Assoc. Prof. Urszula Soler, PhD
Department of Theory of Politics and Eastern Studies
Institute of Political Science and Public Administration
Faculty of Social Sciences, The John Paul II Catholic University of Lublin
E-mail: urszula.soler@kul.pl
Telephone: 81 445-33-53
ORCID ID: 0000-0001-7868-8261
www.kul.pl

Stefano Lovi, PhD Student
University of International Studies of Rome UNINT
E-mail: stefano.lovi@unint.eu
ORCID ID: 0009-0009-9978-8689

THE ROLE OF TELEGRAM IN COORDINATING CYBER ATTACKS AND PROPAGANDA CAMPAIGNS BY RUSSIAN HACKERS

Abstract

The purpose of the article was to analyze the role of the Telegram platform in the cyber and disinformation activities of Russian hacking groups (APTs) during the war in Ukraine. The authors focused on examining how Telegram supported the organization of attacks, propaganda, recruitment of saboteurs, and real-time management of operations. The responses of the international community (including Poland, the US and the UK) and key cybersecurity challenges are also discussed in this context. Telegram has evolved from an application designed for secure communication into a multifunctional tool used by pro-Russian APT groups. Its features - strong encryption, lack of content moderation, and ease of channel creation - allow them to coordinate cyberattacks, spread disinformation, and recruit collaborators. Groups such as Gamaredon and Sandworm use Telegram to attack Ukraine's public infrastructure, while NoName057(16) organizes DDoS attacks on institutions of countries supporting Ukraine. The conclusions of the analysis show that Telegram has become not only a communication tool, but even an operational center for hybrid operations. The authors emphasize the urgent need to develop defense strategies - both technological and social. Raising awareness among users and systematic training in threat detection are extremely important. This is the only way to build a resilient cybersecurity culture capable of responding effectively to the challenges posed using Telegram as a weapon in modern information warfare.

Key words: Telegram, cyber threats, cybersecurity, war in Ukraine

INTRODUCTION

In recent years, the digital landscape has undergone a profound transformation, changing not only the methods of disseminating information, but also the ways in which it is used. From an academic perspective, it is crucial to take a critical approach to assessing the impact of this change, especially in the context of the rapid spread of disinformation on popular social media platforms. This raises questions about the reliability of the content being transmitted and the intentions behind its dissemination. Numerous scientific studies highlight the transformation of terrorism in the digital age, indicating that cyberspace has become a key domain for the intensification of terrorist activities[1].

In this context, in addition to official channels of communication, alternative have emerged, such as Telegram. It offers a secure and often anonymous environment that is used not only for private communication, but also for coordinating cyber-attacks and implementing propaganda campaigns. The platform acts not only as a primary communication tool, but also as a strategic operations centre for Russian hackers, who are increasingly using its unique features to carry out a variety of illegal activities.

Telegram has evolved from a simple messaging platform into a powerful tool for communication, coordination, and information dissemination. While originally designed as a secure app with strong encryption features, it has increasingly been exploited by state-sponsored cybercriminal groups, particularly those aligned with Russia. These groups leverage Telegram not only to coordinate cyber-attacks but also to recruit operatives, share malicious tools, and execute large-scale propaganda efforts aimed at shaping public perception[2].

The complexity of Telegram's use in such contexts is exacerbated by the evolving cyber threats accompanying rapid technological advances. This creates an increasingly dangerous situation for both individuals and institutions, especially in the context of ongoing hybrid wars. Numerous scientific studies highlight the transformation of terrorism in the digital age, indicating that cyberspace has

[1] M.S. Lund, *Hybrid threats in cyberspace. What do Russia's cyberspace operations in Ukraine tell us?*, in: O.J. Borch & T. Heier (Eds.), *Preparing for Hybrid Threats to Security: Collaborative Preparedness and Response* (1st ed.), Routledge, https://doi.org/10.4324/9781032617916 (retrieved: 12.04.2025); S.I. Kuzina, I.G. Sagiryan, *Cyberterrorism as a Real Threat to the National Security of the Russian Federation*, Legal Order and Legal Values, 2024, https://www.semanticscholar.org/paper/92fb4a58134040e33dc1ac6a6358afb1fa276f09 (retrieved: 12.04.2025); M. Karpiuk, C. Melchior, U. Soler, *Cybersecurity Management in the Public Service Sector*, *Prawo i więź*, nr 4(47)/2023, ss. 9–29, https://doi.org/10.36128/PRIW.VI47.751 (retrieved: 12.04.2025); K. Kaczmarek, M. Karpiuk, U. Soler, *The Potential Use of Artificial Intelligence in Crisis Management*, *Sicurezza, Terrorismo e Società*, 2/2024, pp. 141–151 (retrieved: 12.04.2025).

[2] M. Albrecht, L. Mareková, K.G. Paterson, I. Stepanovs, *Four attacks and a proof for Telegram*, IEEE Symposium on Security and Privacy, San Francisco, 2022, pp. 87–106, https://doi.org/10.1109/SP46214.2022.9833666 (retrieved: 13.04.2025).

become a key domain for the intensification of terrorist activities[3]. When analyzing this phenomenon, it is important to consider how such changes significantly increase the reach and impact of harmful campaigns, capable of affecting a wide range of individuals and institutions around the world[4]. Therefore, understanding these complex dynamics is essential to show the multi-faceted role of Telegram in modern cyberwarfare and the broader implications for international security and digital sovereignty, while remaining vigilant to the ethical challenges posed by such far-reaching technological developments.

The Russian invasion of Ukraine in 2022 marked a turning point in the use of Telegram as a cyber-warfare tool. Since then, Russian Advanced Persistent Threat (APT) groups have intensified their reliance on the platform, using it to launch Distributed Denial of Service (DDoS) attacks, malware campaigns, and disinformation efforts designed to destabilize adversaries. The platform's encrypted communication features, ease of use, and lack of strict content moderation have made it an ideal space for covert cyber operations. The extent to which Telegram has facilitated Russian cyber campaigns cannot be underestimated, as it plays a crucial role in spreading disinformation, recruiting hackers, and controlling compromised networks.

The purpose of this article is to analyze the impact of the Telegram platform on Russian cyber and disinformation operations during the war in Ukraine, with a particular focus on its use by Advanced Persistent Threat (APT) groups. The article seeks to understand how Telegram supports the organization of cyberattacks, propaganda efforts, recruitment of saboteurs, and real-time management of operations, as well as the challenges this poses to the countries targeted by such activities.

To achieve this goal, the following research questions were formulated:

[3] N.M. Ochara, N.A. Odhiambo, A. Kadyamatimba, *The digitalised terrorism ecology: A systems perspective*, The African Journal of Information and Communication (AJIC), vol. 25, 2020, pp. 1–19, https://doi.org/10.23962/10539/29196 (retrieved: 13.04.2025); C.S. Adigwe, N.R. Mayeke, S.O. Olabanji, O.J. Okunleye, P.C. Joeaneke, O.O. Olaniyi, *The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks*, Asian Journal of Economics, Business and Accounting, vol. 24, no. 3, 2024, pp. 289–306, https://doi.org/10.9734/ajeba/2024/v24i31287 (retrieved: 13.04.2025); A. Kruglova, *Terrorist recruitment, propaganda and branding: Selling terror online*, Abingdon; New York: Routledge, 2023, p. X, 181, ISBN: 9781032249186 (retrieved: 17.04.2025); N. Lawrence, B.W. Robertson, *Extremist organizations and online platforms: A systematic literature review*, Qualitative Research Reports in Communication, vol. 25, no. 1, 2023, pp. 93–103, https://doi.org/10.1080/17459435.2023.2240808 (retrieved: 13.04.2025); D. Ball, R. Montasari, *The evolution of terrorism in digital era: Cyberterrorism, social media, and modern extremism*, in: R. Montasari, H. Jahankhani, A.J. Masys (eds), *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance*, Advanced Sciences and Technologies for Security Applications, Springer, Cham, 2025, https://doi.org/10.1007/978-3-031-72821-1_9 (retrieved: 13.04.2025).

[4] G. Ptaszek, B. Yuskiv, S. Khomych, *War on frames: Text mining of conflict in Russian and Ukrainian news agency coverage on Telegram during the Russian invasion of Ukraine in 2022*, Media, War & Conflict, vol. 17, no. 1, 2023, pp. 41–61, https://doi.org/10.1177/17506352231166327 (retrieved: 12.04.2025).

- What features of Telegram make it an attractive cyber warfare tool for Russian APT groups?
- How are Russian APT groups using Telegram to coordinate cyberattacks and conduct disinformation campaigns against Ukraine and other countries?
- How are international communities (e.g. Ukraine, Poland, USA, UK) responding to the threats posed by the use of Telegram in warfare and disinformation operations?
- What are the main cybersecurity challenges related to the presence of Russian hacking groups on Telegram?

The goal was achieved by using the method of analyzing existing literature and available media sources, primarily those found on the Internet.

TELEGRAM IN THE SPOTLIGHT OF RESEARCHERS - STATE OF RESEARCH

Among the first signs of Telegram's growing role in cyberattacks were reports from companies such as ESET, Palo Alto Unit42, and Check Point, which tracked the activities of Russian APTs. Malware (e.g., some Gamaredon/Primitive Bear Trojans) that used the Telegram API to transmit stolen data or commands had been described prior to 2022, although the trend became more widespread during the war. In 2021, the ToxicEye malware was discovered sending stolen information to Telegram chats hosted by attackers (at the time, this was a case of ransomware using Telegram for C2). The breakthrough, however, was a series of reports related to the war in Ukraine. Mandiant (Google)[5] published an analysis of hacktivists working with GRU-sponsored APT28 in September 2022 (supplemented with new findings in 2024), which revealed mechanisms of cooperation between official grassroots Telegram groups and state-sponsored APTs. Mandiant used security incident response data - including logs from victims' networks and the timing of material published on Telegram - to match the activities of APT28 and APT44 (Sandworm) groups, as well as posts from "XakNet Team" channels and others. The report posited that some of the pro-Russian groups on Telegram are fronts or intermediaries controlled by the service - while they may recruit genuine ideological hackers, the channels' leadership operates in concert with the GRU. These findings have been widely cited as evidence of the blurring lines between state operations and grassroots activity in cyberspace. Security and disinformation think tanks have also taken up the issue. The DFRLab (Atlantic Council)[6] published a comprehensive report in June 2024, ana BECID (a consortium studying

[5] Mandiant (Google), *Hacktivists collaborate with GRU-sponsored APT28 to target Ukraine*, Google Cloud Blog, 2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions (retrieved: 13.04.2025).

[6] E. Soula, B. Dubow, R. Osadchuk, *Another battlefield: Telegram as a digital front in Russia's war against Ukraine*, Atlantic Council – DFRLab, 25 June 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/another-battlefield-telegram-as-a-digital-front-in-russias-war-against-ukraine/ (retrieved: 14.04.2025).

disinformation in the Baltic region) in 2023[7]. This report focused on telegram propaganda in the Baltics. It used a case study approach - monitoring the most popular Russian-language channels targeting audiences in Latvia, Lithuania, and Estonia. BECID also found that Telegram's lack of moderation mechanisms - unlike Facebook or Twitter - made it a safe space for Kremlin narratives, even in the face of efforts by authorities in EU countries to curb disinformation.

Academic interest in Telegram's role in conflict and propaganda increased significantly after 2022. The journal Media, War & Conflict (2024) published an article by Miglė Bareikytė et al. entitled. "Digitally witnessed war from pereklychka to propaganda: The unfolding of Telegram communication during Russia's war in Ukraine"[8]. In it, the authors analyze how Telegram communication evolved from grassroots information (so-called pereklychka - spontaneous exchange of information among citizens) to organized state propaganda. This study shows that Telegram has enabled the parallel existence of eyewitness accounts and propaganda narratives, often in the same communication space. This phenomenon of digital "war witnessing" while manipulating the message is a new research challenge that combines media, conflict, and technology studies.

Another strand of academic research focuses on automatic detection of propaganda and disinformation. There have been papers proposing machine learning methods to detect pro-Russian propaganda in Telegram posts. One such study used a multilingual language model to analyze thousands of messages from propaganda channels in an attempt to detect distinctive linguistic and thematic features that distinguish propaganda from reliable information. While still in its early stages, this approach represents an attempt to technologically combat the flood of disinformation on this platform.

In Poland, the impact of Russian cyber operations and disinformation has also been analyzed, although more often in a broader perspective rather than focusing solely on Telegram. For example, the CERT Orange Poland 2023 report[9] noted attacks by Russian groups on Polish institutions (such as the incident of publishing data of the Polish Investment and Trade Agency on Telegram after the March 2023 attack) - and pointed out that Telegram is also used to distribute stolen victim data in the Polish context (creating a media effect). The Kosciuszko

[7] A. Tatarinova-Supe, *Kremlin's propaganda in our pockets: Telegram channels feed Baltic Russian-speakers with fake news*, Re:Baltica / BECID, May 2023, https://en.rebaltica.lv/2023/07/kremlins-propaganda-in-our-pockets-how-disinformation-thrives-on-telegram/ (retrieved: 15.04.2025).

[8] M. Bareikytė, M. Makhortykh, *Digitally witnessable war from pereklychka to propaganda: Unfolding Telegram communication during Russia's war in Ukraine*, Media, War & Conflict, vol. 0, no. 0, 2024, https://doi.org/10.1177/17506352241255890 (retrieved: 15.04.2025).

[9] CERT Orange Polska, *Raport CERT Orange Polska za rok 2023*, Orange Polska, 2024, https://cert.orange.pl/wp-content/uploads/2024/04/Raport_CERT_Orange_Polska_2023.pdf (retrieved: 15.04.2025).

Institute's Cyber Power (2020) report[10], on the other hand, describes a model of cooperation between Russian hacking groups (e.g., selling access to a hacked network to another group to carry out the next stage of the attack) - such a model fits well with the use of Telegram as a meeting place for offers and information exchange in the cybercriminal semi-community. While the CI report did not focus on a single medium, it does provide a broader picture of the ecosystem in which Telegram is one of the communication channels.

Research in recent years clearly shows that Telegram has become a strategic platform in the arsenal of Russian APT groups and related propaganda companies. From the point of view of cyber-attacks, Telegram facilitates rapid coordination, recruitment and dissemination of the results of attacks (increasing their reach and psychological impact). From the perspective of information warfare, Telegram is now for the Kremlin what state media used to be: the main narrative channel, only without any external control. The platform allows for the instantaneous dissemination of propaganda content on a massive scale, by passing censorship (or rather, exploiting the lack of moderation) in democratic countries. Initiatives such as improving algorithms for detecting disinformation, raising user awareness about the sources of information on Telegram, and international cooperation in prosecuting criminals using the platform are the answer.

It is already clear that revealing links between seemingly spontaneous channels and state actors (as in the Mandiant report) helps expose propaganda and undermines its credibility. Nevertheless, Telegram remains a difficult battleground - on the one hand, it provides researchers with valuable material (archives of public channels), and on the other hand, it is a tool efficiently used by Russian groups to adapt and escalate both cyberattacks and disinformation campaigns. In summary, the state of research in recent years confirms that Telegram is for Russian APT groups what secret servers and pirate radio stations once were - a command centre and propaganda megaphone in one. Understanding its role is therefore critical to gaining a full picture of today's cyber and information threats and developing effective defence strategies in the era of hybrid warfare.

AN OVERVIEW OF THE CYBERSECURITY THREATS

In recent months, the conflict between Russia and Ukraine has seen an intensification of cyber threats and disinformation campaigns. Ukrainian authorities have reported a 70% increase in cyber-attacks in 2024, attributed primarily to pro-Russian groups. These attacks have targeted critical sectors,

[10] I. Albrycht (ed.), E. Kasprzyk, A. Kozłowski, J. Collier, M. Krawczyk, T. Piekarz, K. Mikulski, *Three Seas United in Cyber Power*, Instytut Kościuszki, Kraków, 2020, https://3seaseurope.com/wp-content/uploads/2022/05/3S-united-in-cyber-power-ENG-online-strony.pdf (retrieved: 15.04.2025).

including government infrastructure and public services, causing significant disruptions[11].

A notable example was the cyber-attack on December 19, 2024, which paralyzed Ukrainian state registries, preventing, among other things, the registration of births and deaths[12]. This incident highlighted the vulnerability of Ukrainian digital infrastructure and the direct impact on the daily lives of citizens.

In parallel, Russia has stepped up its disinformation campaigns using advanced technologies such as generative artificial intelligence. These operations aim to spread false information on social media, making it harder for users to distinguish between real and fake news. According to Anton Demokhin, Deputy Foreign Minister of Ukraine, such campaigns have become more complex and pervasive, requiring international cooperation to effectively counter them[13].

In response to these threats, in June 2024 Poland and the United States launched the Ukraine Communications Group[14], a Warsaw-based initiative involving a dozen Western countries. The goal is to coordinate efforts to counter Russian disinformation and promote an accurate narrative about the invasion of Ukraine[15].

However, it is unclear how the situation, and the funding, will evolve given the recent stances of the Trump Administration. Defense Secretary Pete Hegseth has recently ordered a temporary halt to offensive cyber operations against Russia, a decision that has raised debate about the implications for national security and international alliances[16]. Recent weeks have seen a significant escalation of cyber threats and disinformation operations by Russia against Ukraine and its allies. This situation underscores the urgency of a coordinated and robust response by the international community to protect the integrity of digital infrastructure and ensure access to accurate information.

[11] L. Hierro, *La guerra cibernética entre Ucrania y Rusia se intensifica en paralelo al conflicto militar*, El País, 19 January 2025, https://elpais.com/internacional/2025-01-19/la-guerra-cibernetica-entre-ucrania-y-rusia-se-intensifica-en-paralelo-al-conflicto-militar.html (retrieved: 15.04.2025).

[12] Reuters, *Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says*, 20 December 2024, https://www.reuters.com/technology/cybersecurity/russia-conducted-mass-cyber-attack-ukraines-state-registries-deputy-pm-says-2024-12-19/ (retrieved: 11.04.2025).

[13] Reuters, *Russia using generative AI to ramp up disinformation, says Ukraine minister*, 16 October 2024, https://www.reuters.com/technology/artificial-intelligence/russia-using-generative-ai-ramp-up-disinformation-says-ukraine-minister-2024-10-16/ (retrieved: 11.04.2025).

[14] Ministry of Foreign Affairs Republic of Poland, *Ukraine Communications Group launched in Warsaw,* 10 June 2024, https://www.gov.pl/web/diplomacy/ukraine-comunications-group-launched-in-warsaw (retrieved: 12.04.2025).

[15] S. Bertolli, *Polonia e Stati Uniti lanciano un gruppo per combattere la disinformazione russa sulla guerra in Ucraina*, Euractiv, 11 June 2024, https://euractiv.it/section/digitale/news/polonia-e-stati-uniti-lanciano-un-gruppo-per-combattere-la-disinformazione-russa-sulla-guerra-in-ucraina/ (retrieved: 12.04.2025).

[16] C. Kube, N. Egwuonwu, *Defense Secretary Pete Hegseth orders a halt to offensive cyber operations against Russia*, NBC News, 3 March 2025, https://www.nbcnews.com/politics/trump-administration/defense-secretary-pete-hegseth-orders-halt-offensive-cyber-operations-rcna194435 (retrieved: 17.04.2025).

RUSSIAN APT GROUPS ACTIVITIES

Since October 2024, Russian-aligned APT (Advanced Persistent Threat) groups have intensified their cyber operations against Ukraine, adopting sophisticated strategies that combine cyber-attacks, disinformation campaigns, and psychological operations. However, in recent weeks, several APT groups have also intensified their activities with offensive tactics not only limited to the Ukrainian scenario but also targeting countries and political figures that have openly sided against Russia.

Gamaredon remains the most active APT group in Ukraine and its activity continues to rely on large-scale spear phishing[17] campaigns with attachments that use HTML smuggling[18]. Active since at least 2013, it has primarily targeted Ukrainian government institutions, non-governmental organizations, and other related entities. The group has improved its tools, including the PteroPSDoor backdoor[19] and the PteroSig data exfiltration tool[20].

PteroPSDoor is a backdoor developed and used by the Gamaredon group to maintain access to compromised networks[21]. A backdoor is software that allows an attacker to gain access to a compromised system without the victim's knowledge, bypassing normal security mechanisms. The PteroPSDoor backdoor is designed to operate stealthily and persistently within the attacked systems, allowing hackers to collect sensitive information and perform further malicious actions. The name

[17] Spear phishing is a targeted form of phishing where cybercriminals craft personalized messages to deceive specific individuals or organizations into revealing sensitive information or installing malware. Unlike traditional phishing, which casts a wide net, spear phishing focuses on a particular victim, using details gathered from social media, company websites, or previous breaches to make the attack more convincing.
Kaspersky, *What is spear phishing? Definition and risks*, https://www.kaspersky.com/resource-center/definitions/spear-phishing (retrieved: 15.04.2025).

[18] ESET Research, *ESET Research investigates the Gamaredon APT group: Cyberespionage aimed at high-profile targets in Ukraine and NATO countries*, 26 September 2024, https://www.eset.com/us/about/newsroom/research/eset-research-investigates-the-gamaredon-apt-group-cyberespionage-aimed-at-high-profile-targets-in-ukraine-and-nato-countries-1/ (retrieved: 15.04.2025).

[19] A backdoor in cybersecurity is a hidden method of bypassing normal authentication to gain unauthorized access to a system, network, or software. It can be intentionally created by developers for maintenance purposes or exploited by cybercriminals to control a system remotely. Backdoors are dangerous because they allow attackers to steal sensitive data, install malware or ransomware, and manipulate system functions without detection. Some common types of backdoors include rootkits, Trojan horses, and botnets, which can remain dormant until activated by an attacker.
B. Lutkevich, *Backdoor (computing)*, TechTarget, January 2023, https://www.techtarget.com/searchsecurity/definition/back-door (retrieved: 15.04.2025)

[20] ESET Research, *Cyberespionage the Gamaredon way: 26 September, 2024 – Analysis of toolset used to spy on Ukraine in 2022 and 2023*, 26 September 2024, https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf (retrieved: 16.04.2025).

[21] The Hacker News, *Hackers leveraging Cloudflare tunnels, DNS fast-flux to hide GammaDrop malware*, 6 December 2024, https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html (retrieved: 16.04.2025).

"PteroPSDoor" refers to a combination of remote control and data exfiltration capabilities, with the ability to receive commands from a remote server and perform malicious actions. This tool allows the group to easily control compromised devices, collect data, and send it to servers controlled by the group.

PteroSig is a data exfiltration tool that the group uses to extract information from compromised systems. Exfiltration is the process of stealing data from a system without the user's knowledge. PteroSig allows the group to extract large amounts of sensitive data from victims, including confidential documents, login credentials, and other valuable information, sending it to the command and control (C&C)[22] server operated by the Gamaredon group. The tool is designed to be highly effective and difficult to detect, using obfuscation[23] and encryption techniques to hide the exfiltrated data traffic. In some cases, PteroSig uses encrypted communication channels to prevent security solutions from identifying and blocking the flow of stolen data.

Sandworm is the other major APT linked to the Ukrainian conflict, associated with the Russian GRU unit 74455, which since October 2024 has targeted around twenty Ukrainian organizations, including entities providing energy, water and heating services, using the WrongSens backdoor for Windows and the Linux malware LOADGRIP and BIASBOAT[24]. The latter is notable for its complexity and the use of machine-specific IDs to decrypt the payload. In addition, in July 2024, Sandworm launched a disinformation campaign, creating fake websites imitating

[22] Command and Control (C&C), also known as C2, refers to the communication channel that attackers use to control compromised systems or networks. It is a critical component of many cyberattacks, enabling threat actors to send instructions to infected devices and receive stolen data.
Attackers infiltrate a system using methods like phishing, malware, or exploiting vulnerabilities. Then, to establishing a connection, is created a backdoor, allowing the compromised system to communicate with the attacker's C&C server. The attacker uses the C&C server to issue commands, such as stealing data, spreading malware, or creating botnets. Sensitive information is extracted and sent to the attacker via the C&C channel.
There are different types of c&c techniques, Like Botnets, DNS Tunneling or Encrypted Channels; B. Lenaerts-Bergmans, *Command and Control (C&C) attacks explained*, CrowdStrike, 19 July 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/command-and-control-cac-attack/ (retrieved: 16.04.2025).

[23] Obfuscation refers to the practice of deliberately making code, data, or communication difficult to understand or analyze. It is often used to protect sensitive information or intellectual property, but it can also be exploited by malicious actors to hide malware or evade detection by security systems; N. Balaji, *Understanding malware obfuscation: A guide for cybersecurity professionals*, Cyber Security News, 30 August 2024, https://cybersecuritynews.com/malware-obfuscation/ (retrieved: 16.04.2025).

[24] D. Antoniuk, *Sandworm-linked hackers target users of Ukraine's military app in new spying campaign*, The Record, 19 December 2024, https://therecord.media/ukraine-military-app-espionage-russia-sandworm (retrieved: 17.04.2025).

the Ukrainian military app "Army+", to steal information from devices used by Ukrainian soldiers[25].

As last, we must mention the **SideWinder** APT group, known for its persistent cyber espionage activities since 2012, has recently broadened its geographic scope, extending its operations beyond South Asia into the Middle East and Africa. This shift signals a strategic evolution, likely aimed at targeting new geopolitical interests and high-value entities in these regions. The group's latest campaigns have exhibited a high degree of sophistication, making use of advanced espionage tools to compromise their targets[26]. One of the most notable developments in SideWinder's arsenal is the deployment of "StealerBot", an advanced modular toolkit discovered by Kaspersky in October. This tool is designed for comprehensive cyber-espionage, performing a wide range of malicious functions. It enables attackers to install additional malware on compromised systems, capture screenshots, log keystrokes, and extract sensitive information, including stored passwords from web browsers. Moreover, StealerBot is capable of intercepting credentials used in Remote Desktop Protocol (RDP) sessions, a technique that allows cybercriminals to gain unauthorized access to critical systems. The tool also facilitates file exfiltration, ensuring that valuable data is covertly transferred to the attackers' infrastructure[27].

The recent campaigns attributed to SideWinder have targeted high-profile organizations and strategic infrastructure, raising concerns about the group's broader ambitions. The specific nature of these targets suggests an interest in intelligence gathering, potentially in support of geopolitical objectives. Given the advanced capabilities of StealerBot and the widening scope of SideWinder's operations, it is plausible that their cyber espionage activities will continue to expand, posing a growing threat to governments, businesses, and critical infrastructure in the regions they now operate in. This ongoing expansion highlights the importance of strengthened cybersecurity measures and continuous monitoring to counteract the evolving tactics of this formidable threat actor.

NONAME057(16): DDOS ATTACKS AGAINST ITALIAN ENTITIES

The pro-Russian collective **NoName057(16)**, active since March 2022, has launched a series of Distributed Denial-of-Service (DDoS) attacks against Italian

[25] V. Telychko, *UAC-0125 attack detection: Hackers use fake websites on Cloudflare Workers to exploit the "Army+" application*, SOC Prime, 18 December 2024, https://socprime.com/blog/uac-0125-attacks-against-ukraine-detection/ (retrieved: 16.04.2025).

[26] Kaspersky, *Kaspersky identifies SideWinder APT expanding attacks with new espionage tool*, 15 October 2024, https://www.kaspersky.com/about/press-releases/kaspersky-identifies-sidewinder-apt-expanding-attacks-with-new-espionage-tool (retrieved: 16.04.2025).

[27] AdnKronos, *Kaspersky rileva l'APT SideWinder, che intensifica gli attacchi con un nuovo strumento di spionaggio*, 16 October 2024, https://www.adnkronos.com/immediapress/kaspersky-rileva-lapt-sidewinder-che-intensifica-gli-attacchi-con-un-nuovo-strumento-di-spionaggio_505Y1vHuvByxvEhaXkLXag (retrieved: 16.04.2025).

institutions. NoName057(16) emerged in March 2022, aligning itself with the Russian Federation. The group has claimed responsibility for cyberattacks on countries including Ukraine, the United States, and several European nations, typically targeting government agencies, media outlets, and private company websites. On February 17, 2025, the group targeted the websites of Linate and Malpensa airports, the Transport Authority, Intesa San Paolo bank, and the ports of Taranto and Trieste. These attacks were a response to statements by Italian President Sergio Mattarella, who had compared Russia's actions in Ukraine to the Third Reich. Despite the attacks, the Italian National Agency for Cybersecurity (ACN) intervened promptly, limiting the impact on the affected infrastructures[28].

More recently, NoName057(16) has resumed its hostile activities against various Italian targets through DDoS attacks. This resurgence has affected entities such as the Ministry of Infrastructure and Transport, the Eastern Adriatic Port Authority, and Linate Airport. In response to these attacks, Telegram has been actively moderating NoName057(16)'s content, forcing the group to frequently change channels to continue their operations[29].

In November 2024, the group launched a wave of DDoS attacks against several local councils in the UK. These attacks began after the UK government renewed its support for Ukraine, a move that sparked a backlash from the group. The websites of local councils, including those of Bradford, Salford and Eastleigh, were targeted, causing disruption to access services for citizens[30].

The DDoS attacks, while not particularly sophisticated, have managed to temporarily block websites, disrupting online services that in some cases are crucial to citizens' daily functions. The UK's National Cyber Security Centre (NCSC) has been quick to step in to offer technical support to local councils, helping them mitigate the effects of the attacks and protect digital infrastructure.

THE ROLE OF TELEGRAM

Russian APT groups have used Telegram as a strategic platform to coordinate and promote their operations against Ukraine. Groups like NoName057(16) have exploited Telegram to organize Distributed Denial of Service (DDoS) attacks against Ukrainian government websites and infrastructure. Through dedicated channels, they have claimed attacks, mocked victims, issued threats, and shared educational

[28] P. Paganini, *Pro-Russia collective NoName057(16) launched a new wave of DDoS attacks on Italian sites*, Security Affairs, 17 February 2025, https://securityaffairs.com/174294/hacktivism/noname05716-launched-ddos-attacks-on-italian-sites.html (retrieved: 16.04.2025).

[29] Red Hot Cyber, *NoName057(16) è tornato! Nuova ondata di DDoS sulle infrastrutture italiane*, 23 March 2025, https://www.redhotcyber.com/post/noname05716-e-tornato-nuova-ondata-di-ddos-alle-infrastrutture-italiane/ (retrieved: 17.04.2025).

[30] C. Jones, *UK councils bat away DDoS barrage from pro-Russia keyboard warriors*, The Register, 1 November 2024, https://www.theregister.com/2024/11/01/uk_councils_russia_ddos/ (retrieved: 17.04.2025).

content to educate others on the techniques used. But Telegram has been used to disseminate pro-Russian propaganda and disinformation campaigns too. For example, the Gamaredon group opened a Telegram channel focused on spreading Russian propaganda in the Odessa region, trying to influence local public opinion[31].

Journalistic investigations have revealed that individuals have been recruited on Telegram to carry out acts of sabotage for Russia in Europe. Offers of up to 10,000 euros have been made for actions such as setting fire to armoured vehicles or assassinating opponents of Russia. These offers were posted on Telegram channels affiliated with groups such as the Wagner paramilitary group[32]. In the end, some APT groups have used Telegram not only for information dissemination, but also for control of their cyber operations. For example, in the second quarter of 2022, several Russian-affiliated groups used Telegram to access command and control (C&C) servers or as a tool for leaking information[33]. Telegram has been exploited by Russian APT groups as a multifunctional platform to coordinate attacks, spread propaganda, recruit collaborators, and manage cyber operations against Ukraine and other targets.

SOCIAL ENGINEERING THREATS

However, Russian cyber operations are not limited to the work of brilliant hackers; often, it is enough to exploit the adversary's vulnerabilities to gain access to sensitive information or to disrupt essential services. Social engineering is one of the most insidious and underestimated threats in the cybersecurity landscape. It's not just about technicalities or viruses: often, what allows an attack to succeed is human error, such as simply clicking on a seemingly harmless email attachment.

The Computer Emergency Response Team of Ukraine (CERT-UA) recently identified a series of targeted cyber-attacks against Ukrainian institutions, attributed to the threat group called UAC-0226. These attacks were aimed primarily at military formations, law enforcement agencies, and local self-government bodies, especially in the regions close to Ukraine's eastern border[34].

[31]SecurityOpenLab, *APT: dall'Europa all'Oriente l'evoluzione avanza*, 14 November 2024, https://www.securityopenlab.it/news/4250/apt-dalleuropa-alloriente-levoluzione-avanza.html (retrieved: 14.04.2025).

[32] Le Monde, *Sur Telegram, des utilisateurs recrutés pour des actes de sabotage prorusses en Europe*, 26 September 2024, https://www.lemonde.fr/pixels/article/2024/09/26/sur-telegram-des-utilisateurs-recrutes-pour-des-actes-de-sabotage-prorusses-en-europe_6334667_4408996.html (retrieved: 13.04.2025).

[33] Data Manager Online, *ESET pubblica il primo APT Activity Report che illustra le attività dei gruppi affiliati a Russia, Corea del Nord, Iran e Cina*, 15 December 2024, https://www.datamanager.it/2022/12/eset-pubblica-il-primo-apt-activity-report-che-illustra-le-attivita-dei-gruppi-affiliati-a-russia-corea-del-nord-iran-e-cina/ (retrieved: 17.04.2025).

[34] R. Lakshmanan, *UAC-0226 deploys GIFTEDCROOK stealer via malicious Excel files targeting Ukraine*, The Hacker News, 8 April 2025, https://thehackernews.com/2025/04/uac-0226-deploys-giftedcrook-stealer.html (retrieved: 13.04.2025).

Attackers used phishing emails containing Excel attachments with malicious macros. The file names and subjects of the emails referenced sensitive and current topics, such as demining, administrative fines, drone production, and compensation for destroyed property, to increase the likelihood that victims would open the attachments. To lend more credibility to the phishing emails, attackers sent the messages from compromised accounts, often using the web interface of email clients. This ploy aimed to fool victims into believing that the communications were coming from trusted sources.

Once the victim opened the Excel file and enabled macros, two malicious components were automatically executed. The first was a PowerShell code taken from the GitHub repository "PSSW100AVB" that established a reverse shell connection, allowing attackers to gain remote control of the infected system. The second was a new malware written in C/C++, "GIFTTEDCROOK Malware", designed to steal sensitive data from popular web browsers, such as Google Chrome, Microsoft Edge, and Mozilla Firefox. The stolen information included cookies, browsing history, and authentication data. Although CERT-UA attributed these activities to the UAC-0226 group, no clear indication of the country of origin of this group was provided.

CONCLUSION

Telegram has become a cornerstone of Russia's cyberwarfare strategy, serving as a command center for cyberattacks, a recruitment platform for saboteurs, and a tool for widespread propaganda. The increasing sophistication of these operations underscores the urgent need for Ukraine and its allies to strengthen their cybersecurity defences and develop countermeasures to mitigate the misuse of the platform. As cyberattacks and disinformation campaigns escalate, governments must adopt proactive strategies to counter threats emanating from Telegram and ensure that digital resilience remains a top priority in the face of evolving cyberwarfare tactics. Telegram's technical features - strong encryption, lack of content moderation, ease of setting up channels, ability to communicate in real time - make the platform an ideal environment for coordinating offensive actions. Groups such as Gamaredon and Sandworm use Telegram to plan and execute cyberattacks on Ukrainian public institutions, as well as to share malware tools (e.g. PteroPSDoor, PteroSig, LOADGRIP). Other groups, such as NoName057(16), use Telegram to organize DDoS attacks against the infrastructure of countries supporting Ukraine, including Italy and the United Kingdom. The platform is also used to publish instructions, glorious accounts of attacks carried out, and even financial offers for those willing to carry out acts of sabotage against Russia.

The activities of Russian APT groups in and outside of Ukraine since October 2024 have demonstrated a multi-pronged strategy that combines sophisticated cyberattacks, disinformation operations, and physical attacks on critical infrastructure. These operations underscore the need for Ukraine and its allies to strengthen cybersecurity measures and develop effective strategies to counter disinformation. The issue of local government resilience to cyber threats and the need to invest more in protecting their networks and systems is critical, as we have seen in the UK case. At a time when cyber threats are becoming more sophisticated and frequent, support and preparedness to deal with these attacks has become essential to ensure the continuity of public services. Finally, it is important to reiterate the importance of investing in training and prevention. You cannot rely on protection technologies and software alone, because no system is completely invulnerable to human error. Training serves to bridge this gap, transforming employees from potential unwitting targets into a true active barrier against threats.

It is essential that everyone in an organization understands how malicious actors operate, the most common social engineering techniques, and how to recognize the signs of a potential attack. This kind of preparation must be concrete, up-to-date and implemented in the daily reality of the work context. This is the only way to develop a true culture of security that involves everyone, not just insiders. Ultimately, training is the first and most effective line of defence. In a landscape where cyber-attacks are becoming increasingly sophisticated, the only true human antivirus is awareness. And awareness is built through education, training, and experience.

Therefore, one of the most important conclusions of the analysis is the need for systematic training, both for employees of public institutions and ordinary citizens, in recognizing digital threats. Only by building a culture of cybersecurity - based on knowledge, vigilance and awareness - will it be possible to effectively counter the growing threats posed by platforms such as Telegram.

Bibliography

Adigwe, C.S., Mayeke, N.R., Olabanji, S.O., Okunleye, O.J., Joeaneke, P.C., Olaniyi, O.O., *The evolution of terrorism in the digital age: Investigating the adaptation of terrorist groups to cyber technologies for recruitment, propaganda, and cyberattacks*, Asian Journal of Economics, Business and Accounting, vol. 24, no. 3, 2024, pp. 289–306, https://doi.org/10.9734/ajeba/2024/v24i31287

AdnKronos, *Kaspersky rileva l'APT SideWinder, che intensifica gli attacchi con un nuovo strumento di spionaggio*, 16 October 2024, https://www.adnkronos.com/immediapress/kaspersky-rileva-lapt-sidewinder-che-intensifica-gli-attacchi-con-un-nuovo-strumento-di-spionaggio_505Y1vHuvByxvEhaXkLXag

AdnKronos, *Kaspersky rileva l'APT SideWinder, che intensifica gli attacchi con un nuovo strumento di spionaggio*, 16 October 2024, https://www.adnkronos.com/immediapress/kaspersky-rileva-lapt-sidewinder-che-intensifica-gli-attacchi-con-un-nuovo-strumento-di-spionaggio_505Y1vHuvByxvEhaXkLXag

Albrecht, M., Mareková, L., Paterson, K.G., Stepanovs, I., *Four attacks and a proof for Telegram*, IEEE Symposium on Security and Privacy, San Francisco, 2022, pp. 87–106, https://doi.org/10.1109/SP46214.2022.9833666

Albrycht, I. (ed.), Kasprzyk, E., Kozłowski, A., Collier, J., Krawczyk, M., Piekarz, T., Mikulski, K., *Three Seas United in Cyber Power*, Instytut Kościuszki, Kraków, 2020, https://3seaseurope.com/wp-content/uploads/2022/05/3S-united-in-cyber-power-ENG-online-strony.pdf

Antoniuk, D., *Sandworm-linked hackers target users of Ukraine's military app in new spying campaign*, The Record, 19 December 2024, https://therecord.media/ukraine-military-app-espionage-russia-sandworm

Antoniuk, D., *Sandworm-linked hackers target users of Ukraine's military app in new spying campaign*, The Record, 19 December 2024, https://therecord.media/ukraine-military-app-espionage-russia-sandworm

Balaji, N., *Understanding malware obfuscation: A guide for cybersecurity professionals*, Cyber Security News, 30 August 2024, https://cybersecuritynews.com/malware-obfuscation/

Balaji, N., *Understanding malware obfuscation: A guide for cybersecurity professionals*, Cyber Security News, 30 August 2024, https://cybersecuritynews.com/malware-obfuscation/

Ball, D., Montasari, R., *The evolution of terrorism in digital era: Cyberterrorism, social media, and modern extremism*, in: Montasari, R., Jahankhani, H., Masys, A.J. (eds), *Navigating the Intersection of Artificial Intelligence, Security, and Ethical Governance*, Advanced Sciences and Technologies for Security Applications, Springer, Cham, 2025, https://doi.org/10.1007/978-3-031-72821-1_9

Bareikytė, M., Makhortykh, M., *Digitally witnessable war from pereklychka to propaganda: Unfolding Telegram communication during Russia's war in Ukraine*, Media, War & Conflict, vol. 0, no. 0, 2024, https://doi.org/10.1177/17506352241255890

Bertolli, S., *Polonia e Stati Uniti lanciano un gruppo per combattere la disinformazione russa sulla guerra in Ucraina*, Euractiv, 11 June 2024, https://euractiv.it/section/digitale/news/polonia-e-stati-uniti-lanciano-un-gruppo-per-combattere-la-disinformazione-russa-sulla-guerra-in-ucraina/

CERT Orange Polska, *Raport CERT Orange Polska za rok 2023*, Orange Polska, 2024, https://cert.orange.pl/wp-content/uploads/2024/04/Raport_CERT_Orange_Polska_2023.pdf

Data Manager Online, *ESET pubblica il primo APT Activity Report che illustra le attività dei gruppi affiliati a Russia, Corea del Nord, Iran e Cina*, 15 December 2024, https://www.datamanager.it/2022/12/eset-pubblica-il-primo-apt-activity-report-che-illustra-le-attivita-dei-gruppi-affiliati-a-russia-corea-del-nord-iran-e-cina/

ESET Research, *Cyberespionage the Gamaredon way: 26 September, 2024 – Analysis of toolset used to spy on Ukraine in 2022 and 2023*, 26 September 2024, https://web-assets.esetstatic.com/wls/en/papers/white-papers/cyberespionage-gamaredon-way.pdf

ESET Research, *ESET Research investigates the Gamaredon APT group: Cyberespionage aimed at high-profile targets in Ukraine and NATO countries*, 26 September 2024, https://www.eset.com/us/about/newsroom/research/eset-research-investigates-the-gamaredon-apt-group-cyberespionage-aimed-at-high-profile-targets-in-ukraine-and-nato-countries-1/

Hierro, L., *La guerra cibernética entre Ucrania y Rusia se intensifica en paralelo al conflicto militar*, El País, 19 January 2025, https://elpais.com/internacional/2025-01-19/la-guerra-cibernetica-entre-ucrania-y-rusia-se-intensifica-en-paralelo-al-conflicto-militar.html

Jones, C., *UK councils bat away DDoS barrage from pro-Russia keyboard warriors,* The Register, 1 November 2024, https://www.theregister.com/2024/11/01/uk_councils_russia_ddos/

Kaczmarek K., Karpiuk M., Soler U., *The Potential Use of Artificial Intelligence in Crisis Management*, “Sicurezza, Terrorismo e Società” 2024, No. 2.

Karpiuk M., Melchior C, Soler U., *Cybersecurity Management in the Public Service Sector*, “Prawo i Więź” 2023, No. 4(47), https://doi.org/10.36128/PRIW.VI47.751.

Kaspersky, *Kaspersky identifies SideWinder APT expanding attacks with new espionage tool*, 15 October 2024, https://www.kaspersky.com/about/press-releases/kaspersky-identifies-sidewinder-apt-expanding-attacks-with-new-espionage-tool

Kaspersky, *What is spear phishing? Definition and risks*, https://www.kaspersky.com/resource-center/definitions/spear-phishing

Kube, C., Egwuonwu, N., *Defense Secretary Pete Hegseth orders a halt to offensive cyber operations against Russia*, NBC News, 3 March 2025, https://www.nbcnews.com/politics/trump-administration/defense-secretary-pete-hegseth-orders-halt-offensive-cyber-operations-rcna194435

Lakshmanan, R., *UAC-0226 deploys GIFTEDCROOK stealer via malicious Excel files targeting Ukraine*, The Hacker News, 8 April 2025, https://thehackernews.com/2025/04/uac-0226-deploys-giftedcrook-stealer.html

Le Monde, *Sur Telegram, des utilisateurs recrutés pour des actes de sabotage prorusses en Europe*, 26 September 2024, https://www.lemonde.fr/pixels/article/2024/09/26/sur-telegram-des-utilisateurs-recrutes-pour-des-actes-de-sabotage-prorusses-en-europe_6334667_4408996.html

Lenaerts-Bergmans, B., *Command and Control (C&C) attacks explained*, CrowdStrike, 19 July 2023, https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/command-and-control-cac-attack/

Lutkevich, B., *Backdoor (computing)*, TechTarget, January 2023, https://www.techtarget.com/searchsecurity/definition/back-door

Mandiant (Google), *Hacktivists collaborate with GRU-sponsored APT28 to target Ukraine*, Google Cloud Blog, 2022, https://cloud.google.com/blog/topics/threat-intelligence/gru-rise-telegram-minions

Paganini, P., *Pro-Russia collective NoName057(16) launched a new wave of DDoS attacks on Italian sites*, Security Affairs, 17 February 2025, https://securityaffairs.com/174294/hacktivism/noname05716-launched-ddos-attacks-on-italian-sites.html

Ptaszek, G., Yuskiv, B., Khomych, S., *War on frames: Text mining of conflict in Russian and Ukrainian news agency coverage on Telegram during the Russian invasion of Ukraine in 2022*, Media, War & Conflict, vol. 17, no. 1, 2023, pp. 41–61, https://doi.org/10.1177/17506352231166327

Red Hot Cyber, *NoName057(16) è tornato! Nuova ondata di DDoS sulle infrastrutture italiane*, 23 March 2025, https://www.redhotcyber.com/post/noname05716-e-tornato-nuova-ondata-di-ddos-alle-infrastrutture-italiane/

Reuters, *Russia conducted mass cyberattack on Ukraine's state registries, deputy PM says*, 20 December 2024, https://www.reuters.com/technology/cybersecurity/russia-conducted-mass-cyber-attack-ukraines-state-registries-deputy-pm-says-2024-12-19/

Reuters, *Russia using generative AI to ramp up disinformation, says Ukraine minister*, 16 October 2024, https://www.reuters.com/technology/artificial-intelligence/russia-using-generative-ai-ramp-up-disinformation-says-ukraine-minister-2024-10-16/

SecurityOpenLab, *APT: dall'Europa all'Oriente l'evoluzione avanza*, 14 November 2024, https://www.securityopenlab.it/news/4250/apt-dalleuropa-alloriente-levoluzione-avanza.html

Soula, E., Dubow, B., Osadchuk, R., *Another battlefield: Telegram as a digital front in Russia's war against Ukraine*, Atlantic Council – DFRLab, 25 June 2024, https://www.atlanticcouncil.org/in-depth-research-reports/report/another-battlefield-telegram-as-a-digital-front-in-russias-war-against-ukraine/

Tatarinova-Supe, A., *Kremlin's propaganda in our pockets: Telegram channels feed Baltic Russian-speakers with fake news*, Re:Baltica / BECID, May 2023, https://en.rebaltica.lv/2023/07/kremlins-propaganda-in-our-pockets-how-disinformation-thrives-on-telegram/

Telychko, V., *UAC-0125 attack detection: Hackers use fake websites on Cloudflare Workers to exploit the "Army+" application*, SOC Prime, 18 December 2024, https://socprime.com/blog/uac-0125-attacks-against-ukraine-detection/

The Hacker News, *Hackers leveraging Cloudflare tunnels, DNS fast-flux to hide GammaDrop malware*, 6 December 2024, https://thehackernews.com/2024/12/hackers-leveraging-cloudflare-tunnels.html

ROLA TELEGRAMU W KOORDYNOWANIU CYBERATAKÓW I KAMPANII PROPAGANDOWYCH ROSYJSKICH HAKERÓW

Abstrakcyjny

Celem artykułu była analiza roli platformy Telegram w cybernetycznych i dezinformacyjnych działaniach rosyjskich grup hakerskich (APT) podczas wojny na Ukrainie. Autorzy skupili się na zbadaniu, w jaki sposób Telegram wspierał organizację ataków, propagandę, rekrutację sabotażystów i zarządzanie operacjami w czasie rzeczywistym. W tym kontekście omówiono również reakcje społeczności międzynarodowej (w tym Polski, USA i Wielkiej Brytanii) oraz kluczowe wyzwania cyberbezpieczeństwa. Telegram ewoluował z aplikacji przeznaczonej do bezpiecznej komunikacji w wielofunkcyjne narzędzie wykorzystywane przez prorosyjskie grupy APT. Jego cechy - silne szyfrowanie, brak moderacji treści i łatwość tworzenia kanałów - pozwalają im koordynować cyberataki, rozprzestrzeniać dezinformację i rekrutować współpracowników. Grupy takie jak Gamaredon i Sandworm wykorzystują Telegram do atakowania publicznej infrastruktury Ukrainy, podczas gdy NoName057(16) organizuje ataki DDoS na instytucje krajów wspierających Ukrainę. Wnioski z analizy pokazują, że Telegram stał się nie tylko narzędziem komunikacji, ale nawet centrum operacyjnym operacji hybrydowych. Autorzy podkreślają pilną potrzebę opracowania strategii obronnych – zarówno technologicznych, jak i społecznych. Podnoszenie świadomości użytkowników i systematyczne szkolenia w zakresie wykrywania zagrożeń są niezwykle ważne. To jedyny sposób na zbudowanie odpornej kultury cyberbezpieczeństwa, zdolnej do skutecznego reagowania na wyzwania stawiane przez Telegram jako broń w nowoczesnej wojnie informacyjnej.

Słowa kluczowe: Telegram, cyberzagrożenia, cyberbezpieczeństwo, wojna na Ukrainie