THE INFLUENCE OF NON-STATE CYBER ACTORS IN CONVENTIONAL ARMED CONFLICTS: A CASE STUDY OF THE WAR IN UKRAINE

Aleksandar Bogićević
Strategic Research Institute, University of Defence in Belgrade, Belgrade, Republic of Serbia
Email: aleksandar.bogicevic@mod.gov.rs

Abstract

Although cyber operations have been conducted for more than a quarter of a century, their limited application in previous conflicts and the absence of confrontations between states with advanced cyber capabilities have left numerous questions concerning their effectiveness in the context of conventional warfare. In this regard, the war in Ukraine represents a critical juncture in the evolution of cyber warfare, both in terms of the scale and destructiveness of cyberattacks and the level of sophistication involved. Throughout the conflict, there has been a marked increase in the participation of non-state cyber actors, including hacktivist collectives, private companies, and volunteer groups. These actors predominantly operate in collaboration with state structures and are motivated by either material incentives or ideological alignment. This paper investigates the ways in which non-state actors contribute to cyber operations within the framework of conventional armed conflicts, focusing on the war in Ukraine as a case study. It specifically examines their selected targets, the nature and extent of damage inflicted, and the degree of institutional cooperation between state and non-state entities. The research is grounded in the hypothesis that while the role of non-state actors in the cyber domain is expanding, their involvement, although tactically significant, does not currently constitute a decisive factor in determining the overall conduct of military operations. The objective is to identify the key factors influencing the effectiveness of such engagements and to assess the role of cyber capabilities in contemporary warfare.

Keywords: non-state cyber actors, war in Ukraine, cybersecurity, cyber warfare, conventional armed conflict

Introduction

The emergence of cyber warfare has fundamentally transformed the nature of modern conflicts, introducing a new dimension in which existing ways of thinking are not fully applicable. Cyber warfare defined, as the unauthorized intrusion into foreign computer systems for the purposes of data manipulation, infrastructure damage, and the execution of other malicious operations (Novaković & Rizmal, 2017, p. 252) has evolved from a theoretical concept into practical implementation that shapes contemporary geopolitical dynamics. The digital space has become a theatre of confrontation, where states engage in espionage, manipulation, and intellectual property theft to gain an advantage over

adversaries without provoking escalations. In an effort to conceal their participation in such activities, states employ organized cyber groups which, acting as cyber proxies, are tasked with carrying out illegal activities.

The employment of cyber actors provides states with the opportunity to choose how they will respond to allegations of attacks. (Brown & Fazal, 2021, p. 402) The convergence of economic and patriotic motives (Canfil, 2022, p. 2) of the cyber underground, on the one hand, and state sponsorship and the need to fulfill strategic objectives, on the other, has resulted in new types of non-state actors in the digital space, which now pose significant threats to states. The war in Ukraine has inaugurated a new chapter in armed conflicts, challenging all pre-war assumptions regarding the nature of warfare in digital space. Shortly after the war's onset, cyber warfare in digital space witnessed the involvement of other actors, including various cybersecurity companies, as well as criminal groups whose knowledge became highly valuable to states engaged in the conflict. This integration of cyber and conventional warfare has demonstrated that cyber remains a novel domain, one in which states continue to explore new possibilities, particularly in the offensive domain.

The research explores the role and extent to which non-state actors participate in cyber operations within conventional armed conflicts, specifically investigating the degree of cooperation between state and non-state entities, their strategic objectives, and the outcomes of their actions. The study examines the nature of their cooperation with state structures and the broader implications for international security. The research concludes that while the role of non-state actors in the cyber domain is expanding, particularly regarding actions within the "gray zone" of conflict, their participation in large-scale conventional conflict does not currently provide a decisive advantage in the overall conduct of military operations in the digital space. This study employs a qualitative case study methodology, focusing on the war in Ukraine as the conflict marked by extensive cyber operations involving both state and non-state actors. The research is based on the analysis of secondary sources, including official reports from cybersecurity agencies, and investigative journalism. Given the covert nature of cyber activities and the challenges in attribution, the study acknowledges limitations regarding the reliability and verification of sources.

Cyber Proxies and the Architecture of State-Sponsored Operations

The contemporary cyber environment is characterized by an intricate nexus of relationships between state and non-state actors, wherein traditional boundaries between official and unofficial cyber operations become increasingly ambiguous. Such obfuscation complicates the terminological conceptualization of state-supported cyber groups, as evidenced by divergent scholarly definitions. Borghard and Lonergan conceptualize these entities as actors who execute offensive actions within the digital sphere to achieve political objectives on behalf of a patron state (2016, p. 2). Conversely, Maurer adopts a more expansive definitional framework, encompassing all intermediaries who knowingly facilitate, whether actively or passively, the implementation of offensive actions against adversarial targets (2018, p. 17).

Actors operating in cyberspace may choose to pursue one of three types of attacks during offensive operations. Targets may encompass vital objectives whose incapacitation could permanently destabilize a state; however, such operations demand extensive resources and capabilities possessed only by specialized state units in cyber warfare. A lower level of capability is required for activities such as digital espionage operations, intellectual property theft, and isolated attacks on critical

infrastructure elements. The lowest tier of complexity encompasses DDoS attacks and defacement attacks on institutional websites, whose effects are, individually, devoid of strategic significance for states. (Pijpers, 2023, p. 7) The achievement of strategically consequential effects through cyber resources via a singular, comprehensive attack, is dismissed as a viable possibility (Gartzke, 2013, p. 54); considerably greater apprehension is generated by the proliferation of smaller-scale incidents that may incrementally attrite state resources, a phenomenon characterized as "slow-bleed tactic" (Harknett & Smeets, 2020, p. 545).

The engagement of diverse organizations in conducting illicit activities on behalf of state interests entails considerable risks for the sponsoring state, particularly regarding reputational losses. The existence of such risks raises a question: why states enter into such arrangements, or alternatively, what strategic advantages might be derived from the utilization of non-state actors. Firstly, cyber proxy actors conduct operations within the gray zones of the international system, thereby providing protective cover for governments that may seek to disavow involvement in offensive cyber operations that become publicly exposed (Akoto, 2021, p. 313), thus furnishing plausible deniability. Secondly, the instrumentalization of hacking collectives can prove exceptionally valuable as a coercive mechanism during international crises and disputes, enabling states to exert pressure on adversaries without escalating tensions through direct or overt state involvement.

States may establish various modalities of cooperation with non-state actors. Maurer elucidates the relationship between non-state actors and states through three governance strategies: direct delegation of tasks, principled guidance, and tacit support (Maurer, 2018, p. 42). In contrast, Healey provides a more detailed categorization of this relationship by identifying ten distinct mechanisms through which states may collaborate with cyber criminal, ranging from full operational control to complete disavowal (Healey, 2011). Determining the relationship between non-state actors and their sponsors, as well as the degree of cooperation achieved between them, proves exceedingly difficult to ascertain due to the limited availability of information, whose reliability remains perpetually questionable (Akoto, 2021, p. 322).

An additional challenge in perpetrator identification is posed by the possibility of malicious software exchange between state agencies and hacking groups. Such operational paradigms involve the sale or licensing of ransomware to technologically less sophisticated groups through various dark web forums, thereby further complicating the process of identifying the perpetrators of cyberattacks (Martin & Whelan, 2023, p. 6). The conflict in Ukraine has further accelerated the dissemination of cyberattack expertise, as evidenced by the distribution of the notorious Pegasus spyware on Russian forums (CyberPeace Institute, 2023, p. 16), and the training of interested parties in the execution of cyberattacks, exemplified by the IT Army of Ukraine, thereby rendering the internet increasingly militarized and hazardous for all stakeholders.

The Digital Front in the War in Ukraine: Actors, Strategies, and Normative Challenges

Accompanying the initial waves of aviation and cruise missile strikes, Russian hacking groups, both state and non-state actors, launched attacks targeting Ukrainian digital infrastructure, thus initiating the first conventional conflict in cyberspace. The objectives of these groups included degrading the functionality of institutional and corporate computer networks, data theft, the disclosure of sensitive information, and the dissemination of specific narratives. Although the initial impression

suggests that Russia's cyber offensive at the war's onset yielded no tangible results (Beecroft, Bateman, & Wilde, 2022) or, even worse, hurt its war efforts by triggering a rally-around-the-flag effect on the Ukrainian side (Wilde, 2024), it is essential to consider the objectives and initial positions from which both sides commenced the conflict.

Russia conceptualizes the digital domain as an integral component of the broader information sphere, through which it seeks to alter the balance of power between adversaries. The *Information Security Doctrine*, adopted in 2016, identifies the information space as a strategic dimension of national security, with a particular emphasis on the protection of moral and social values from perceived external threats (Russian Federation, Security Council, 2016). Central to Russia's approach has been the deliberate contestation of narratives and the destabilization of the political and social fabric of its opponents (Wilde, 2024, p. 1). These efforts, which began in Ukraine, have since expanded to target Western allies, aiming to provoke internal discord and erode public support for Ukraine (ENISA, 2024, p. 10). The information sphere serves as a space through which Russia aims to weaken its adversaries from within by exploiting societal divisions. The intensification of the contest in the informational space of Western countries was notably pronounced in 2024 due to the conduct of several important elections whose results could substantially impact support for Ukraine (Microsoft, 2023). Elections have proven particularly susceptible to manipulation due to the potential for influencing dominant themes (agenda setting), campaigns targeting the reputations of politicians, and undermining public trust in the legitimacy of the entire process (ENISA, 2024, p. 95).

Beyond conducting attacks of lower complexity, such as DDoS attacks and manipulation in the information space, non-state cyber actors on both sides have achieved success in operations that are traditionally within the purview of intelligence agency hacking groups. For instance, when pro-Russian hacking organization "KillNet" breached the networks of Ukraine's Ministry of Foreign Affairs and Ministry of Economy (State Service of Special Communications and Information Protection of Ukraine, 2023, p. 30). Over time, pro-Russian cyber actors have diverted their focus, increasingly targeting the digital infrastructure of countries providing support for Ukraine. (Microsoft Threat Intelligence, 2022) This trend is reflected in the significant rise in cyberattacks conducted by the pro-Russian hacking groups against European Union member states, rising from 10% in the first quarter of 2022 to as much as 50% in 2023 (Thales Cyber Threat Intelligence Team, 2023). On the other hand, Ukraine, having successfully defended its own digital space, undertook its own cyber offensive, employing identical means to those used by Russia: highly sophisticated operations conducted by intelligence agencies, and lower-complexity raids carried out by cyber proxies. However, unlike Moscow, which distances itself from its ties with hacking collectives, Kyiv has decided to provide support to cybercriminals conducting attacks by rewarding them with medals. (BBC News, 2024) Such instances of rewarding civilians for committing criminal acts and attacks in cyberspace against enemy targets indicate a complete erosion of the boundaries between third parties and active participants in armed conflict, as well as between civilians and military personnel.

Although mutual attacks by pro-Russian and pro-Ukrainian groups have not resulted in changes on the battlefield, their actions may serve as an indicator of their future roles and emerging trends. With the growing number of states possessing offensive cyber capabilities (Stoddart, 2022, p. 7), examples of collaboration between state structures and non-state actors during the war in Ukraine, as well as the willingness of civilians to participate in attacks through digital means, point to a concerning

trend of cyberspace militarization. Further escalation of the current state of cyber warfare could potentially be triggered by the emergence of "rogue" groups that cease to operate in accordance with their sponsor-state's interests, or by a change in the previously restrained strategy of Western governments, which, according to available data (Stoddart, 2022, p. 35), still refrain from responding symmetrically to attacks.

Conclusion

The case of the war in Ukraine reveals a qualitative transformation in the nature of contemporary armed conflicts, as it represents the first instance of the systematic and large-scale employment of cyber capabilities by both sides in a conventional war. This study demonstrates that non-state actors, including hackers, criminal networks, and hacktivist groups, have become integral components of digital operations, either through cooperation with state institutions or as independent actors motivated by political or financial interests. Simultaneously, institutional support and public recognition ofthese actors' activities demonstrate an increasingly profound erosion of traditional distinctions between civilians and combatants, as well as between the state and its proxies in cyberspace.

Despite the growing importance and presence of non-state actors, the findings of this research indicate that their role, while strategically valuable within the so-called "gray zone" of conflict, has not yet constituted a decisive factor in determining the outcome of conventional military operations. Their primary value lies in their capacity to disrupt the functioning of institutions and economic entities, shape public perceptions, and exert pressure without provoking open escalation. However, such practices raise numerous questions regarding international law, accountability, and future regulation of cyber warfare.

Ultimately, the militarization of cyberspace and the increasing involvement of civilians in conducting cyber operations underscore the urgent need for the development of clearer normative frameworks and attribution mechanisms. Should the international community fail to address the challenges posed by such a transformation, the world may confront an even more perilous form of conflict, one in which boundaries between war and peace, as well as between combatants and civilians, become increasingly blurred. This trend threatens to increase global insecurity significantly and destabilize the already delicate and fragile balance of international relations.

References

1. Akoto, W. (2021). Accountability and cyber conflict: Examining institutional constraints on the use of cyber proxies. *Conflict Management and Peace Science, 39*(3), 311–332.
2. Bateman, J., Beecroft, N., & Wilde, G. (2022). What the Russian invasion reveals about the future of cyber warfare. Carnegie Endowment for International Peace.
3. BBC News. (2024, April 10). Ukraine rewards vigilante hackers for help against the Russian attack. *BBC News*. https://www.bbc.com/news/technology-68722542
4. Borghard, E. D., & Lonergan, S. W. (2016). Can states calculate the risks of using cyber proxies? *Orbis, 60*(3), 395–416.
5. Brown, J. M., & Fazal, T. M. (2021). #SorryNotSorry: Why states neither confirm nor deny responsibility for cyber operations. *European Journal of International Security, 6*(4), 401–417.
6. Canfil, J. K. (2022). The illogic of plausible deniability: Why proxy conflict in cyberspace may no longer pay. *Journal of Cybersecurity, 8*(1).
7. CyberPeace Institute. (2023). *Cyber dimensions of the armed conflict in Ukraine: Quarterly analysis report Q3 July to September 2023*. Geneva: CyberPeace Institute.

8. European Union Agency for Cybersecurity (ENISA). (2024, September 19). *ENISA threat landscape 2024* (ENISA Report). European Union Agency for Cybersecurity.
9. Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to Earth. *International Security, 38*(2), 41–73.
10. Harknett, R. J., & Smeets, M. (2020). Cyber campaigns and strategic outcomes. *Journal of Strategic Studies, 45*(3), 534–567.
11. Healey, J. (2011). The spectrum of national responsibility for cyberattacks. *Brown Journal of World Affairs, 18*(1), 57–70.
12. Martin, J., & Whelan, C. (2023). Ransomware through the lens of state crime: Conceptualizing ransomware groups as cyber proxies, pirates, and privateers. *State Crime Journal, 12*(1), 4–28.
13. Maurer, T. (2018). *Cyber mercenaries: The state, hackers, and power*. Cambridge University Press.
14. Microsoft Threat Intelligence. (2022, October 14). New "Prestige" ransomware impacts organizations in Ukraine and Poland. *Microsoft Security Blog*.
15. Microsoft. (2023). *A year of Russian hybrid warfare in Ukraine* (Microsoft Threat Intelligence Report).
16. Novaković, I., & Rizmal, I. (2017). Cyber warfare: New type of warfare or additional element of conventional warfare. In *ISIKS 2017: Asymmetry and Strategy*. Belgrade.
17. Pijpers, P. B. M. J. (2023). Revisiting the stability/instability paradox in cyberspace: Lessons from the Russo-Ukraine war (No. 146). The Hague Centre for Strategic Studies.
18. Russian Federation, Security Council. (2016). *Doctrine of information security of the Russian Federation* (Decree No. 646).
19. State Service of Special Communications and Information Protection of Ukraine. (2023). *Russia's cyber tactics: Lessons learned in 2022*.
20. Stoddart, K. (2022). Cyberwar: Attacking critical infrastructure. In *Cyberwarfare: Threats to Critical Infrastructure* (pp. 147–225). Palgrave Macmillan.
21. Thales Cyber Threat Intelligence Team. (2023). A year of cyber conflict in Ukraine: Summary of extensive analysis (2022–2023). Thales Group.
22. Wilde, G. (2024). *Russia's countervalue cyber approach: Utility or futility?* Carnegie Endowment for International Peace.