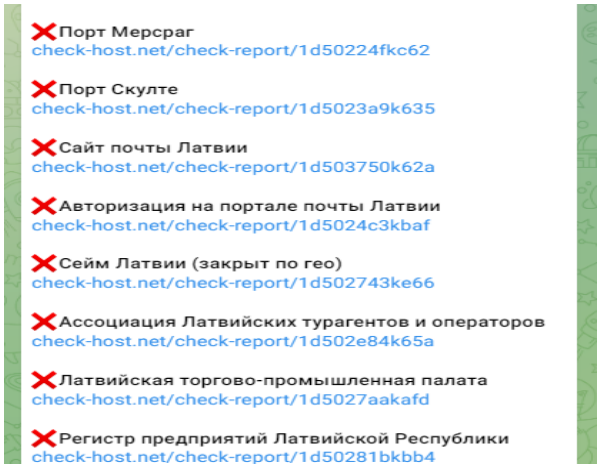

Figure 8. NoName057 posting check-host links to prove that they have taken down Latvian sites.

Russian hacktivist group do not only target military, government, or economic targets. A major part of their cyberattack strategy involves targeting the sectors that maintain essential services for civilians. By attacking these targets, or regions, they can maximize disruption, cause mass inconvenience, and enhance fear. In other words, they intentionally attack those services needed by "common people", banking, transport, postal, and also internet functions. By focusing on these services, they can create humanitarian pressures, erode the public's faith in their governments, and make sure their attacks are widely reported.

Apart from public sector websites, the financial sector is one of the most popular targets for Russian hacktivists. Disruption of national banks, online banking services and credit card transaction services, leads to financial instability and maximum disruption to transactions in the system's functioning, leaving regular citizens frustrated and unable to access their own funds. Besides the financial sector, hacktivist groups regularly target transport network infrastructure such as airports, railways, public transport, and road tolls. The aim of the hacktivist attack is to disrupt travel, logistics, and assume a level of incompetence on behalf of their governments. By crippling high-visibility, mission-critical services, hacktivists virtually guarantee that outages will be reported by mainstream and social media, amplifying their message far beyond the immediate technical impact. The resulting headlines serve as free publicity, helping them shape public narratives and project an image of power and relevance.

Although, the hacktivist groups do not have the level of capability as state sponsored units or sophisticated actors capable of inflicting real damage, they still attempt to target energy and water supply services to cause as much disruption as possible. Attacks on energy and utility services have the aim of creating instability and provoking public discontent. As another target sector, hacktivist attack national media outlets. Attacking national media and independent news websites help Russian Hacktivists to increase their chances of gaining infamy through targeted medias coverage of their attacks.

Additionally, another hallmark of this third-era Russian hacktivism is the openly malicious character of many operations: the goal is no longer just to signal dissent or score propaganda points, but to inflict concrete harm on people, companies, and critical processes. Recent campaigns show actors trying to corrupt industrial-control systems, wipe data, or tamper with safety parameters so that the victim’s products, services, or even customers are put at real risk. A vivid illustration is the Z-Pentest Alliance’s claim that it re-configured the industrial

refrigeration controls at the Spanish meat-processing firm Cárnicas Llorente, allegedly maxing out temperature settings to spoil stored food and jeopardise public health, as demonstrated in figure 10. This shift toward deliberate, physical-world impact blurs the line between hacktivism and outright cyber-sabotage, underscoring how today's Russian hacktivist groups pursue disruption with potentially dangerous, real-life consequences.

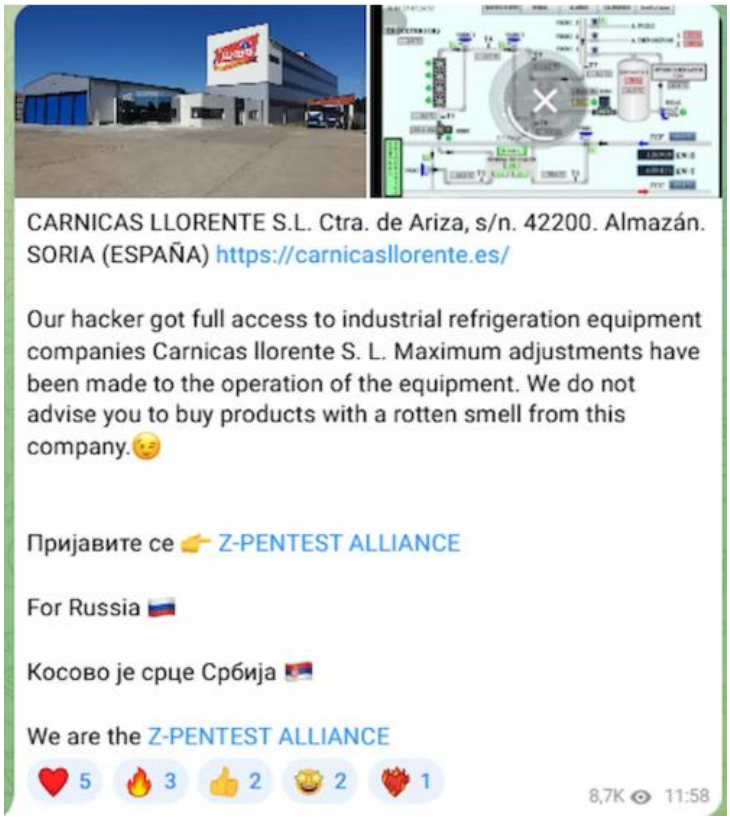

Figure 9. Pro-Russian "Z-Pentest Alliance" boasts on Telegram that it hijacked Cárnicas Llorente's industrial chillers in Spain to ruin the company's meat stocks

A further illustration of this intent to cause tangible harm comes from Killnet. In an August 2022 interview (Mordowanec, 2022) the group's former leader warned that future operations would "turn deadly" and vowed: "I will do my best to make these regions and countries answer for each of our soldiers," predicting that cyber-attacks on medical, transport, or industrial systems would soon claim real human lives.

While post-2022 Russian hacktivism mirrors second-era hacktivism in its use of reactive campaigns and ideological framing, the resemblance is largely superficial. Traditional hacktivists of the second era typically selected targets closely linked to their stated political causes. In contrast, Russian hacktivist groups often use broad geopolitical justifications to attack targets that bear little or no direct connection to the triggering event. Entire sectors such as banking, transportation, or media are taken offline in retaliation for political decisions

made by national leaders, affecting civilians and services with no involvement in those decisions. This disconnect highlights a shift from cause-driven activism to symbolic and indiscriminate digital aggression, where the goal is not just protest, but disruption and spectacle at scale.

3.2 Types of cyber attacks

Russian hacktivist groups' cyberattacks can be broadly categorized into three general types: Distributed Denial-of-Service (DDoS) attacks, website defacements, and data leaks. During chosen time period from November 2023 to February 2025, a total of 20,984 cyberattacks occurred. 19,070 of the occurrences were DDoS attacks, 595 were defacement attacks, and the remainder was different types of compromises and data leaks. The following sections will describe each type of attack, how they function in general, and how the Russian hacktivist groups acted in the observation time frame.

3.2.1 Distributed Denial of Service

Distributed Denial of Service, also known as DDoS, is a type of cyber-attack that aims to disrupt the targeted server with large amounts of traffic. This excessive load exhausts the target's resources, causing slowdowns or making it completely inaccessible to legitimate. In order for the DDoS-attack to have occurred, there must be intentional disruption of impacted systems (Douligeris & Mitrokotsa, 2004) meaning, for example, if someone had scanned a website for penetration testing purposes that subsequently caused outage then it is not a DoS-attack. DDoS attacks can take on different forms, they may be volumetric attacks that completely clog up bandwidth, protocol attacks that take advantage of network weaknesses, or application-layer attacks that knock-off specific services. Effectiveness of the DDoS-attack can be determined predominantly by how many unique devices the attacker has available to him - the more computers, tablets, phones, laptops, etc., that are capable of making network connections - the more volume of DDoS-attack. Therefore, DDoS-attacks use hundreds and sometimes tens of thousands of compromised computer systems as sources of attack traffic to maximize their volume (CF). Compromised devices are known as Zombie machines (Chaudhary & Mishra, 2023) and whole groups of zombie machines are called botnets.

In the case of Russian hacktivists, DDoS attacks made up roughly more than 90 percent of all their recorded operations which is a dominance driven partly by the fact that flooding a victim with junk traffic is technically far easier and cheaper than breaching networks, stealing data, or manipulating industrial-control systems. At the same time, the tactic's blunt-force

nature lets an attacker point the traffic hose at virtually any internet-exposed target worldwide like government portals, banks, hospitals, or small NGOs delivering instant disruption and publicity with minimal skill or preparation. Once the Russian hacktivists have decided on their targeted websites/services, their first step will be to do a DDoS-attack against this said target and make the site/service inaccessible for normal users. The second and very critical part is to then get the proof that they have taken down the target for real. Almost all the Russian hacktivists used the check-host.net tool which checks the availability of any site or server at the time the request was made. After they have received proof of successful DDoS-attacks, the final step that the Russian hacktivist groups do is to share the proof as a post on their public Telegram group for all to see.

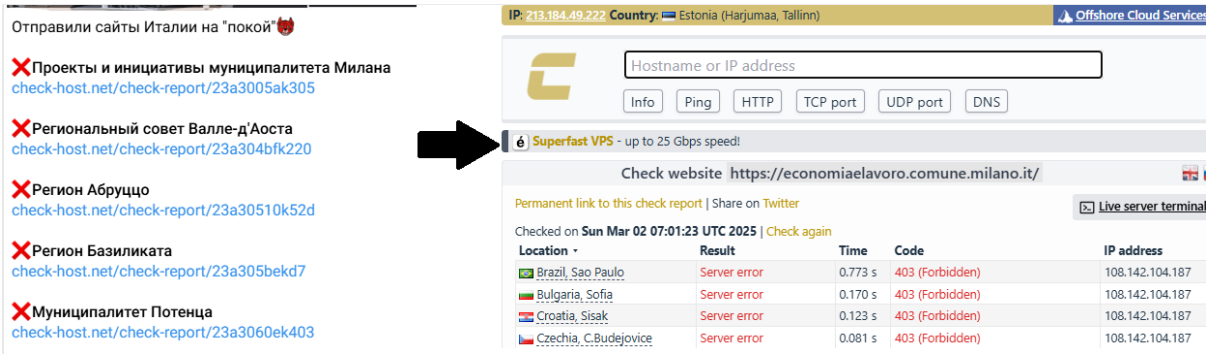

Figure 10. Screenshot from the NoName057(16) Telegram channel (left screenshot) linking to Check-Host reports (right screenshot) that confirm multiple Italian municipal websites were returning 403 errors during the group's DDoS campaign.

Figure 11. is an example of how it looks like for the observer that browses any of the Russian hacktivists channels on Telegram. Each time the Russian hacktivists launch a DDoS-campaign against a certain country they post a list of check-host weblinks that refer to the websites that the hacktivists have taken down. Figure 6. is a screenshot that has been taken from NoName057(16) Telegram channel on 02.03.2025 when they launched a DDoS-campaign against Italy. Once one clicks on one of the provided weblinks, he will be directed to check-host.net that shows how that specific site was not accessible from any part of the world at 02.03 2025 07:01 UTC.

3.2.2 Defacements

A defacement attack is a type of cyberattack that utilizes a vulnerable webserver to gain unauthorized user access to a website in order to alter its content (Albalawi et al. 2022) which usually replaces the original text, images, or functionality with messages that project ideological, political, or theological message. Thus, defacement attacks hold no monetary or strategic value and are mostly political. For this reason, defacement attacks are linked to

hacktivism (Romagna & Van Den Hout, 2017) to a much higher degree, compared to other types of cyber-attacks.

The technical execution of defacement attacks usually make use of exploits originating from weaknesses in web applications, outdated platform software or misconfigured server settings (Nguyen et al, 2021). Attackers will seek to expand the potential for gain by using various methods such as SQL injection, Cross-Site Scripting (XSS), or brute-force to scope-out the ability to gain administrator privileges, this will ultimately allow them to overwrite web content. In certain examples, the hacker will insert bugs which are commonly termed as backdoors that provide access by maintaining a presence via their implementation. Once the attack is executed, the altered content may create disinformation, chastise political or social enemies, or promote extremist ideologies. The impact of defacement attacks usually do not go beyond tweaking few lines of text and may not cause any data compromise nor may cause direct financial loss, yet damage to an organization's reputation (Mao & Bagolibe, 2019) or trust by the public may be the consequence, and may serve the purpose of psychological warfare in geopolitical conflict; cross-national subversion.

In case of Russian hacktivists, the defacement content is always more or less the same; the defaced website of the hacktivist group will display the logo of the hacktivist group that executed the defacement, the hacktivist group name, and some Pro-Russian or anti-EU / anti-Ukraine slogan message as illustrated in figure 12.

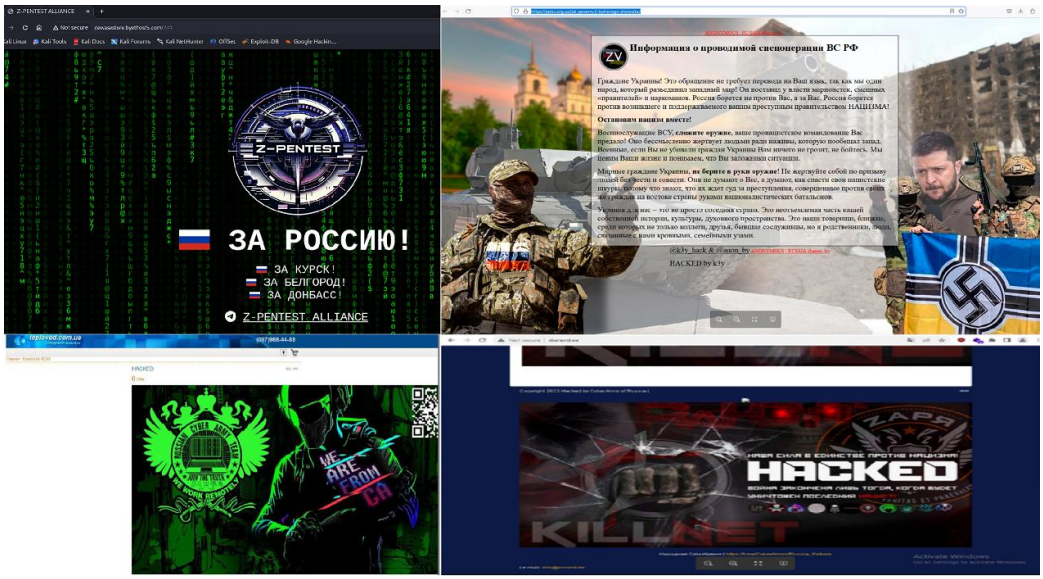

Figure 11. Examples of Russian hacktivist defacement attacks.

Defacement attacks have proven to be an effective tool for Russian hacktivists to, not only further their pro-Russian narrative and disseminate propaganda, but also provide visible, evident proof of successful attacks that can quickly be claimed and used to spread their impact through media and online networks. Even though these hacktivists post proof using Check-Host links of successful DDoS attacks, they are inherently less effective because Check-Host is not always reliable. For example, Check-Host does not provide any indication of geoblocking. The targeted website may be down for one region but still up for others. Moreover, unlike defacements, Check-Host links will not conjure up the same psychological detachment for the viewers. The viewers have to go through the motions of technical verification before they can express disbelief and detachment to the successful attack in social media comments. The same limits exist for data leaks and other forms of hacking damage too. For example, Russian hacktivists may provide the stolen data to substantiate their claim of a successful intrusion; however, it is not the average viewer that will be able to prove legitimacy and/or impact. In contrast to defacements, which provide visible and evident proof of intrusion, leaked data requires non-hacktivists to provide forensic analysis of the validity of the level of intrusion, which acts against instant propaganda or immediate readiness for the common observer.

3.2.3 Data Leaks

A data breach is the intentional or unintentional exposure of confidential information to unauthorized parties (Cheng et al, 2017). In the context of this paper, data leak attacks are a variant of data breach that are characterized by two qualities. Firstly, the attack has to be intentional meaning that the attackers who gain access to unauthorized systems are outsiders who found the necessary vulnerabilities in the targeted system to gain access to data that otherwise is not publicly available. Secondly, the data obtained by the attackers has to be leaked publicly for free. This is an important distinction because intentional data breaches are for the most part committed for either financial (Bhadouria, 2022) or strategic (Nejjari et al, 2024) purposes. For example, with monetary breaches the information that was just stolen is typically either sold to someone for financial gain, or used to financially extort (sometimes) the institution which was stolen from in the first place. Strategic breaches are most generally performed by state-affiliated actors (APTs) and that stolen information is not leaked or sold, but usually handed to the particular government organization that controls them. Hacktivists, however, are driven by political purposes and not financial nor strategic, thus they use leaks

as a tool for public disclosure, aiming to damage the credibility of governments, corporations, or other adversarial entities.

Russian hacktivists differ significantly from traditional, "old-school" hacktivists in their approach to data leak attacks. While conventional hacktivist groups typically target specific institutions or corporations that align with their ideological grievances, such as government agencies engaged in surveillance, oil companies contributing to environmental damage, or corporations accused of unethical practices - Russian hacktivists operate with a broader, more indiscriminate strategy. Instead of focusing on entities directly tied to Ukraine or its allies, they often exploit vulnerabilities in any website or database they can access, regardless of its relevance to the conflict. This means that even small, unrelated businesses, local government portals, or academic institutions can become victims of data leaks simply because they belong to a country deemed adversarial to Russia. The action isn't just to expose (the most exploitable information), it also serves to create a perpetual sense of insecurity that we have no safe space from data intrusions. This indiscriminate approach aligns with Russia's broader information warfare strategy, which prioritizes widespread disruption and psychological impact over targeted ideological protest. As a result, Russian hacktivist-driven data leaks often lack the clear political messaging of traditional hacktivist operations, instead functioning as tools of intimidation and destabilization on a national scale.

Once the Russian hacktivists manage to compromise their target, the stolen data or credentials are usually posted to their public Telegram channels (figure 13).

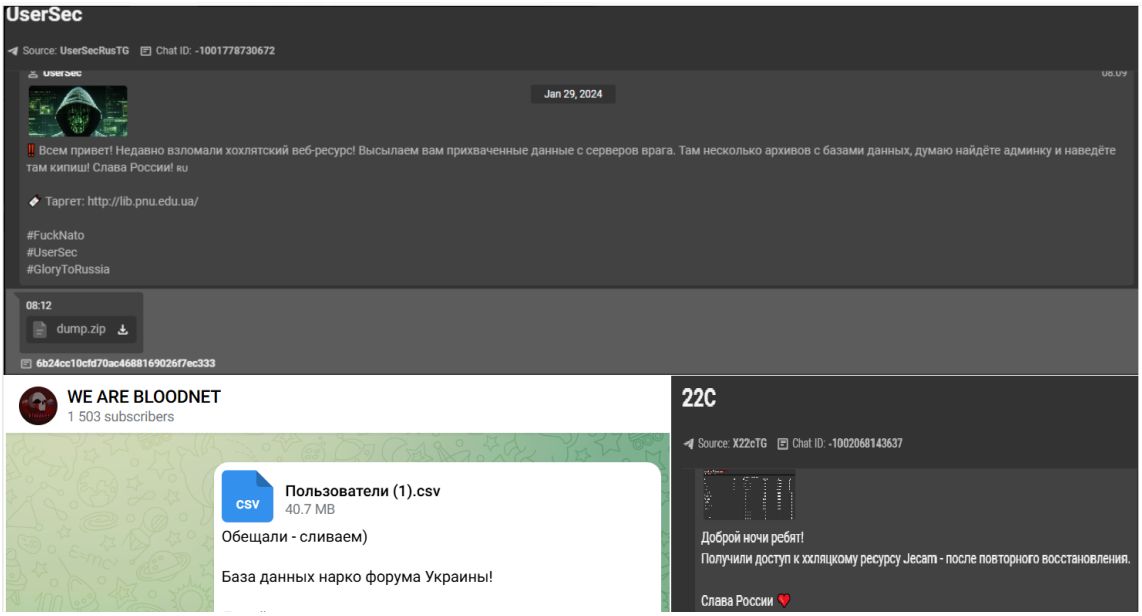

Figure 12. Examples of Rusiian hacktivists leaking stolen data.

Though some of the data leaks made available by Russian hacktivists may be legitimate, in a number of cases Russian hacktivists will fictionalize or distort the available leaked data to gain credibility for themselves and to overstate their influence, knowing that the average user will often not have the tools or capacity to investigate whether the stolen data is legitimate.

3.2.4 Summary of Russian hacktivist cyber attack types and technical sophistication

While many previous geneations of hacktivist groups - many of which demonstrated sophisticated levels of technical understanding and identifiable ideological positions exhibited a greater level of tactical depth than the Russian hacktivists post-2022, in some respects, the Russian hacktivists post-2022 would warrant a fairly low rating. The fact that more than 90% recordable attacks are basic DDoS-campaigns shows a reliance on the most basic techniques of disruption as opposed to complex, technically sophisticated, or fairly impactful operations. For comparison: first-period hacktivist groups such as L0pht and Cult of the Dead Cow partook in responsible vulnerability disclosures, tool development, and ideological action of attacking their targets in ways that included ethics, transparency, and digital rights. Second-period hacktivist groups including Anonymous and LulzSec conducted digital breaches of many high-profile institutions including the CIA, Sony, and PayPal, and leaked sensitive data in operations that frequently required sophisticated technical understanding and social engineering.

The Russian hacktivists, on the other hand, are more focused on scale and visibility than, for example, precision. Their attacks on a mass scale against civilian infrastructure and evidence of disruption just to put something on Telegram show an intention to apply psychological pressure or publicize impact where ideology or participant intentions are secondary. By using sheer mass or quantity over quality, similar to how the Russian hacktivist community identifies more largely and uncertainly as propaganda actors within the broader Russian information warfare domain, where the symbolic, disruptive impact, and soundbites are more important than programming or technical accomplishments.

3.3 Communication

In this sub-chapter, the content of the most frequently exposed in Russian hacktivist Telegram channels will be outlined, while providing a few examples to illustrate each concept. Upon reviewing the hacktivist groups' posts common content in the form of attack announcements,

proof of successful hacks, ideological messages, recruiting members, and calls for actionable causes or actions become visible. Understanding the ternary of the content provides palpable clues about how the groups operate, how they structure and organize to communicate, and how they attempt to influence their friends, followers, and enemy groups

3.3.1 Telegram

Telegram is a feature-rich and cloud-based messaging application that provides fast, secure, and convenient messaging for individuals and groups (Thomas & Bhat, 2022). Telegram was first launched by Pavel Durov in 2013. The service has attracted users due to its company's strong emphasis on privacy and encryption services along with its many features such as channels, groups, and bots. Unlike many messaging services, Telegram allows users to send messages, media and file transfers without size limits. Subsequently, Telegram has become popular among various communities like activists and journalists, and even cyber criminal groups. Telegram allows individuals to communicate privately and publicly through direct messaging, which can either be one-on-one or via a group chat, and channels in which one or more administrators can broadcast messages to an unlimited number of subscribers. The platform has "Secret Chats" designated for end-to-end encryption, while other messages are encrypted in transit, stored on cloud servers, and synchronized across all applicable devices. Users also have the option of creating an anonymous account, as users can register with a phone number but choose to communicate without revealing other personal identifying information. The mixture of security, anonymity, and mass communications capabilities have made Telegram an important resource for various extremist movements, underground networks, and hacktivist groups, especially in countries that employ strict internet censorship and monitoring of citizens. Telegram's privacy policies continue to attract extremist users from hate-driven and violent ideological groups that have been removed from other social media platforms (Walther & McCoy, 2021).

Telegram represents the most significant avenue for Russian hacktivists and their primary medium to announce cyber-attacks to a wider audience. Almost every Russian hacktivist group has at least one public Telegram channel - open to all users of the platform. Their channels facilitate a variety of uses to include but not limited to announcing successful attacks, planning and coordinating activities, disseminating ideological narratives, and recruiting fellow Russians. Telegram facilitates some level of anonymity and limited content restrictions which provides Russian hacktivists the freedom to broadcast their attacks while

addressing a variety of audiences. Because of the groups' use of public and "unrestricted" Telegram channels to announce their activities, it is much easier to track and monitor Russian hacktivists compared to other cybercriminal groups that operate in limited and sometimes restricted environments. Traditional cybercriminals tend to utilize encrypted forums, private marketplace, and the dark web since their intent is generally to keep their operations secret. As such, the outcomes of their operations are unseen for all intents and purposes, thus delineating Russian hacktivists from traditional cybercriminals, as the need for visibility in their operations be it through propaganda, responsibility for attacks or other means of soliciting support prohibits their duly and justifiable anonymity. As a result, researchers, security analysts, law enforcement agencies and are able to track the activities of Telegram-based hacktivists in "real" time via the groups' Telegram channels, studying their messages and analyzing their technology processes and tactics. The hacktivist activity outputs present in a public forum provide researchers a unique opportunity to assign responsibility for attacks, procure intelligence, gather threat assessments, unbeknownst or unrecognzed situational awareness regarding their mandates, technology processes, and modus operandi. Even though some hacktivists attempt to use less public or private anonymous channels, their need for public exposure is a significant and identifiable difference between hacktivist groups and other cybercriminal actors who rely on greater secrecy.

3.3.2. Cyber-attack announcements

The primary type of content shared on Russian hacktivist Telegram channels revolves around cyberattacks. Hacktivist groups regularly post updates on their latest attacks, specifying the targeted country and detailing the systems or institutions they have compromised, as illustrated in figure 14. These posts often include screenshots, stolen data, or website defacement images as proof of their success. Alongside these attack claims, hacktivists frequently provide political justifications for their actions, framing their cyberattacks as retaliatory measures or part of a broader geopolitical struggle. Whether targeting Western governments, critical infrastructure, or media organizations, their messaging typically aligns with Russia’s strategic interests, portraying their activities as acts of digital warfare against perceived enemies.

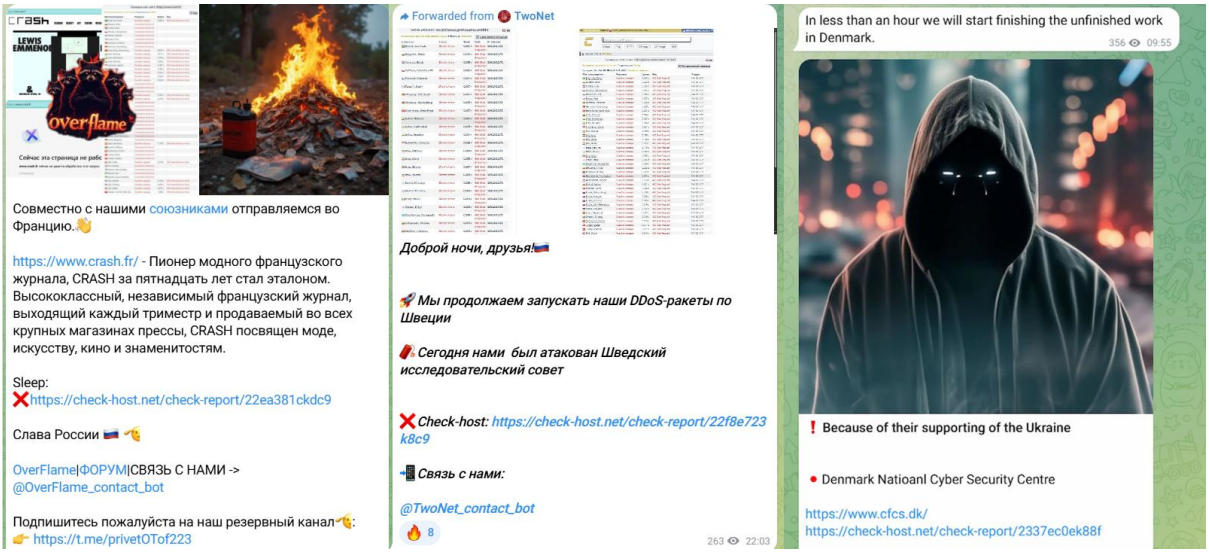

Figure 13. Examples of cyber attack announcements by Russian hacktivist groups.

One of the few things that Russian hacktivist groups have in common with earlier generations of hacktivists is the way they announce their attacks - providing real-time updates, screenshots, and public explanations. Whether they announce their attacks through real-time updates or screenshots, Russian hacktivists typically post their attacks or public justifications on Telegram as their primary means of communication, much like Anonymous, LulzSec, etc. Each of these groups in this second era, much like Russian hacktivists, used Twitter, Facebook, YouTube, and Pastebin as ways to publicly promote their action and proffer manifestos to justify (or often glorify) their hacktivist actions. The underlying logic remains the same: maximize visibility, control the narrative, and use digital channels to directly reach both the media and the public. This publicity-driven approach mirrors how traditional hacktivists treated social media and defaced websites as stages for ideological performance. However, while earlier groups emphasized political messages or ethical declarations in their press releases and videos, Russian hacktivists often focus more on spectacle and intimidation, reinforcing propaganda over protest

3.3.3 Forming alliances

Russian hacktivists continually use their telegram channels in other ways to announce partnerships with similarly minded hacktivist groups, and potentially create collective impact as illustrated in examples in figure 15. As presented commonly by hacktivists the partnership is framed as a strategic collaboration to improve cyber capabilities, coordinated attacks, or the sharing of resources, such as tools, techniques, or intelligence regarding vulnerabilities, etc. Announcing publicly that they will be working together creates a message of unity for

hacktivist groups, and allows the loyalty of a common adversary to be defined as part of a larger effort of cyber warfare. And the identity of the adversary is not limited to Russian groups - the partnerships can even extend to pro-Russian or anti-western hacktivist organizations in other countries which expand their operational limits. Telegram is the ideal medium for these sorts of connections to take place, where groups can announce that they will work together, endorse each other's messaging, and cooperate with each other's systems to ramp up and coordinate larger organized cyber campaigns with better effectiveness.

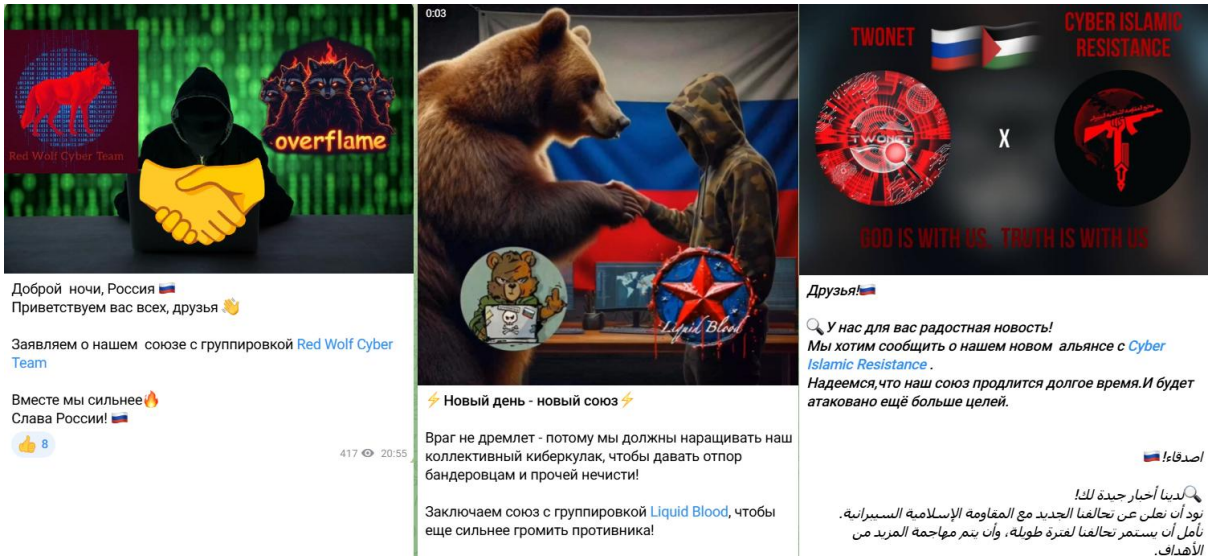

Figure 14. Russian hacktivist groups announcing alliances with various Pro-Palestinian hacktivist groups.

After an alliance is formed, Russian hacktivists often advertise their allies' attacks on their Telegram channels, because not only are they trying to get the most eyes on their attacks, they would also like to gain as many followers and subscribers as possible by engaging a broader audience through concurrent exposure on multiple channels. The promotion of one another's actions can take on a sneakier and more strategic approach; allied groups, by amplifying one another's actions, create a complex ecology of hacktivist channels. If one is a follower of one channel, there is a high likelihood they'll become a subscriber of another. This cross promotion can help the groups widen their audience and propaganda and get attention for their cyber-attacks. Additionally, the act of constantly resharing attacks on channels allows their followers to view their cyber-attacks as connected, and makes the hacktivists appear more organized and functional together than in reality.

3.4 Advertising and selling services

A key feature that sets post-2022 Russian hacktivism apart from earlier eras is its open pursuit of financial gain. While first- and second-era hacktivists generally rejected

monetization in favor of ethical or ideological goals, Russian groups today blend political messaging with systematic profit-making. They operate not just as activists, but as commercial actors within a broader cybercrime ecosystem. Telegram's anonymity and minimal moderation make it an ideal marketplace where Russian hacktivists list illicit services, price charts, and crypto payment details. By selling "hacks-as-a-service" and access to compromised networks, they blur the line between protest and profit, turning hacktivism into a revenue stream that funds and sustains their future operations. Throughout the observation period, four main monetization strategies were identified: advertising third-party services, offering explicitly malicious tools, soliciting crypto donations, and selling their own attack infrastructure and training. The following subchapters examine each of these methods in detail.

3.4.1 Advertising non-malicious services

The first method is advertising random services that may not be illegal or harmful: VPN providers, cybersecurity tools, digital marketing services and so forth. Hacktivists can make money through advertorials, sponsorships or affiliate programs by exploiting a large follower count. Hacktivists will use the visibility of their platform to generate passive income.

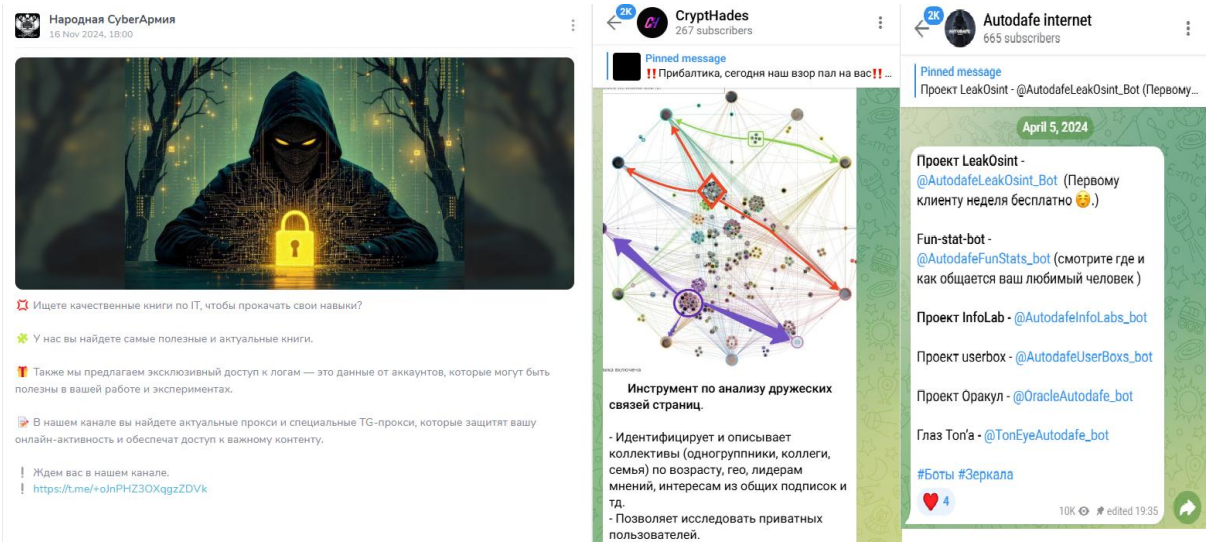

Figure 15. Examples of Russian hacktivists promoting various services on their public Telegram channels.

Figure 16 presents three screenshots of telegram channels that provide examples for Russian hacktivists advertising various services. Left Screenshot (Народная CyberАрмия) - This post is for books on IT in the context of learning cybersecurity and hacking. The services noted indicate they offer "exclusive access to logs", which implies the selling of stolen accounts.. Middle Screenshot (CryptHades) - This post is advertising a tool to analyse the target's online

interactions. The tool states it can group the user's contacts into categories based on interest areas, geographic locations, subscription commonalities and activities of the private user.. Right Screenshot (Autodafe internet) - This post is describing a list of several telegram bots that provide data services. One of the bots , "LeakOsint", offers the first week for free, implying that it likely provides leaked or scrapped content from somewhere. In the advertisements there was nothing described that suggested legality about the content. Others simply described social media, interactive analysis and tracking user activity with both practical and intrusive implications.

3.4.2 Malicious services

The second approach is to advertise explicitly malicious services like botnets, stolen data or access to compromised systems (stolen data can also be an intermediary result). Some of these services are run by groups who have marked themselves as "brokers" or "intermediates" between the cybercriminals and, the "legitimate" third party procuring their services, taking a commission for their efforts. This category would also include the paid for hire DDoS services, where the buyer pays a fee to perform a DDoS attack on the target website or infrastructure.

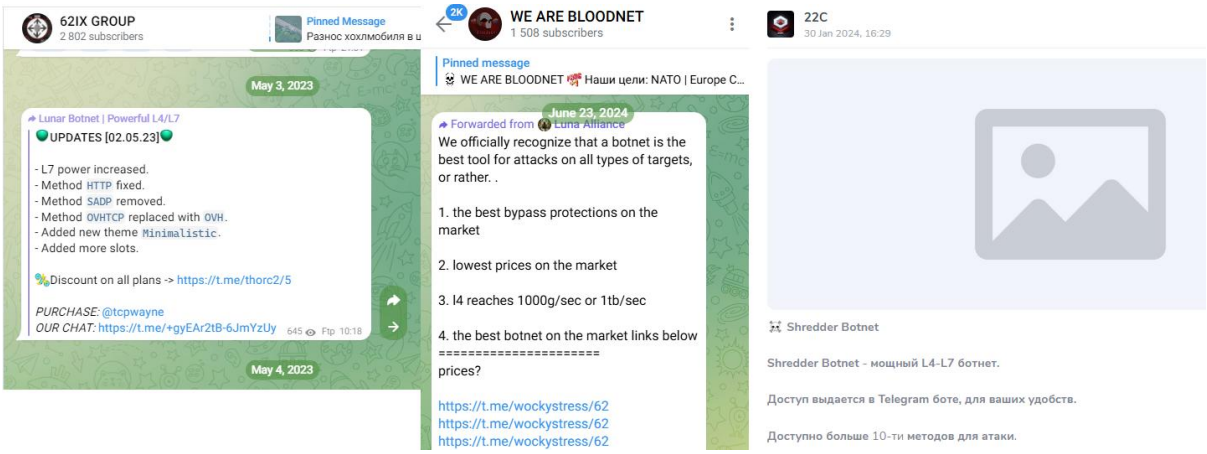

Figure 16. Examples of Russian hacktivists advertising malicious services.

Figure 17 shows three Telegram channels screenshots of Russian hacktivists requesting malicious services (most often denote as a botnet) to carry out cyber-attacks. Left Screenshot (62IX GROUP) - this post promotes the "Lunar Botnet," an L4/L7-Level botnet to carry out Distributed Denial-of-Service (DDoS) attacks. They discuss updates like stronger attacks, set methods of attack, and customizations. They provide a discount on plans for using their botnet and provide links for purchase and communications. Middle Screenshot (WE ARE BLOODNET) - The post promoted the use of a botnet for cyber-attacks as being the best

way. The message provided selling points of the botnet, one of which included bypassing protections that they have in place, cheap per-use pricing, and attack rates of up to 1Tb/sec. The group also provided some links that directed the user to purchase the botnet services they promoted. Right Screenshot (22C) - This post promoted the "Shredder Botnet" another L4-L7 botnet used to carry out attacks. They promote that botnet access, and provide access through a telegram bot to simply user, and promote that they had access to more than ten methods of attack to offer customers.

3.4.3 Asking for donations

The third method is soliciting donations from followers, typically in cryptocurrency to ensure anonymity. Many hacktivist groups post crypto wallet addresses in their Telegram channels, asking supporters to contribute financially to sustain their operations. These donations are often framed as a way to fund future cyber-attacks, cover infrastructure costs, or support the broader ideological movement behind their activities (example figure 18).

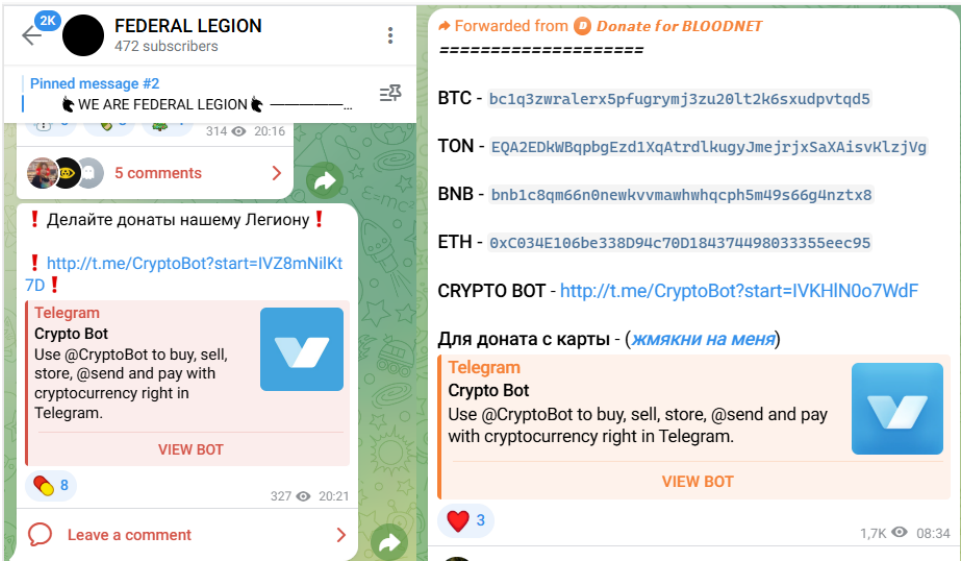

Figure 17. Russian hacktivists asking for donations from their followers

The process of requesting donations is relatively straightforward - Russian hacktivists will post on their public telegram channel, and list various crypto wallet addresses (typically, they'll provide some rationale for the need for money.

3.4.4 Providing services

Recognizing the limitations of advertising and donations as stable revenue streams, Russian hacktivist groups began pivoting in early 2024 toward selling their own tools and services. These include custom-built botnets, exploit kits, and hacking tools, along with paid courses

teaching cyber-attack techniques, particularly DDoS attacks. By directly monetizing their expertise, hacktivists have created a more sustainable financial model, ensuring a continuous influx of funds while expanding their influence within the cybercriminal ecosystem.

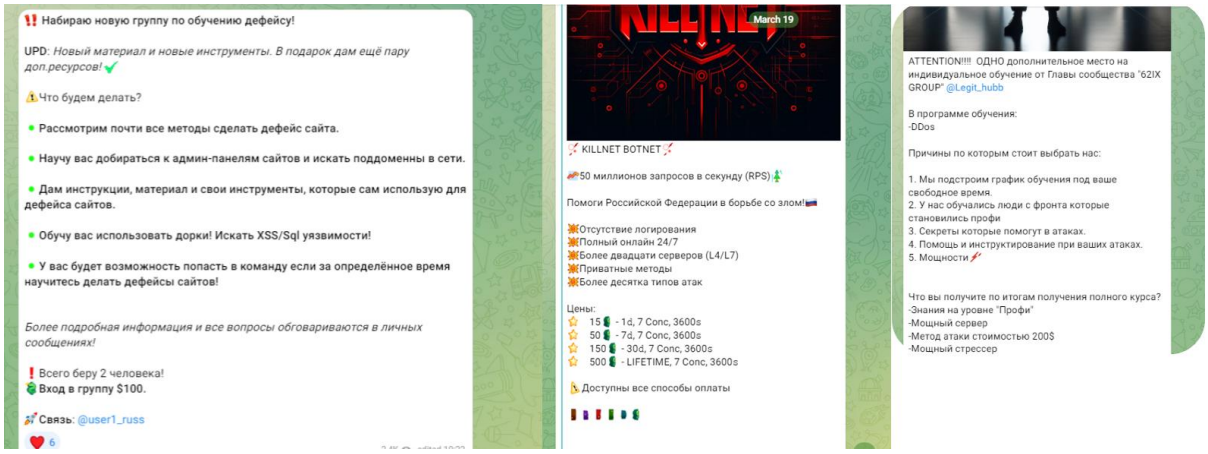

Figure 18. Examples of Russian hackivists promoting their own malicious services.

Figure 19 shows three Telegram posts with three different examples of Russian hacktivist groups; UserSec, Killnet 2.0, and 62IX, selling their cyber services to generate profit.

The **left Screenshot (UserSec - Website Defacement Course)** shows an offer for an online defacement course. Defacement is a common tactic used by hacktivists to deface and vandalize websites. The course teaches various defacement methods and how to get into an admin panel while leveraging XSS/SQL vulnerabilities. The course also included educational materials, tools, and hands-on training. The post indicated that those who have demonstrated the ability to perform defacements would be considered for membership to the UserSec group. The course costs $100 a person, illustrating the idea on how hacktivists leverage their hacking skills and knowledge to generate income by developing novice hackers around cyber-attacks.

The **middle Screenshot (Killnet 2.0 - Botnet Rental Service)** illustrates a discussion about the Killnet Botnet which facilitates large-scale DDoS attacks. The post highlights the botnet's attack rates of up to 50 million requests a second and its 24/7 online capabilities; Additionally, the botnet promotes various attack mechanisms, including private attack mechanisms, which is quite common among hacktivist organizations. The post indicates a tiered pricing mechanism, with attack plans ranging from $15 per day to $500 for lifetime access. Killnet 2.0 frame the service in a broader effort for cyberwarfare purpose and called for awareness of the Russian Federation, simultaneously combining hacktivism with cybercriminal monetization.

The r**ight Screenshot (62IX - DDoS Training and Attack Tools)** llustrates a discussion about a personalized DDoS training by 62IX Group. The training is advertised as a high-level professional course with flexible scheduling and the instructional guidance of "experts." The course claims to provide real-world knowledge, attack plans, and successful tools. At the end of the course, they receive a certificate designating them with "pro-level" skills as well as access to a private server and one attack plan worth $200. Evidence that hacktivist groups do not just execute cyber attacks, but are trying to develop a financially motivated 'community' through selling training and selling attack infrastructure.

The commercialization of hacktivism stands out as one of the defining features of the third era of hacktivism, as illustrated by Russian hacktivist groups. Unlike the politically idealistic actors of the first era or the ideologically reactive movements of the second era, third-era hacktivists openly integrate financial motives into their operations. Russian groups such as Killnet and UserSec exemplify this shift: alongside political rhetoric and propaganda campaigns, they advertise DDoS-for-hire services, sell hacking tools and training courses, and solicit cryptocurrency donations. This blending of political activism with profit-driven activity reflects a broader evolution in hacktivism, where visibility, disruption, and economic sustainability now coexist. Thus, the Russian case demonstrates how third-era hacktivism has transformed into a hybrid phenomenon, combining ideological goals with systematic monetization.

3.5 Recruitment

Russian hacktivist groups frequently use their Telegram channels to post recruitment announcements, aiming to expand their ranks and attract individuals with various skill sets. Unlike traditional cybercriminal organizations that operate in closed forums or invite-only networks, hacktivists often publicly call for new members, framing their activities as part of a broader ideological or geopolitical struggle. Recruitment posts typically identify the skills they seek to obtain such as experienced performing DDoS attacks, website defacement, and open-source imaging (OSINT), but also thematically represent, entry-level loading even non-technical personnel for tasks like media contacts, propaganda shares, or coordination. Some groups even have training for amateurs, who can be lead participants in the recruitment as they can "fight" against a political enemy while learning cyber TTP. Often, the recruitment is invitations to smaller groups or newly assigned private chats before execution with the main actors.

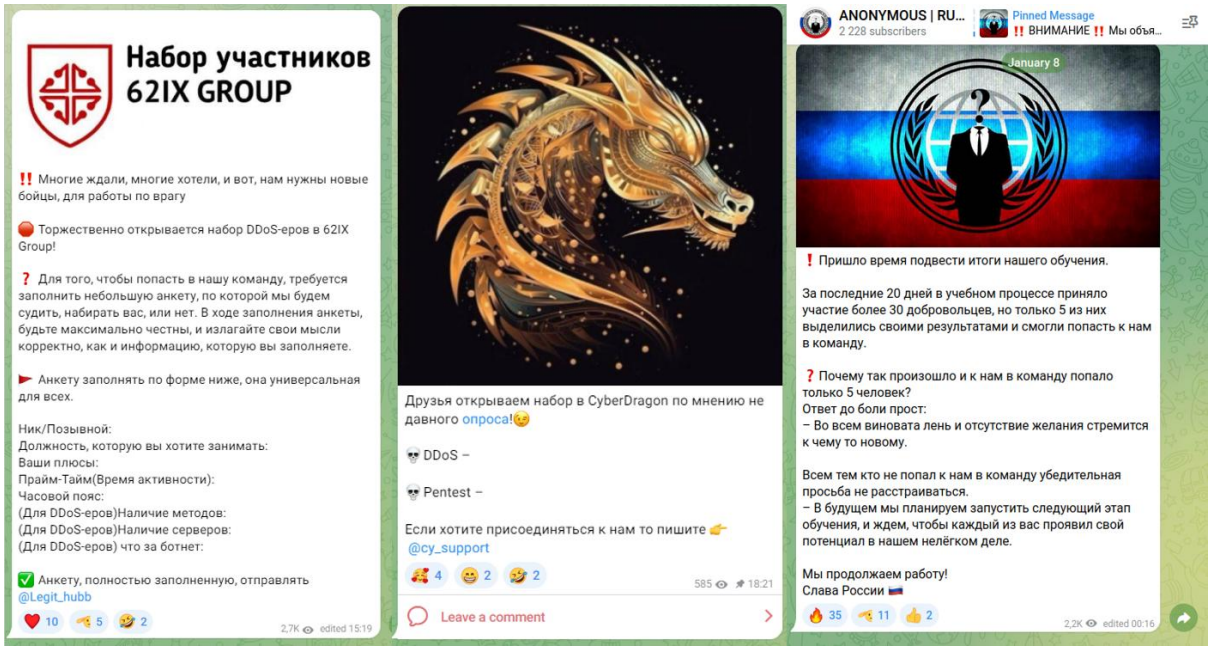

Figure 19. Examples of public recruitment announcements by Russian hacktivist groups.

Figure 20 shows three Telegram recruitment announcements from Russian hacktivist groups: 62IX Group, CyberDragon, and Anonymous Russia, each seeking to expand the number of members on their team by recruiting people to conduct cyber operations.

The **left Screenshot (62IX Group – DDoS Recruitment)** illustrates the recruitment of the 62IX Group. It is publicly recruiting new members for its DDoS operations, emphasizing the need for "fighters" working against their enemies. The post describes a methodical recruitment process requiring the applicants to fill out an application, indicating what type of position, skill-level, availability, and experience (with attack types, servers and botnets) is preferable. The encouragement of candidates applying honestly implies they are trying to screen candidates before bringing them in, while the overtly regimented recruitment post shows a unit that appears to be structured.

The **middle Screenshot (CyberDragon – DDoS and Pentest Recruitment)** illustrates an example of the recruitment into the group CyberDragon. It is open for recruitment and is looking to recruit people needing interested in DDoS attacks and penetration testing. The recruitment call is less formal when compared to 62IX Group, and whereas 62IX Group followed up on a previous poll (possibly indicating there was interest in bringing on new members) CyberDragon offers no detailed process, instead asking those interested to reach out to a support handle. This very direct approach suggests CyberDragon is hoping to recruit in a more fluid, immediate way without a highly regimented screening process.

The **right Screenshot (Anonymous Russia – Training Based Recruitment)** illustrates an example of the recruitment into the group Anonymous Russia. The group reflects on finishing a training program, in which over 30 volunteers participated, but only five had enough skill to be considered to join. The post criticizes the applicants who did not pass the training with implied character and moral judgments of laziness and lack of motivation. Anonymous Russia advised those who did not pass the training to try again in upcoming offerings, indicating that this is an ongoing recruitment strategy to develop the skills of volunteers. Anonymous Russia's approach to recruitment seems to value training: encouraging participants that did not yet pass to try again suggests they want to try to build a higher caliber team of committed volunteers.

When someone responds to a recruitment announcement, typically by contacting the Telegram link, they go through some kind of initial scrutiny process. In most circumstances, the first hurdle is submitting a cyber-focused CV, which details education, work experience, technical skills, and experiences with various hacking tools and attack types. This step in the vetting process allows a hacktivist group to see if an applicant has particular experience or expertise, like DDoS attacks, penetration testing, or OSINT (open-source intelligence) collection. Some groups have a strict selection process and wants more advanced cybersecurity knowledge and experience, while others are more lenient and train those with minimal experience. Depending upon the group, recruits may be questioned on their motivations for applying, whether their ideology coincides with the groups, and their availability for cyber operations. This structured, yet fluid-process works for Russian hacktivists in determining if applicants have enough expertise, and expand networks to include skilled operatives and newcomers willing to learn.

Figure 21 depicts an example of initial contact with the well-known Russian hacktivist group KillNet 2.0 (not to be confused with original KillNet, KillNet 2.0 was created after the demise of original KillNet) via Telegram, followed by a recruitment request. The recruiter immediately replies with an application to be filled out, requesting the following information:the specialization the applicant wants to be involved in (DDoS attacks, pentesting, or OSINT), the applicant's age, the applicant's work experience, the applicant's skills, and fields of expertise related to the specialization there applying for.

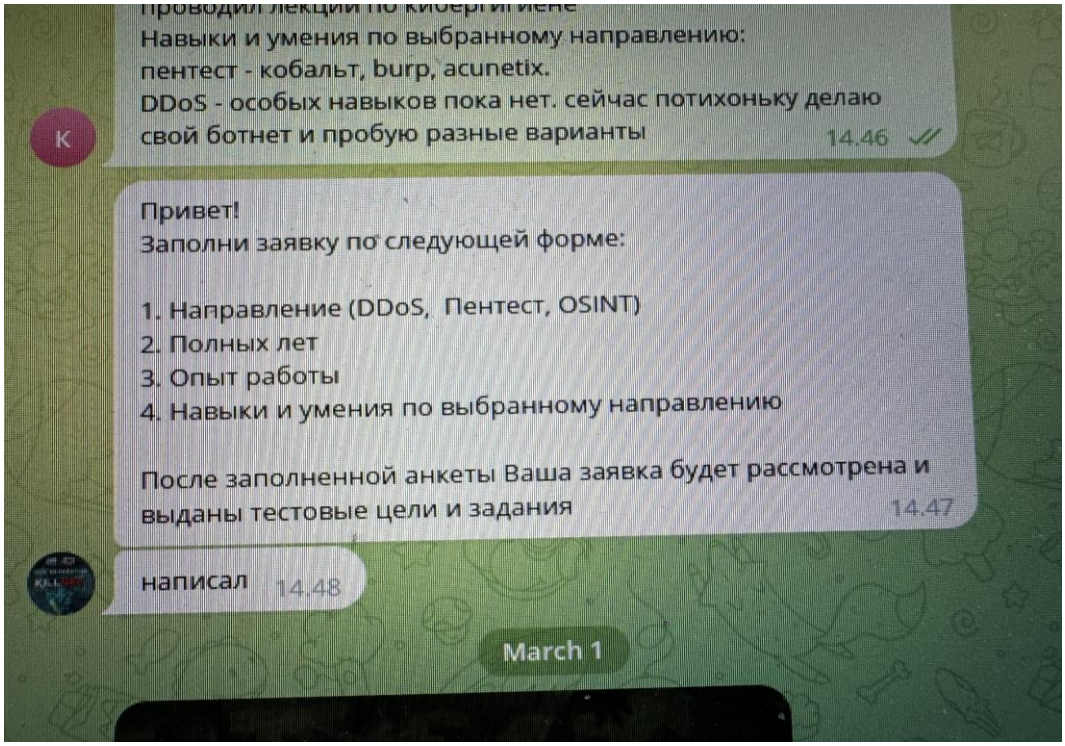

Figure 20. Screenshot of a message chat with a recruiter from the KillNet 2.0 group

The recruiter states that once the application is filled out and submitted, the recruiter's submit will be reviewed to complete the application. If the selected candidate is accepted after the review, they will be given objectives and tasks to demonstrate their skills. This clearly suggests that the group has a process of vetting recruits, and they require recruits to demonstrate skills associated with their specialization before receiving final membership.

After a recruit is accepted into the initial recruitment process, they will usually be given a task to demonstrate their skills. In the majority of the cases, these tasks are explicitly malicious, and test not only technical skills but also applicants capacity and willingness to perform illegal cyber attacks (in case of KillNet 2.0, the task was to compromise a specific Ukrainian website). Hacktivist groups that have a recruitment process for members frequently ask recruits to conduct a DDoS attack on a target and provide evidence of successful disruptions such as captured screenshots of the site being down, or logs of the requests to attack. Another routine task is to have the applicant hack into a site and provide the recruiter with credentials to access the site or provide access to stolen data, showing competence and trustworthiness. Some groups preferred to have potential candidates purely OSINT-related missions, for example deanonymizing an individual by gathering their personal information to expose them in a doxxing way.

During the first-hand research for this study one example from the NET-WORKER ALLIANCE group had the recruit given a specific malicious entry task. The group assigned a Distributed Denial-of-Service (DDoS) attack against the European Central Bank (ECB) website and told the recruit to keep the attack going for around four to five hours (figure 22). The communication depicted a clear assignment, as the recruiter shared the link to attack and the told the recruit to keep the attack going for a designated amount of time.

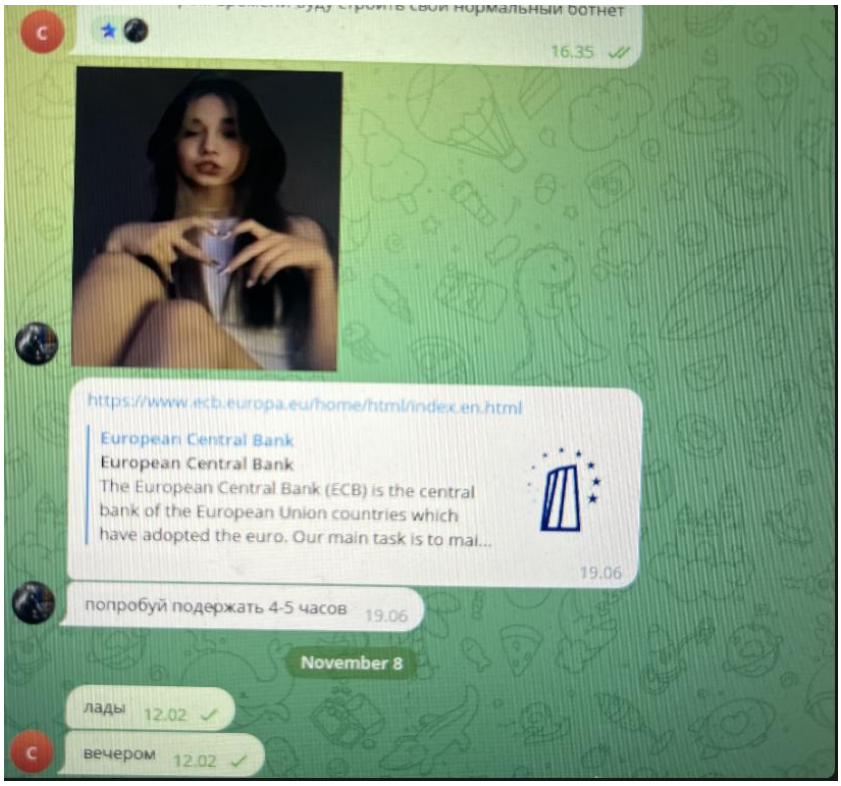

Figure 21. Telegram direct message chat with recruiter from Net-Worker Alliance group

These initial tasks serve at least two objectives for the hacktivist group; firstly, the hacktivist group can assess the recruit's practical abilities and secondly the group ensures that only those willing to commit cyber offences are provided full membership. Forcing recruits to commit illegal acts from the outset creates leverage on the group to compromise participants who are obliged in some small way to illegal acts. The formalized entry tasks provide assurance to the group's organizers that new members are technically competent and that they have some ideological or financial commitment to the group's on-going cyber campaigns.

When the recruit completely their entry- test task and is accepted as a member then he is invited to a separate Telegram channel which is meant for members only. These private groups, restricted to only active members, are much different from the public recruitment and propaganda channels that serve as one dimension of hacktivist coordination. These private

channels are the primary coordination sites for cyber operations. Members strategize about an attack, assign who's going to be attacking what, and agree upon timelines to execute plans and complete recon and reconnaissance. Active discussions in these channels center around identifying targets that are more valuable (higher priority), who is going to attack what, and sharing technical resources , botnets, exploits, VPNs making anonymity more viable. Some groups also use channels to instruct less experienced participants, providing guidelines to ensure all individuals are able to meaningfully contribute to new operational stages. This structure indicates the level of organization within Russian hacktivist collectives, where attacks are motorized by organized systematic approaches to attack and not haphazardly, following highly structured attack plans materially as indicated through closed Telegram environments and private coordination channels. By discussing these operational details in private groups, hacktivists create a controlled environment for fellow hackers where they can have secure communication when executing cyber-attacks at an increased efficiency.

There are a number of ways that recruitment differs most greatly between Russian hacktivist groups and prior generations of hacktivists. First and second eras of hacktivism, where generally anarchistic groups clouded in ambiguity such as Anonymous created open participatory avenues to join, i.e. endorse a cause or participate in an operation, by being able to join; Someone could be an anonymous hacktivist just by endorsing and most, if not all earlier era movements rooted themselves in this model. Thus, where it contrasts is that recruitment is highly organized and more selective. Recruitment is promoted through Telegram, the groups provide information regarding recruitment campaigns and request that candidates provide detailed cyber-oriented CVs, undergo vetting, prove their skill: this is often involving real cyberattacks as practical tests- when they pass, they are brought into private coordination channels and organized cyber operations are discussed and fully planned. As such, Russian hacktivist groups offer a clear and formalized task-based recruitment model- which is a world away from the self-selection and unfettered access open to participants in previous eras driven by ideology. In the third era, like Russian hacktivists represent as a reality of the digital ecosystem of contemporary hacktivism, the third era of hacktivism has gone a direction of controlled and hierarchical networks organized around tasks and operational outcomes. In short, it represents a movement away from the spontaneous mass strategies of earlier era hacktivism with more tactical goal oriented cyber operational planning.

4. Empirical Analysis – Part II

This chapter tests whether there is a correlation between media attention and the frequency of cyberattacks claimed by Russian hacktivist groups. This analysis uses an original dataset that was built during a 16-month period (November 2023 – February 2025). The central assumption guiding the analysis is that greater domestic media visibility for Russian hacktivist groups leads to a higher frequency of their cyberattacks targeting that country. This assumption is based on the premise that media attention and visibility serve as a strategic signal to hacktivist actors, linking to a functional desire of symbolic validation, in addition to the opportunities for additional sources of revenue through new audience. To explore the links between media attention and Russian hacktivist groups, media visibility will be examined in terms of two datasets, that were both created by monitoring Russian-language Telegram channels and performing keyword searches of national media outlets. The first dataset captures 20,985 unique cyberattacks claimed by Russian-language hacktivist groups, targeting 103 distinct countries, that were anniunced on public Telegram postings (and for NoName057(16) through passive monitoring of their DDoSia botnet infrastructure). The second dataset captures 5,521 unique media articles describing Russian hacktivist groups, together sourced from 16 European Union member states which were among the most frequently targeted countries throughout the observation period.

The abovementioned datasets not only provide a basis for the analysis of whether countries with greater media coverage of Russian hacktivist groups experience more frequent cyberattacks. It furthermore allows for cross-national investigations—identifying patterns in media attention across countries with differing levels of media attention—and longitudinal analysis, exploring surge events in media stories and confirming these with a corresponding increase in cyberattacks. The aim is not simply to identify statistically significant correlations, but to also consider the overall strategic logic in terms of media-attentive target behaviour by Russian hacktivist actors. For clarity, the two-part analysis will consider a cross-national relationship between the number of cyberattacks and the amount of media attention paid to those cyberattacks and then consider the temporal characteristics of the media attention within specific countries. Italy serves as predominant case study where the analysis will identify potential signals of peak reporting and attacks.

4.1 Cross-National Patterns of Cyberattacks and Media Visibility

For background to the media analysis that follows, it is useful to first establish which countries were the most frequently targeted by Russian hacktivist groups during the 16-month observation period. As shown on the table 2, the most attacked target was Ukraine with 4246 cyberattacks, followed by Italy (1350), Germany (1210), Poland (1181), and Czechia (1178). Close behind those countries were Spain (1128) and France (1042), and 21 additional countries both within and outside the European Union.

Table 2. List of 26 most attacked countries by Russian hacktivist groups during the 16-month observation period

Country	Number of Cyber Attacks
Ukraine	4246
Italy	1350
Germany	1210
Poland	1181
Czechia	1178
Spain	1128
France	1042
Canada	1016
Finland	630
Austria	485
Denmark	482
Sweden	441
Belgium	417
Switzerland	410
Israel	409
Lithuania	390
Japan	339
Taiwan	329
United States	308
Latvia	301
Netherlands	217
South-Korea	205
Australia	192
Slovenia	187
Luxembourg	178
Estonia	144

Among the top 26 most attacked countries, 16 are member states of the European Union, including all those up to Estonia, which marks the lower boundary of this EU subset with 144 recorded cyberattacks. This distribution reflects the strategic targeting of EU member states by Russian hacktivist groups, due to their political support for Ukraine, alignment with

NATO, and symbolic value in broader geopolitical narratives. The media-focused analysis that follows therefore concentrates specifically on these 16 most attacked EU member states, ranging from Italy to Estonia. By narrowing the scope in this way, the analysis ensures both comparability of media systems and relevance to the central hypothesis, which is that domestic media visibility positively correlates with cyberattack frequency.

One of the first notable findings is the disproportionate volume of media articles originating from Italy compared to other European countries. While Italy did record the highest number of cyberattacks (1,350), its lead over other top-targeted countries such as Germany (1,210), Poland (1,181), and Czechia (1,178) is relatively marginal. Conversely, Italian outlets published 1,175 articles regarding Russian hacktivism which is more than double compared to the number of articles produced by Germany (461), and greater than any other country in the dataset. The degree of difference in Italy's media output demonstrates that Italian media may have been exceptionally responsive or perhaps, more willing to inflate coverage of hacktivism incidents, regardless of whether the number of hacktivism attacks warranted the extensive media coverage.

Table 3. 16 most attacked European Union memberstates during the 16-month observation period.

Country	Number of cyber attacks	Number of media articles
Italy	1350	1175
Germany	1210	461
Poland	1181	245
Czechia	1178	122
Spain	1128	313
France	1042	136
Finland	630	81
Austria	485	60
Sweden	441	56
Belgium	417	147
Lithuania	390	56
Latvia	301	25
Netherlands	217	90
Slovenia	187	45
Luxembourg	178	14
Estonia	144	15

4.1.2 General Patterns and Correlation

The broader dataset reveals several important trends regarding the relationship between the number of cyberattacks and the volume of media coverage across the 16 most targeted EU member states.

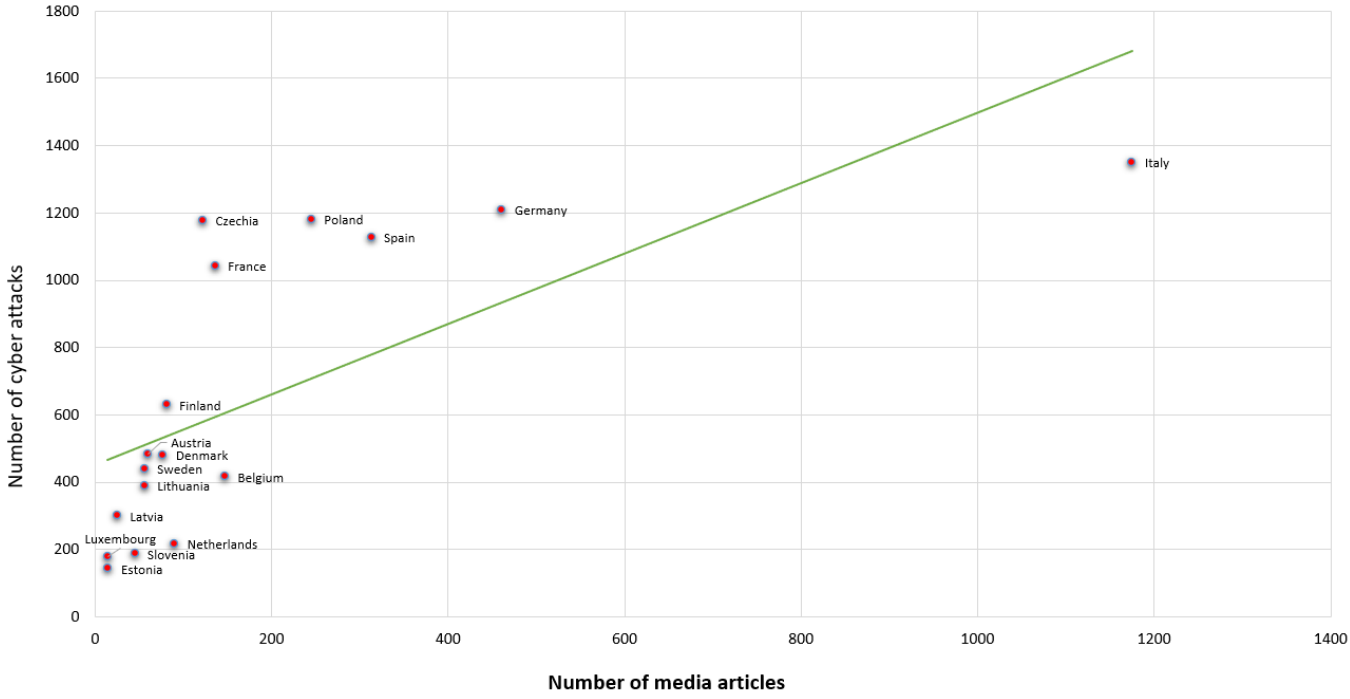

Figure 22. Scatterplot showing the relationship between the number of domestic media articles and the number of Russian hacktivist cyberattacks across European countries (November 2023 – February 2025).

Beyond the case of Italy, there is a general but not strictly linear correlation between the number of cyberattacks and the volume of domestic media articles as illustrated in the figure 23. Countries with a higher frequency of cyberattacks such as Germany (1,210 attacks), Poland (1,181), and Spain (1,128) also tend to exhibit relatively high media visibility, with 461, 245, and 313 articles respectively. However, the strength of this correlation varies, suggesting that while media coverage may partially reflect attack volume, other factors such as media culture, political salience, or public sensitivity may also play critical roles. For example, after Poland and Germany, Czechia had the third highest number of cyberattacks (1178). However, Czechia provided significantly lower number of cyberattacks media coverage (122). The pattern is similar in France (1042 cyberattacks, 136 articles) and Finland (630 cyberattacks, 81 articles), suggesting media attention appears to follow behind the objective levels of threat presented by the hackers. These cases suggest that some national media ecosystems may underreport hacktivist activity or frame it less prominently, potentially due to editorial norms or perceived strategic insignificance.

Although a broad positive correlation can be observed between the number of cyberattacks and the volume of domestic media coverage, several cases stand out for illustrating how higher media attention may be followed by more frequent targeting by Russian hacktivist groups. This supports the hypothesis that greater media visibility may incentivize further attacks, as hacktivist actors often seek public recognition. Countries such as Austria, Sweden, and Lithuania provide clear examples of this pattern's limits. Despite facing hundreds of attacks—485 in the case of Austria, 441 in Sweden, and 390 in Lithuania—these countries generated only minimal media coverage, each publishing between 56 and 60 articles. Their relatively low media visibility may help explain why they were not targeted even more extensively. In these cases, limited public attention could signal to hacktivist actors that further campaigns might yield less recognition or political reaction, thereby reducing the incentive for repeated strikes. The pattern observed here suggests that low media amplification may function as a form of passive deterrence, whether intentionally or not.

Luxembourg and Estonia present interesting cases. The countries published only 14 and 15 relevant articles while being targeted only 178 and 144 times respectively. Both countries have the lowest media engagement in dataset, and either suggest a strategy to limit coverage on cyber threats or even a more limited editorial decision rationale. In Estonia's case, the robust capabilities of their cybersecurity posture, and greater familiarity and awareness of Russia-associated cyber threats may prevent the newsworthiness of such incidents, thus attracting less media retelling and consequently attract less attention from hacktivists. Other countries, such as Belgium, the Netherlands, and especially Italy demonstrate how increased media coverage translates to more sustained or systemic targeting. Belgium, with 147 articles and 417 attacks is somewhat notable for producing more media volume than countries with similar or larger amounts of attacks. The Netherlands (90 articles, 217 attacks), and Spain (313 articles, 1,128 attacks) seem to provide a more clear causal relationship between higher levels of hacktivist attention correlating with better media coverage. These examples reinforce the notion that public media exposure may not merely follow attacks but potentially fuel additional waves of targeting by increasing the symbolic and psychological returns for the perpetrators.

Overall, the analysis of this section suggests a general positive correlation between domestic media coverage and the frequency of Russian hacktivist cyberattacks across EU countries.

Countries like Italy, Germany, and Spain with high media visibility faced the most frequent targeting, indicating that public attention may incentivize further attacks. However, this pattern is not uniform. Countries such as France, Czechia, and Finland experienced many attacks despite limited media coverage, while Estonia and Luxembourg had both low visibility and low attack volumes. These discrepancies suggest that, in addition to media exposure, other factors such as public announcements of military support to Ukraine or outspoken anti-Russian rhetoric may also shape hacktivist target selection.

4.2 Timing and Event-Driven Spikes in Media Attention

While the first part of this analysis examined the cross-national relationship between the frequency of cyberattacks and the volume of media coverage, this section turns to the question of timing. Specifically, it investigates whether domestic media coverage precedes cyberattacks, thereby supporting the hypothesis that increased visibility incentivizes further targeting by Russian-aligned hacktivist groups. The timing of media attention is essential to evaluate if there is a causal correlation. If media articles consistently appear after an attack, it suggests a reactive press and if they appear before, it supports the idea that visibility may itself act as a trigger. To explore this dynamic, the analysis compares two distinct groups of countries. The first group consists of the three most targeted members of the European Union excluding Italy, due to its disproportionate and anomalously high volume of media articles. The second group consists of the three least targeted countries within the top 16 EU states by attack volume. The first group includes Germany, Poland, and Czechia, which experienced over 1,170 attacks each. The second group includes Luxembourg, Estonia, and Slovenia, all of which were targeted fewer than 190 times over the same period. Italy is excluded from this comparative section because its media output with over 1,100 articles is not only an outlier but also shaped by a distinct media environment, characterized by high-volume syndication and frequent redundancy across platforms. By examining the daily sequencing of attacks and media articles in each of these six countries, this subchapter assesses whether media attention appears to provoke, coincide with, or follow cyberattack waves. If the hypothesis holds, one would expect to observe peaks in media coverage before or during attack campaigns, rather than in their aftermath.

4.2.1 Use Case: Germany

The timeline for Germany indicates some general alignment between increases in media attention and increases in cyberattack activity. While same-day correlations between media articles and attacks are limited, a clearer pattern emerges when looking at short-term follow-up periods. Specifically, several instances show that spikes in media attention were followed by a surge in cyberattacks within the next seven days as illustrated in the figure 22.

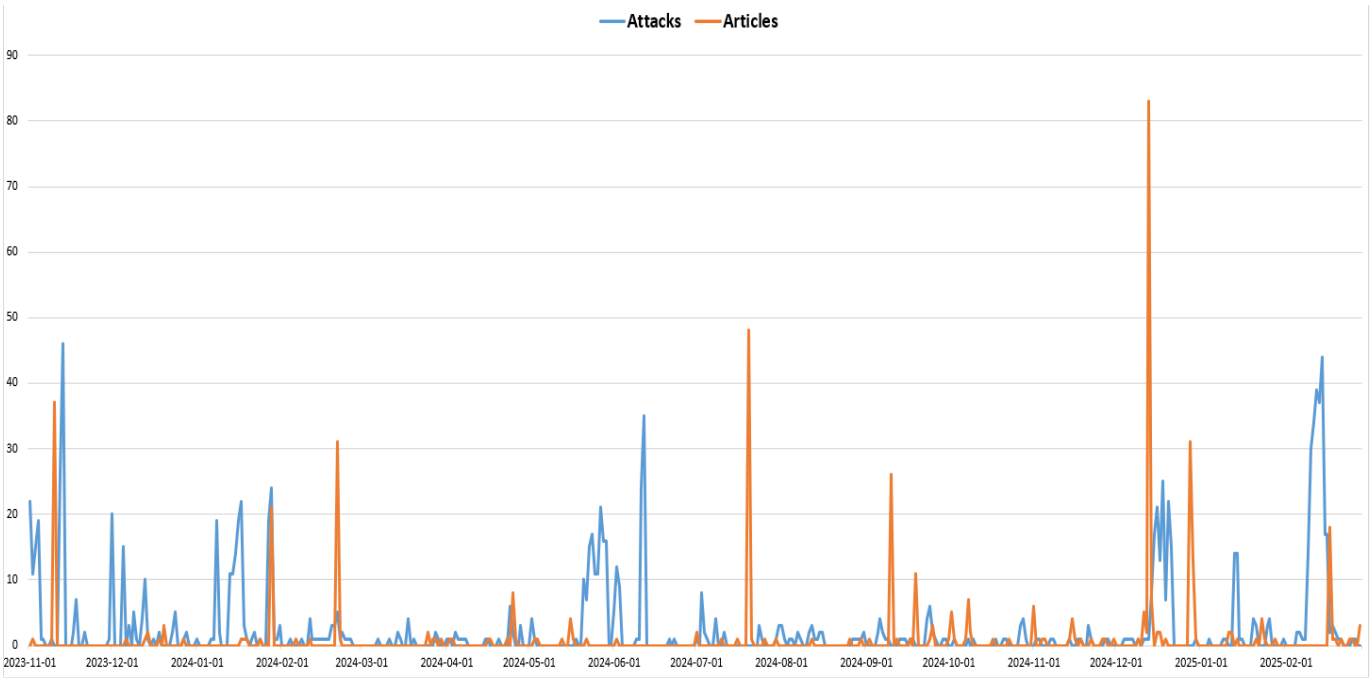

Figure 23. Number of recorded cyberattacks against Germany and domestic media articles mentioning Russian hacktivists in Germany (November 2023 – February 2025).

For example, on December 14, 2024, German media published an unusually high number of articles on Russian hacktivism. In the following week, Germany recorded 120 cyberattacks. Similar patterns occurred around December 13 and December 11, where heightened media visibility was followed by 113 and 86 attacks, respectively. Earlier in the dataset, November 10, 2023, also saw a noticeable media uptick, followed by 74 attacks over the next seven days. Thus, In Germany's case, this suggests that media attention may not merely reflect cyber threat activity but could inadvertently shape it. While geopolitical alignment and military support for Ukraine remain core drivers of targeting, media visibility appears to reinforce and sustain hacktivist interest, particularly when it reaches a certain threshold.

4.2.2 Use Case: Poland

The timeline of cyberattacks and media coverage in Poland reveals a contrasting pattern to countries like Germany. Despite being one of the most frequently targeted EU nations, Polish media coverage of Russian hacktivist activity remains consistently low, even during intense attack periods.

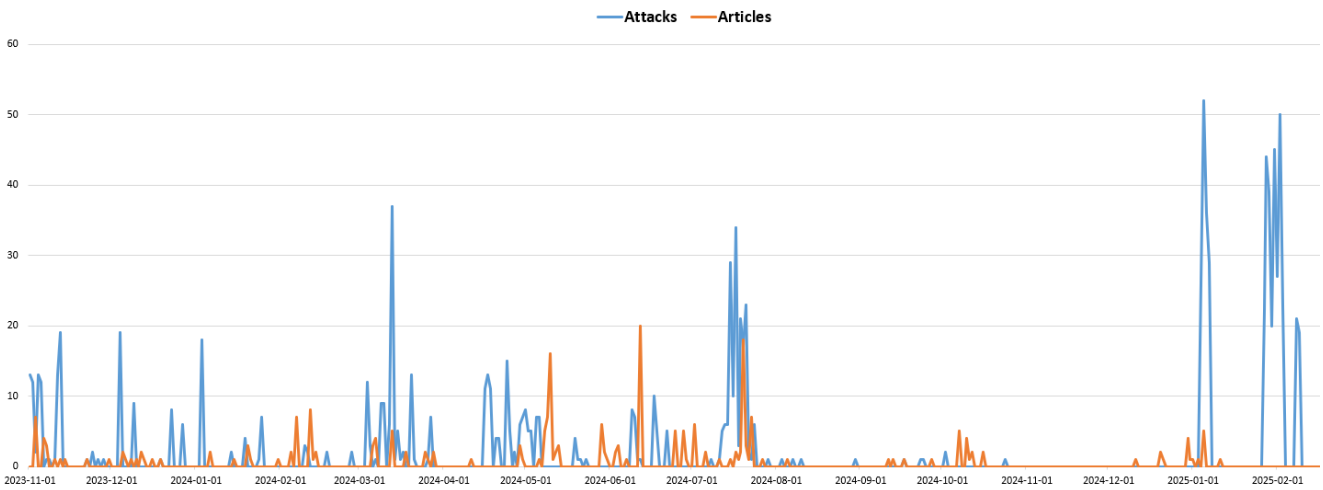

Figure 24. Number of recorded cyberattacks against Poland and domestic media articles mentioning Russian hacktivists in Poland (November 2023 – February 2025).

For instance, during major attack waves in January and February 2025, and again in March and July 2024, Polish media output remained minimal or altogether absent. This suggests that media visibility is not a primary driver of cyberattacks in Poland, at least in terms of immediate or delayed causal influence. Instead, Poland appears to be targeted for other reasons. Its geopolitical role, strong support for Ukraine, and alignment with NATO might be factors regardless of how prominently these attacks are covered by domestic news outlets. While a few short-term spikes in coverage were followed by increases in attacks (e.g., late December 2024), these are exceptions rather than the rule. The overall trend indicates a disconnect between media attention and hacktivist behavior, making Poland an outlier that challenges the general hypothesis of media-driven targeting.

4.2.3 Use Case: Czechia

The data for Czechia reveals that, despite being one of the most frequently targeted EU countries by Russian hacktivists, domestic media coverage remained low and sporadic throughout the 16-month period. While a few dates such as in November 2023 or late summer 2024 show brief increases in article volume, these moments are rare and do not align consistently with the country's numerous attack waves. As illustrated on figure 24, Czechia

experienced intense and repeated cyberattack activity across nearly the entire period, including visible peaks in late 2023, July to August 2024, and late 2024, with little to no corresponding surge in media reporting.

.

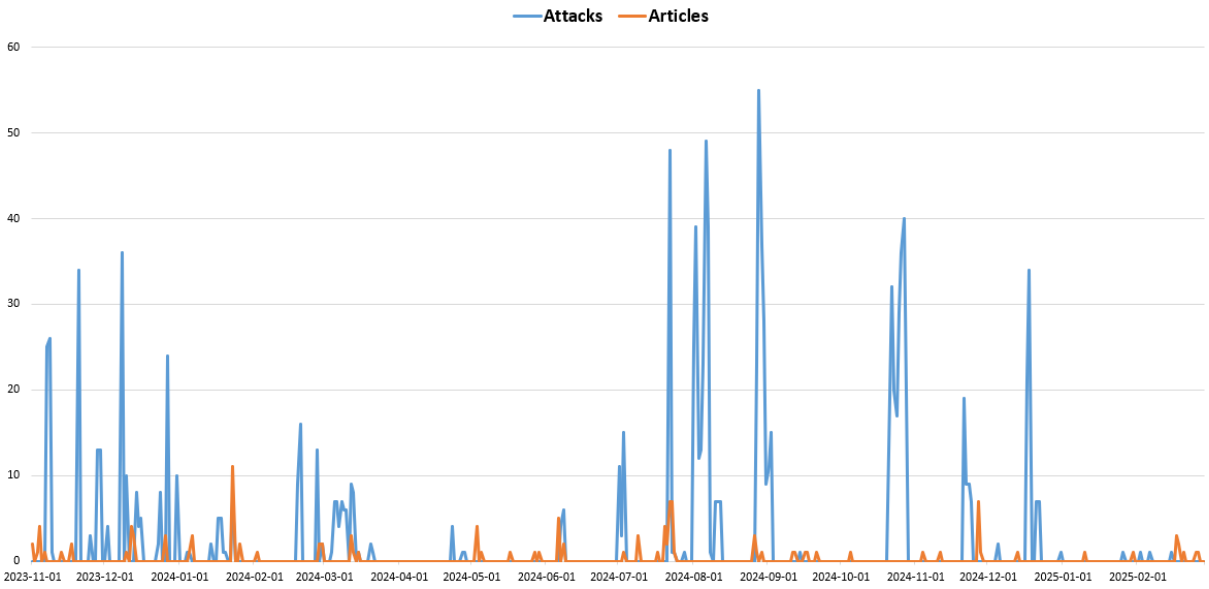

Figure 25. Number of recorded cyberattacks against Czechia and domestic media articles mentioning Russian hacktivists in Czechia (November 2023 – February 2025).

This suggests that media visibility was not a strong influencing factor in the targeting of Czechia. Unlike in Germany, where some article spikes preceded or accompanied attack waves, the Czech case points to a disconnect between media attention and hacktivist behavior. In sum, Czechia provides evidence that high media visibility is not essential for hacktivists to develop a pattern of targeting.

4.2.4 Use Case: Slovenia

Slovenia, one of the least attacked countries, represents an interesting example of episodic visibility leading to temporary interest. As illustrated on the figure 25, the clearest example of this dynamic occurs in late March 2024, when Slovenian media outlets published 11 articles on March 27, marking the country's largest single-day spike in coverage. At that time, only three cyberattacks were recorded. Yet in the days that followed, a sudden surge in attack activity unfolded. Slovenia was hit by 12 attacks on March 28, followed by 6 more on March 29, and continued disruptions into early April. A second, smaller spike in media articles appeared around late June 2024, again followed by a short string of attacks in early July.

Although smaller in scale, this repeated sequence reinforces the idea that visibility might function as a soft signal for hacktivist targeting.

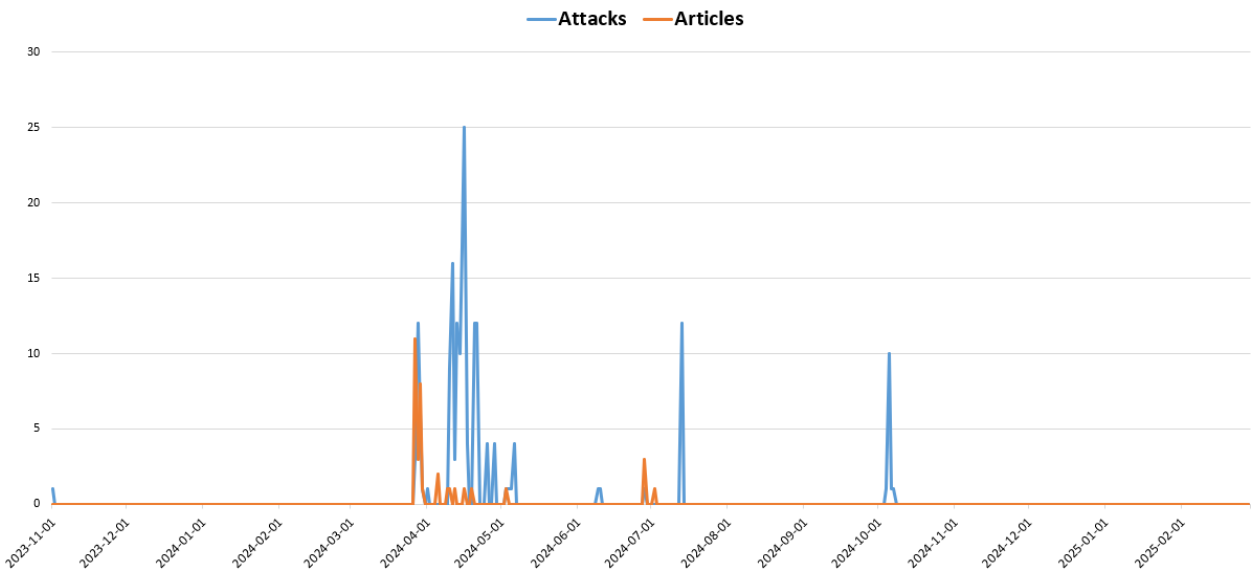

Figure 26. Number of recorded cyberattacks against Slovenia and domestic media articles mentioning Russian hacktivists in Slovenia (November 2023 – February 2025).

Outside of two aforementioned spikes in media attention, Slovenia remained largely ignored, with sustained low media coverage and no significant long-term targeting. This suggests that without continued visibility or geopolitical salience, Slovenia offered little symbolic or propaganda value to Russian hacktivist groups. As such, its case supports the broader pattern where consistent underexposure may act as a passive shield, making countries less attractive targets for Russian hacktivist groups.

4.2.5 Use Case: Luxembourg

Luxembourg experienced a brief and intense wave of cyberattacks in March 2024, with a peak of over 30 incidents in a single day. Notably, this surge in attacks occurred with no significant media coverage at the time. Instead, media articles began to appear much later, from around August 2024 onward, with small, scattered spikes in October, November, and December - none of which were followed by new waves of attacks.

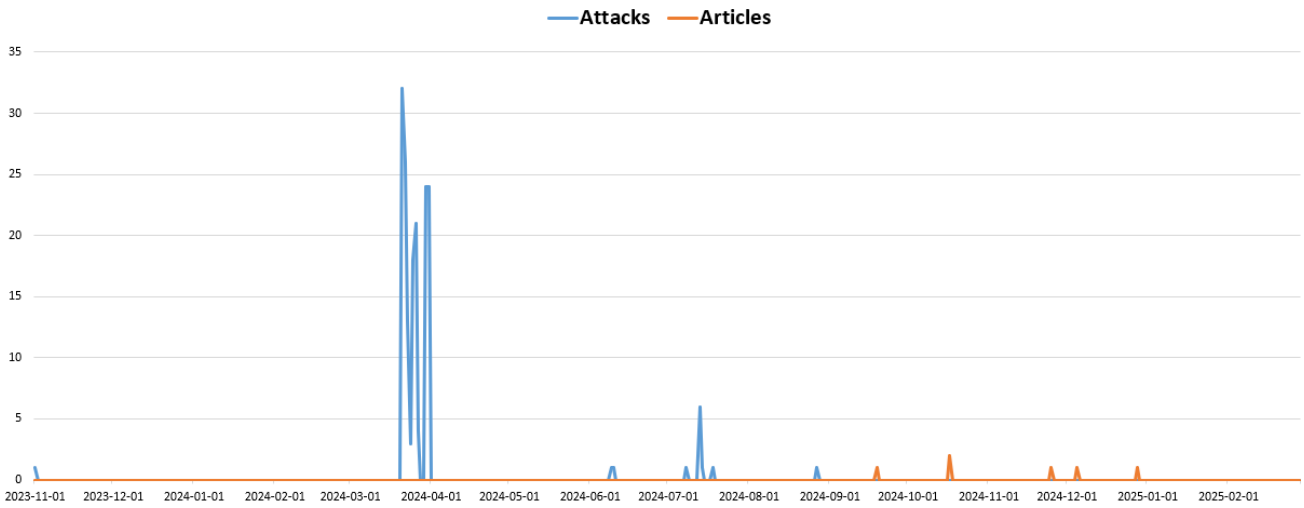

Figure 26. Number of recorded cyberattacks against Luxembourg and domestic media articles mentioning Russian hacktivists in Luxembourg (November 2023 – February 2025).

This temporal disconnect suggests that Luxembourg's targeting was not driven by visibility, nor did later visibility rekindle attacker interest. The initial attack wave may have been opportunistic or misaligned with Luxembourg's perceived relevance in the conflict. Once media attention did increase, it failed to attract further hacktivist activity, likely due to Luxembourg's limited symbolic or geopolitical value. Overall, the case demonstrates that low visibility and strategic irrelevance can insulate a country from sustained targeting, even after isolated surges in either attacks or press coverage. It reinforces the assumption that Russian hacktivists prioritize countries where media amplification, geopolitical stakes, or symbolic impact are higher.

4.2.6 Use Case: Estonia

Estonia, despite expressing strong support for Ukraine and offering significant political support to the country, had the fewest cyberattacks of the EU countries. Like Luxembourg, Estonia had very low levels of media reporting on Russian hacktivist activity. As illustrated in figure 28, Estonia was also not preceded by any significant media spikes prior to attacks. It is notable that there was a low level of media coverage and a low volume of cyberattacks throughout the analysis period. This suggests that Estonia's low level of media hyper-visibility and high levels of cyber maturity may have also lowered the symbolic appeal to hacktivist groups to attack Estonia notwithstanding its geopolitical relevance. Estonia's case provides strong evidence for the proposition that low levels of media visibility mitigate a country's exposure to hacktivist campaigns.

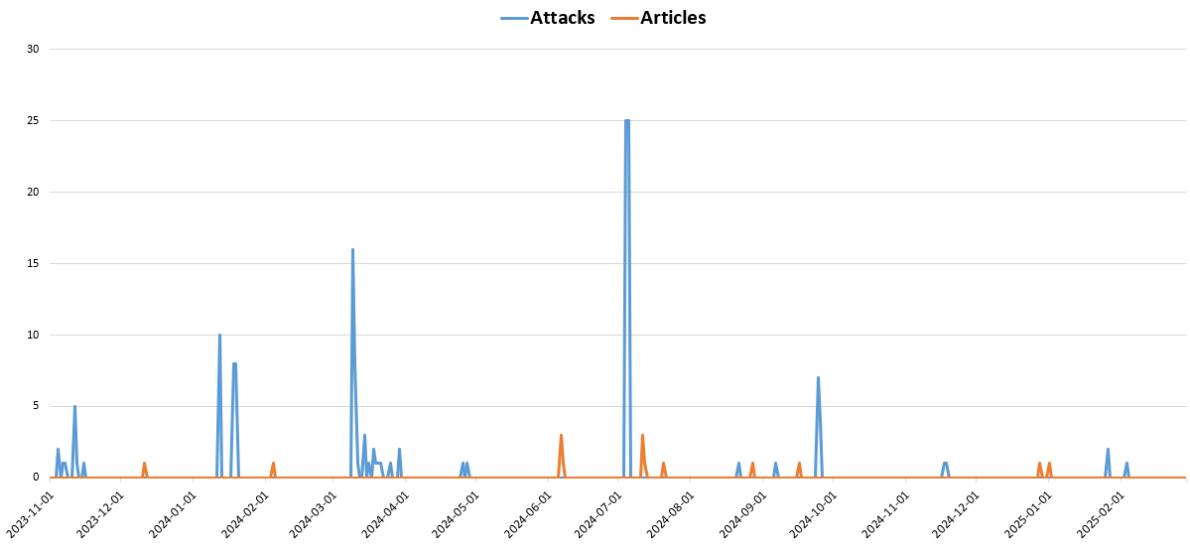

Figure 27. Number of recorded cyberattacks against Estonia and domestic media articles mentioning Russian hacktivists in Estonia (November 2023 – February 2025).

5. Conclusion

This thesis set out to examine the emergence and characteristics of post-2022 Russian hacktivism, focusing on two interlinked objectives. The first objective was to conceptualize the Telegram-based Russian hacktivism as a new phenomenon that differs from the previous generations of hacktivism in terms of motivation, structure, target selection and operational organization. The second objective was to explore whether the amount of visibility these groups have gained in national media correlates to the number of cyberattacks which these groups have claimed against those countries - thereby assessing whether media coverage might serve as an incentive for future attacks. Both aims were derived from a more general research problem concerning the lack of information about the nature and operational logic of contemporary Russian hacktivist groups as well as the lack of known countermeasures.

The thesis sought to answer two central research questions: 1. In what ways does Telegram-based Russian hacktivism differ from earlier forms in terms of motivations, methods, and operational logic? 2. To what extent does domestic media coverage influence the frequency of cyberattacks claimed by Russian hacktivist groups? To answer these questions, the thesis introduced a theoretical framework built upon a historical periodization of hacktivism. It proposed a three-era model, distinguishing the first era of ethical, symbolic hacktivism (1990s–early 2000s), the second era of decentralized and confrontational collectives (mid-2000s–2010s), and the third era of centralized, profit-driven Telegram-based Russian hacktivism that has surged since the full-scale invasion of Ukraine in 2022. The first two eras from the framework were constructed by using existing academic literature on earlier generations of hacktivism. The underlying characteristis found in the litearature were later compared to post-2022 hacktivism, which constitutes a third era of hacktivism. This framework provided a basis for systematically assessing whether contemporary Russian hacktivist groups represent a continuation of earlier practices or a meaningful departure. By applying this typology to empirical material gathered through direct observation, the thesis was able to identify how current Russian hacktivism blends ideological, financial, and performative elements in ways not previously captured by traditional definitions of digital activism.

To conceptualize post-2022 Russian hacktivism and the potential relationship between media visibility and cyberattack frequency, this thesis adopted a mixed-methods research design.

The qualitative component aimed to conceptualize Telegram-based Russian hacktivism as a distinct phenomenon. It involved the manual monitoring of 48 Russian-language hacktivist Telegram groups over a 16-month period (November 2023 to February 2025). This first-hand data collection enabled the systematic coding of key operational features of the monitored groups, such as motivations, target selection, attack types, communication strategies, monetization methods, and recruitment practices. The goal of this approach was to identify recurring patterns and organizational logics that could distinguish contemporary Russian hacktivist groups from earlier generations of digital activism. The quantitative component was designed to assess whether media coverage influences the targeting behavior of Russian hacktivist groups. Two original datasets were compiled for this purpose: one documenting over 20,000 publicly claimed cyberattacks by Russian hacktivists, and another logging more than 5,500 domestic media articles referencing these groups across 16 EU member states. By comparing country-level media visibility with cyberattack frequency over time, the analysis sought to determine whether increased public attention corresponds with elevated levels of targeting. This dual approach, conceptual and correlational, was selected to both capture the internal characteristics of the phenomenon and examine its external strategic dynamics.

The results of the qualitative analysis indicate that the post-2022 Russian hacktivism should be viewed as a distinct version of hacktivism. While these Telegram-based Russian hacktivist groups adopt the language of political resistance, their actions are shaped by geopolitical opportunism, visibility-seeking behavior, and financial incentives. Their operations are mainly reactive and mostly aligning with Russia-Ukraine war related media coverage and political events. However, they lack the ideological consistency of earlier hacktivist collectives. Their cyberattacks, particularly DDoS campaigns, are technically more simplistic compared to earlier generations of hacktivist activity. However, they are frequently aimed at civilian infrastructure such as banking systems, transportation networks, and public services, increasing their disruptive impact on everyday life. Additionally, their recruitment processes are task-based and selective, further signaling a shift toward quasi-professional organization. Most of these operational characteristics further signify a major departure from hacktivism as a form of digital activism, and rather, a semi-criminal performative practice hidden within the general architecture of information warfare in Russia.

The results of the quantitative analysis addressing the extent to which domestic media coverage influences the frequency of cyberattacks claimed by Russian hacktivist groups, reveal a generally positive, but inconsistent, relationship. Countries like Italy, Germany, and

Spain—where media coverage was relatively high—also experienced higher attack volumes, suggesting that visibility may incentivize targeting. However, this pattern did not hold uniformly. Several countries, such as Poland and Czechia, faced frequent cyberattacks despite limited media attention, indicating that other factors—such as geopolitical alignment—also play a significant role. In the second stage of the analysis, the temporal relationship between media reporting and attack frequency was examined in a subset of countries to assess whether media visibility could act as a short-term trigger. This timing analysis revealed that in only a few cases—most notably Germany and Slovenia—spikes in media coverage were followed by a noticeable surge in cyberattacks. In most other cases, no clear temporal link could be established. These findings suggest that while media attention may contribute to hacktivist targeting decisions in select contexts, it is not a consistent or universal driver. Strategic, political, and symbolic considerations continue to shape attack behavior alongside, and sometimes independently from, public visibility.

From these findings, several conclusions can be drawn. First, the post-2022 Russian hacktivism landscape should be viewed as a distinct phase of the evolution of hacktivism that has nothing to do with classical digital activism and instead combines ideological signaling, financial opportunism, and propaganda. Second, these groups work in an operational logic that is primarily performative: rather than impacts, visibility is the end goal, and domestic media ecosystems unknowingly act as targeting environments. Third, media coverage is not a passive reflection of cyber incidents, it might potentially produce them. If hacktivists use shared public narratives to pursue visibility and legitimacy, national media outlets can become unwitting agents in targeting dynamics. This leads to broader implications for both policy and media practice. Governments and media outlets in targeted states must recognize that publicity may inadvertently incentivize further attacks. This is not to advocate censorship, but to suggest that national media outlets should carefully consider how their reporting practices may unintentionally amplify the propaganda aims of hostile actors. At the same time, awareness of this visibility loop could inform public communication strategies that reduce symbolic payoffs without compromising transparency. For cybersecurity practitioners, understanding hacktivism as a media-driven phenomenon may help prioritize protective resources, especially around high-visibility events, government anniversaries, or media-intense political moments.

The findings of this thesis provide a foundation for future research on the topic of the evolving landscape of hacktivism. While this thesis centered on post-2022 Russian hacktivist

groups, scholars should explore the applicability of these dynamics to other third-era Telegram-based collectives, such as those with pro-Palestinian or radical Islamist affiliations. Furthermore, future research should critically examine the suitability of the term "hacktivist" for these Russian collectives, given their divergence from established digital activism. Future studies could also assess the efficacy of media minimization strategies or examine alternative drivers, including measuring the effect of public officials rhetoric that can be considered as anti-Russian or overall cyber-resilience posture. Finally, future research could employ statistical models that are potentially more sophisticated in order to refine the correlation measures, or to investigate causality more rigorously.

References

Albalawi, M., Aloufi, R., Alamrani, N., Albalawi, N., Aljaedi, A., & Alharbi, A. R. (2022). Website defacement detection and monitoring methods: A review. Electronics, 11(21), 3573.

Alexopoulou, S., & Pavli, A. (2021). 'Beneath This Mask There Is More Than Flesh, Beneath This Mask There Is an Idea': Anonymous as the (Super) Heroes of the Internet?. *International Journal for the Semiotics of Law-Revue internationale de Sémiotique juridique*, *34*(1), 237-264.

Baringhorst, S. (2014). Internet und Protest. Zum Wandel von Organisationsformen und Handlungsrepertoires–Ein Überblick. In: Voss, K. (eds.), Internet und Partizipation: Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet (pp. 89-113). Springer.

Bhadouria, A. S. (2022). Study of: impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications, 10(10), 1-11.

Best, K. (2003). The Hacker's Challenge: Active Access to Information, Visceral Democracy and Discursive Practice. Social Semiotics. 13(3).

Budge, I. (1981). Political Action: Mass Participation in Five Western Democracies. By Samuel H. Barnes, Max Kaase and Associates.(Beverly Hills, Calif.: Sage Publications, 1979. Pp. 609). American Political Science Review, 75(1), 221-222.

Brooks, R. R., Yu, L., Ozcelik, I., Oakley, J., & Tusing, N. (2021). Distributed denial of service (DDoS): a history. IEEE Annals of the History of Computing, 44(2), 44-54.

Brunk, I. & Hakimi, M. (2022). Russia, Ukraine, and the Future World Order. American Journal of International Law, 116(4), 687–697

Canevez, R. N., Maikovska, K., & Zwarun, L. (2024). Tactics and affordances in the mediatization of war: pro-Ukrainian cyber resistance on Telegram. Digital War, 5(3), 167-180.

Chaudhary, S., & Mishra, P. K. (2023). DDoS attacks in Industrial IoT: A survey. Computer Networks, 236.

Chopitea, T. (2012). Threat modelling of hacktivist groups Organization, chain of command, and attack methods.

Coleman, G. (2013). Anonymous in context: The politics and power behind the mask.

Dautaj, A. (2018). FSociety: Hacktivism and the Disruptive Innovation of the Social Movement. Central European University.

Denning, D. E. (2001). Activism, hacktivism, and cyberterrorism: The Internet as a tool for influencing foreign policy. Networks and netwars: The future of terror, crime, and militancy, 239, 288.

Denzin, N. K., & Lincoln, Y. S. (Eds.). (2018). The SAGE handbook of qualitative research (5th ed.). SAGE Publications.

Dominguez, R. (2016). Fearless Art in the Age of Fear: Electronic Disturbance Theater's Parrhesian Gestures. Social Research: An International Quarterly, 83(1), 107-113.

Dominguez, R. (2009). Electronic civil disobedience: Inventing the future of online agitprop theater. PMLA, 124(5), 1806-1812.

Dosek, T. (2021). Snowball Sampling and Facebook: How Social Media Can Help Access Hard-to-Reach Populations. PS: Political Science & Politics, 54(4), 651–655.

Douligeris, C., & Mitrokotsa, A. (2004). DDoS attacks and defense mechanisms: classification and state-of-the-art. Computer networks, 44(5), 643-666.

Farmer, F. (2022). Cybercrime vs Hacktivism: Do we need a differentiated regulatory approach?. University of Exeter (United Kingdom).

Fielitz, M., & Staemmler, D. (2020). Hashtags, Tweets, Protest? Varianten des digitalen Aktivismus. Forschungsjournal Soziale Bewegungen, 33(2), 425-441.

Furnell, S. (2003). Cybercrime: Vandalizing the Information Society. In: Lovelle, J.M.C., Rodríguez, B.M.G., Gayo, J.E.L., del Puerto Paule Ruiz, M., Aguilar, L.J. (eds.) Web Engineering. ICWE 2003. Lecture Notes in Computer Science, vol 2722. Springer, Berlin, Heidelberg.

Gabriel, O. W. (2013). Politische Partizipation. Politik im Kontext: ist alle Politik lokale Politik? individuelle und kontextuelle Determinanten politischer Orientierungen (pp. 381-411). Springer.

Gorham, A. (2015). Does information want to be free? Hacktivism and the democratization of information. *The Journal of International Relations, Peace Studies, and Development*, *1*(1), 7.

Grindal, K. (2022). Artist collectives as the origins of ddos the strano network and electronic disturbance theater. IEEE Annals of the History of Computing, 44(3), 30-42.

Grossman, T., Kaminska, M., Shires, J., & Smeets, M. (2023). The cyber dimensions of the russia-ukraine war. European Cyber Conflict Research Initiative.

Guchua, A., & Zedelashvili, T. (2023). Anonymous Sudan and Killnet Factor in the Russia-Ukraine War in the Context of Cyber Security. Future Human Image, 19.

Harbers, I., & Ingram, M. C. (2020). Mixed-methods designs. In The SAGE Handbook of Research Methods in Political Science and International Relations (pp. 1117-1132). SAGE Publications.

Hamid, N. (2018). The British Hacker Who Became the Islamic State's Chief Terror Cybercoach: A Profile of Junaid Hussain. *CTC Sentinel*, *11*(4), 30-37.

Hearn, K., Mahncke, R. J., & Williams, P. A (2009). Culture Jamming: From Activism to Hactivism. Australian Information Warfare and Security Conference.

Heckathorn, D. D. (2011). Comment: Snowball versus respondent-driven sampling. Sociological methodology, 41(1), 355-366.

Heffelfinger, C. (2013). The Risks Posed by Jihadist Hackers. *CTC Sentinel*, *6*(7).

Held, W. V. (2012). Hacktivism: An analysis of the motive to disseminate confidential information.

Holt, T. (2020). Computer Hacking and the Hacker Subculture. In: T. J. Holt & A. M. Bossler (eds.), The Palgrave handbook of international cybercrime and cyberdeviance (Vol. 2, pp. 725-742). Springer.

Jensen, M. J., Jorba, L., & Anduiza, E. (2012). Introduction. In E. Anduiza, M. J. Jensen, & L. Jorba (eds.), Digital Media and Political Engagement Worldwide: A Comparative Study (pp. 1–15). Cambridge University Press.

Jordan, T., & Taylor, P. (2004). Hacktivism and cyberwars: Rebels with a cause?. Routledge.

Karagiannopoulos, V. (2018). Living with hacktivism. From conflicts to Symbiosis. Palgrave Macmillan.

Kubicek, H., Lippa, B. & Westholm, H. (2009). Medienmix in der Bürgerbeteiligung Die Integration von Online-Elementen in Beteiligungsverfahren auf lokaler Ebene. Nomos.

Machado, M. B. (2015). Entre o controle e o ativismo hacker: a ação política dos Anonymous Brasil. *História, Ciências, Saúde-Manguinhos*, *22*, 1531-1549.

Maggetti, M. (2020). Mixed-methods designs. In: C. Wagemann, A. Goerres, & M. B. Siewert (eds.), Handbuch Methoden der Politikwissenschaft (pp. 193 - 211). Springer

Manion, M., & Goodrum, A. (2000). Terrorism or civil disobedience: toward a hacktivist ethic. Acm Sigcas Computers and Society, 30(2), 14-19.

Mao, B. M., & Bagolibe, K. D. (2019). A contribution to detect and prevent a website defacement. 2019 International Conference on Cyberworlds (CW) (pp. 344-347).

McGraw, G. (2016). Silver Bullet Talks with Peiter (Mudge) Zatko. IEEE Security & Privacy, 14(01), 7-10.

Menn, J. (2019). Cult of the dead cow: how the original hacking Supergroup might just save the world. PublicAffairs.

Mejia, Y. (2017). Truth or dare: anonymous--a self-proclaimed cyber anarchist movement.

Milone, M. (2003): Hacktivism: Securing the national infrastructure. Knowledge, Technology & Policy, 16(1), 75–103.

Milan, S. (2015). Hacktivism as a radical media practice. In The Routledge companion to alternative and community media (pp. 550-560). Routledge.

Mikhaylova, G. (2014). The" Anonymous" Movement: Hacktivism as an Emerging Form of Political Participation.

Mollick, E. (2005). Tapping into the underground. *MIT Sloan management review*, *46*(4), 21.

Mordowanec, N (2022). Russian Hacker Warns Cyberwarfare Will Turn Deadly. URL: https://www.newsweek.com/deadly-cyberwarfare-warning-russian-hacker-killnet-1731949 [19.05.2025]

Murdoch, S. (2010). Destructive activism: The double-edged sword of digital tactics. In: Joyce, M. C. (eds.), Digital Activism Decoded: The new mechanics of change (pp. 137-148). International Debate Education Association.

Murphy, S. (2011). The heart of a hacker. *New Scientist*, *211*(2820), 26-27.

Müller, S. D., & Ulrich, F. (2015). The competing values of hackers: The culture profile that spawned the computer revolution. 48th Hawaii International Conference on System Sciences (pp. 3434-3443).

Nejjari, N., Zkik, K., Hammouchi, H., Ghogho, M., & Benbrahim, H. (2024). Assessing Data Breach Factors Through the Lens of Modern Crime Theory: A Structural Equation Modeling „„Approach.

Nguyen, T. H., Hoang, X. D., & Nguyen, D. D. (2021). Detecting Website Defacement Attacks using Web-page Text and Image Features. International Journal of Advanced Computer Science and Applications, 12(7).

Norris, P. (2009). Political Activism: New Challenges, New Opportunities. In Boix, C. & Stokes, S. (eds), The Oxford Handbook of Comparative Politics (pp. 629-650). Oxford University Press.

Pendergrass, S., & Morris, R. (2012). Hackers gone wild: the 2011 spring break of lulzsec. Issues in Information Systems, 13(1), 133-143.

Richards, I., & Wood, M. A. (2018). Hacktivists against Terrorism: A Cultural Criminological Analysis of Anonymous' Anti-IS Campaigns. International journal of cyber criminology.

Romagna, M. (2020). Hacktivism: Conceptualization, techniques, and historical view. In: T. J. Holt & A. M. Bossler (eds), The Palgrave handbook of international cybercrime and cyberdeviance (Vol. 2, pp. 743–769). Springer.

Romagna, M., & Van den Hout, N. J. (2017). Hacktivism and website defacement: motivations, capabilities and potential threats. In 27th virus bulletin international conference (Vol. 1, pp. 1-10).

Samuel, A. (2004). Hacktivism and the future of democratic discourse. In Democracy Online (pp. 143-160). Routledge.

Sauter, M. (2014). The coming swarm: DDOS actions, hacktivism, and civil disobedience on the Internet. Bloomsbury Academic.

Singer, P. W., & Friedman, A. (2014). Cybersecurity and Cyberwar: What Everyone Needs to Know. Oxford University Press.

Snyder, O. (2022). Hacktivism's Threat to Cyber Security Today. Available at SSRN: https://ssrn.com/abstract=4073748

Tavakkoli, N., Çetin, O., Ekmekcioglu, E., & Savaş, E. (2025). From frontlines to online: examining target preferences in the Russia–Ukraine conflict. International Journal of Information Security, 24(1), 1-15.

Varbanov, V., Kopanov, K., & Atanasova, T. (2024). A Multidisciplinary Approach to Telegram Data Analysis.

Verba, S., & Nie, N. H. (1972). Participation in America: Political Democracy and Social Equality. New York: Harper & Row.

Voss, K. (2014). Internet & Partizipation–Einleitung. In: Voss, K. (eds.), Internet und Partizipation: Bottom-up oder Top-down? Politische Beteiligungsmöglichkeiten im Internet (pp. 9-23). Springer.

Özçelik, İ., & Brooks, R. (2020). Distributed denial of service attacks: Real-world detection and mitigation. CRC Press.

Yang, J. (2013). Post-Lulzsec Cybersecurity. Insight and Inquiry, 6(1), 46-64.

Appendicies

Appendix 1. Python Script for Determining Website Country of Origin

```python
import pandas as pd
import socket
import requests

def get_country(domain):

    domain = str(domain).replace("http://", "").replace("https://", "").rstrip("/")
    try:
        ip = socket.gethostbyname(domain)
        response = requests.get(f'http://ip-api.com/json/{ip}')
        data = response.json()
        return data.get('country', 'Unknown')
    except Exception as e:
        print(f"Error processing {domain}: {e}")
        return 'Unknown'

def is_international_domain(domain):

    if not isinstance(domain, str):
        return False
    domain = domain.replace("http://", "").replace("https://", "").rstrip("/")
    if '.' in domain:
        tld = domain.split('.')[-1].lower()

        if tld in ['com', 'org', 'net', 'info', 'biz']:
            return True

        if len(tld) > 2:
            return True
    return False


df = pd.read_excel('test2.xlsx')


for index, row in df.iterrows():
    website = row['Sihtmärk']
    if is_international_domain(website):
        origin = get_country(website)

        df.at[index, 'Riik2'] = origin
        print(f"Processed row {index+1}: {website} -> {origin}")
    else:
        print(f"Skipped row {index+1}: {website}")


df.to_excel('updated_websites.xlsx', index=False)
print("File saved as updated_websites.xlsx")
```

Appendix 1 is a Python script that was developed to identify the likely country of origin for websites listed in the cyber attack dataset. The script begins by cleaning the domain names, removing common URL prefixes and trailing characters to standardize the input. It then checks whether a domain uses a generic international top-level domain such as .com, .org, or .net, which are filtered in order to find out their country of origin. For domains that pass this filter, the script resolves the domain to an IP address and queries an external API (ip-api.com) to retrieve the country associated with that IP. The script processes each row of an Excel file, extracts the domain from a specific column, and records the identified country into another column only if the domain is considered non-international like .ee for Estonia, .de for germany etc. The dataset is then saved to a new Excel file.