SEVEN publicações acadêmicas

CHAPTER 001

GUERRA CIBERNÉTICA E CONFLITOS FÍSICOS: EVIDÊNCIAS DO CONFLITO RUSSO-UCRANIANO (2022–2024)

CYBER WARFARE AND PHYSICAL CONFLICTS: EVIDENCE FROM THE RUSSIAN-UKRAINIAN CONFLICT (2022-2024)

CIBERGUERRA Y CONFLICTO FÍSICO: DATOS DEL CONFLICTO RUSO-UCRANIANO (2022-2024)

https://doi.org/10.56238/sevened2025.026-001

João Marcos Barbosa Oliveira[1], Carlos Henrique do Nascimento Barros[2], Ismael Deus Marques[3], Jovair Pazzini de Melo Souza[4], Eduardo Stefani[5]

RESUMO

Este artigo investiga o emprego da Guerra Cibernética (G Ciber) durante o conflito entre Rússia e Ucrânia (2022–2024), enfatizando sua interação com operações militares convencionais. Com base em dados do *European Repository of Cyber Incidents* (EuRepoC), analisou-se a correlação entre a intensidade dos ataques cibernéticos e dos combates físicos, a ocorrência de efeitos físicos decorrentes de ações cibernéticas e a temporalidade dos incidentes em relação às fases do conflito. Os resultados demonstram que algumas operações cibernéticas foram coordenadas com ações militares tradicionais, contribuindo para impactos significativos no teatro de operações. Por fim, os achados são discutidos à luz da doutrina de Guerra Cibernética do Exército Brasileiro, identificando potenciais caminhos para sua atualização.

Palavras-chave: Guerra Cibernética. Conflito Rússia-Ucrânia. Doutrina Militar. Infraestrutura Crítica. Operações Cibernéticas.

ABSTRACT

This article investigates the use of cyber warfare during the conflict between Russia and Ukraine (2022-2024), emphasizing its interaction with conventional military operations.

[1] Master's Degree in Military Sciences (EsAO)
Rio de Janeiro, Rio de Janeiro - Brazil
Email: barbosaoliveira.joao@eb.mil.br
[2] Doctor in Military Sciences (ECEME)
Rio de Janeiro, Rio de Janeiro - Brazil
Email: carloshnbarros@gmail.com
[3] Master in Public Policy and Government (FGV)
Brasilia, DF - Brazil
Email: ismaeldmarques@gmail.com
[4] Master's Degree in Military Sciences (EsAO)
Rio de Janeiro, Rio de Janeiro - Brazil
Email: pazzini.jovair@eb.mil.br
[5] Doctorate student in Informatics and Knowledge Management (UNINOVE)
São Paulo, São Paulo - Brazil
E-mail: eduardo_stefani@uni9.edu.br

Based on data from the European Repository of Cyber Incidents (EuRepoC), the correlation between the intensity of cyber attacks and physical combat, the occurrence of physical effects resulting from cyber actions and the temporality of incidents in relation to the phases of the conflict were analyzed. The results show that some cyber operations were coordinated with traditional military actions, contributing to significant impacts in the theater of operations. Finally, the findings are discussed in the light of the Brazilian Army's Cyber Warfare doctrine, identifying potential ways of updating it.

Keywords: Cyber warfare. Russia-Ukraine conflict. Military Doctrine. Critical Infrastructure. Cyber operations.

RESUMEN

Este artículo investiga el uso de la ciberguerra durante el conflicto entre Rusia y Ucrania (2022-2024), haciendo hincapié en su interacción con las operaciones militares convencionales. A partir de datos del Repositorio Europeo de Ciberincidentes (EuRepoC), se analizó la correlación entre la intensidad de los ciberataques y el combate físico, la aparición de efectos físicos derivados de las acciones cibernéticas y la temporalidad de los incidentes en relación con las fases del conflicto. Los resultados muestran que algunas operaciones cibernéticas se coordinaron con acciones militares tradicionales, contribuyendo a producir impactos significativos en el teatro de operaciones. Finalmente, se discuten los resultados a la luz de la doctrina de Ciberguerra del Ejército Brasileño, identificando posibles formas de actualizarla.

Palabras clave: Guerra cibernética. Conflicto Rusia-Ucrania. Doctrina militar. Infraestructuras críticas. Operaciones cibernéticas.

INTRODUCTION

The incorporation of Information and Communication Technologies (ICT) into the operational environment has expanded the spectrum of action of Military Land Operations, enabling the integration of cyberspace as a combat domain. In the context of the Russian-Ukrainian conflict (2022–2024), the use of offensive cyber capabilities was observed by actors of different natures, acting in military or non-military technology assets, evidencing the coordinated employment of capabilities in multiple domains, as provided for in doctrinal principles of maneuver commonly observed in armed forces around the world

In Brazilian military doctrine (BRASIL, 2017, p. 18), Cyber Warfare (G Ciber) "[..] corresponds to the offensive and defensive use of information and information systems to deny C2 [Command and Control] capabilities to the adversary, exploit, corrupt, degrade or destroy them [...]". It constitutes a form of asymmetric conflict with the potential to integrate into the tactical, operational, or strategic actions of the Land Forces, enhancing their effects or anticipating kinetic actions through the denial, deterrence, or paralysis of critical enemy functions (BRASIL, 2023a).

In this context, the present study aims to analyze, based on empirical data from the EuRepoC (*European Repository of Cyber Incidents*) database, how G Ciber articulates with the traditional physical conflict in the Ukrainian theater of operations. To this end, the analysis was structured in three main axes: (1) the correlation between cybernetic intensity and physical intensity of the conflict; (2) the occurrence of physical effects as a result of cyberattacks; and (3) the temporal distribution of cyberattacks in relation to the escalations of the armed conflict.

Authors such as Rid (2012) and Valeriano, Jensen and Maness (2018) have debated the strategic effectiveness of cyber operations in interstate wars. Despite the divergences regarding their isolated strategic effectiveness, there is agreement that such operations contribute to the disruption of logistics flows, degradation of critical infrastructure and saturation of C2 systems. In the case of Ukraine, episodes such as the attack on Kyivstar's infrastructure in December 2023 illustrate the possibility of concrete physical impacts from the cyber domain.

In view of this, this article proposes to contribute to the specialized literature of military doctrine and cybersecurity studies by combining an empirical approach, based on systematized data on cyber incidents, taking as a theoretical reference the Brazilian terrestrial military doctrine and international studies on G Ciber.

THEORETICAL FRAMEWORK

G Ciber is commonly observed as an essential capability in the scope of the Military Ground Operations doctrine, integrating the joint, coordinated, and simultaneous effort of the various means of combat on the contemporary battlefield through the so-called Cyber Operations (Cyber Operation) (BRASIL, 2023a). For the military doctrine of the Brazilian Army (BRASIL, 2017, p. 18), G Ciber "comprises actions that involve ICT tools to destabilize or take advantage of the opponent's information systems and defend the Sist Info itself".

In Brazil's Military Cyber Defense Doctrine (BRASIL, 2023a), Cyber Operations can be classified into three types: cyber attack (Atk Ciber), cyber exploitation (Exp Ciber), and cyber protection (Ptç Ciber). Cyber Atk, in particular, aims to degrade, destroy, or manipulate adversary systems and information, and can be employed autonomously or as an integral part of broader military campaigns. In armed conflicts, these operations can be synchronized with kinetic actions to enhance their effects, being carried out in support of interdiction actions, denial of area or paralysis of command (BRASIL, 2017).

Within the scope of Cyber Ofs, the concept of interdiction stands out, which consists of the execution of actions aimed at denying the enemy's freedom of action, through the degradation or neutralization of its critical infrastructures, information flows, and command and control capabilities (BRASIL, 2017). These actions can precede or accompany conventional offensives, and are planned to compromise the adversary's ability to respond and articulate. Cyber interdiction represents, therefore, a way to enhance the effects of military campaigns by breaking the enemy's operational cohesion.

Exp Ciber, in turn, comprises actions that aim to obtain sensitive information from adversarial computer systems, without necessarily causing noticeable or immediate degradation of these assets. These actions seek to compromise the confidentiality of information, conducted with a veiled and prolonged character, to support other military operations through intelligence collection (BRASIL, 2017). The distinction between Cyber Exp and Cyber Atk lies, in essence, in the affected information security pillar: while the exploitation compromises confidentiality, the attack impacts the availability and/or integrity of the systems.

Ptç Ciber, on the other hand, corresponds to the set of measures and capabilities aimed at the active and passive defense of the Armed Forces' systems and networks, guaranteeing freedom of action in cyberspace, ensuring the continuous operation of their critical capabilities, and promoting the cyber resilience of mission infrastructures. Ptç Ciber ranges from asset monitoring and intrusion detection to threat containment and system

recovery, being essential to preserve the integrity, availability, and confidentiality of operational information. According to the Brazilian doctrine, the effectiveness of Ptç Ciber depends on the integration between technological resources, qualified personnel and well-defined processes, aligned with the information security management cycle (BRASIL, 2017).

The Brazilian doctrine also emphasizes the importance of synergy between the physical and cyber domains, especially in large-scale operations. The ability to integrate cyber actions with land, air, or informational maneuvers broadens the combat spectrum and contributes to the achievement of decision-making superiority (BRASIL, 2017). This alignment is part of the concept of convergence operations, in which cyber and conventional actions act in a coordinated manner to maximize military effects (BRASIL, 2023b). In this context, the protection of national critical infrastructure assumes a strategic role, being considered one of the main objectives of Ptç Ciber actions. The continuity of essential services and the preservation of the technological assets of the Armed Forces are indispensable conditions to guarantee freedom of action in cyberspace, a central element of operability in the twenty-first century.

At the international level, authors such as Thomas Rid (2012) argue that Cyber Op, unlike other dimensions of conventional warfare, rarely produce immediate death or physical destruction, being characterized mostly as actions of limited effects, aimed at disorganization, sabotage or espionage. However, more recent studies indicate that, when integrated into military campaigns, such operations can take on strategic characteristics, as evidenced in attacks on critical infrastructure, command and control, and communication networks of opponents (VALERIANO; JENSEN; MANESS, 2018). Corroborating this perspective, Marini, Pederneiras and Moita (2024) highlight that the rapid technological evolution and the protagonism of cyberspace have made the use of G Ciber as an instrument to achieve military and political objectives increasingly recurrent, including promoting significant impacts on critical state infrastructures. The Stuxnet case, analyzed by the authors, shows that Cyber Op can be characterized as acts of war when used with the purpose of compelling the opponent's will and achieving strategic purposes.

The literature also emphasizes G Ciber's role in hybrid conflicts, in which irregular actions, disinformation, political influence, and cyber operations are employed in a coordinated manner. According to Kello (2013), G Ciber challenges the traditional boundaries between peace and war, creating a continuous state of ambiguous hostility, typical of the so-called gray zone conflicts, in which Atk Ciber or Exp Ciber precede, accompany or replace physical confrontations.

From a doctrinal point of view, G Ciber can also support the concept of Military Maneuver, by acting on the vectors of time, space and information, contributing to the rupture of enemy cohesion and to the decision-making superiority of friendly forces (BRASIL, 2017). This capability becomes particularly relevant in offensive, defensive, and stabilization operations, as observed in several modern campaigns, including in the context of the conflict between Russia and Ukraine. With this, the question studied in this article arises: how does the cyberwarfare observed in contexts where there is a military maneuver corroborate what is described by the Brazilian military doctrine, that is, the coordination of physical and cybernetic actions?

METHODOLOGY

This study adopts a qualitative and quantitative approach, based on the analysis of empirical data from the EuRepoC – *European Repository of Cyber Incidents database*, focusing on the period from January 2022 to December 2024, corresponding to two years of the Russian-Ukrainian conflict. The objective of the methodology is to identify patterns and correlations between the use of G Ciber and observations in the military maneuver.

Methodologically, cyberattacks were classified based on the country affected by the cyberattack. This choice is justified due to the difficulty of identifying the origin of Atk and Exp Ciber, that is, state and non-state groups can camouflage the origin of their actions, but the target country is more easily identified.

The research is structured in three analytical axes:

- Analysis of the correlation between cybernetic intensity and physical conflict intensity;
- Identification of cyberattacks with direct or indirect physical effects;
- Observation of the chronology of cyberattacks in relation to moments of escalation or retraction of the armed conflict.

The database used contains 198 unique records, categorizing cyber incidents by attributes such as date of occurrence, target country (*receiver_main_country*), type of operation (*attack_type*), cyber intensity (*weighted_cyber_intensity*), existence of physical impacts (*physical_impact*), and association with military events (*offline_conflict_intensity*). The analyses were performed using the R language, with the support of *the tidyverse*, *lubridate* and *ggplot2* packages for data manipulation, cleaning and visualization.

For the analysis of the first axis, the records were segmented by target country and classified according to the intensity of the associated physical conflict ("*Yes*", "*Unknown*" or

"*Not available*"), allowing the construction of *comparative boxplots*. In the second axis, the events that presented the variable *physical_impact* marked as true were filtered. The third axis consisted of aggregating incidents over time and visually comparing them with indicators of escalation of the physical conflict, observing possible temporal correlations. The term Offensive Cyber Operation (Cyber Ofs Operation) was adopted to cover both Cyber Atk and Cyber Exp actions, considering that originally the EuRepoC base does not make this distinction.

In addition to the quantitative approach, the article also incorporates an illustrative case study, centered on the cyberattack against the infrastructure of the Kyivstar operator, which took place in December 2023. This incident was selected because it has high cyber intensity and relevant physical impacts, in addition to wide repercussion in the media and specialized sources, being cross-referenced with external information from open and academic sources.

The methodological choice for the EuRepoC database is due to its emphasis on attributed and documented attacks, with academic curation, which makes it suitable for studies of correlation between cyber actions and geopolitical phenomena. However, the dependence on open data and the possible underreporting of incidents are recognized as a limitation, especially in environments with less informational transparency.

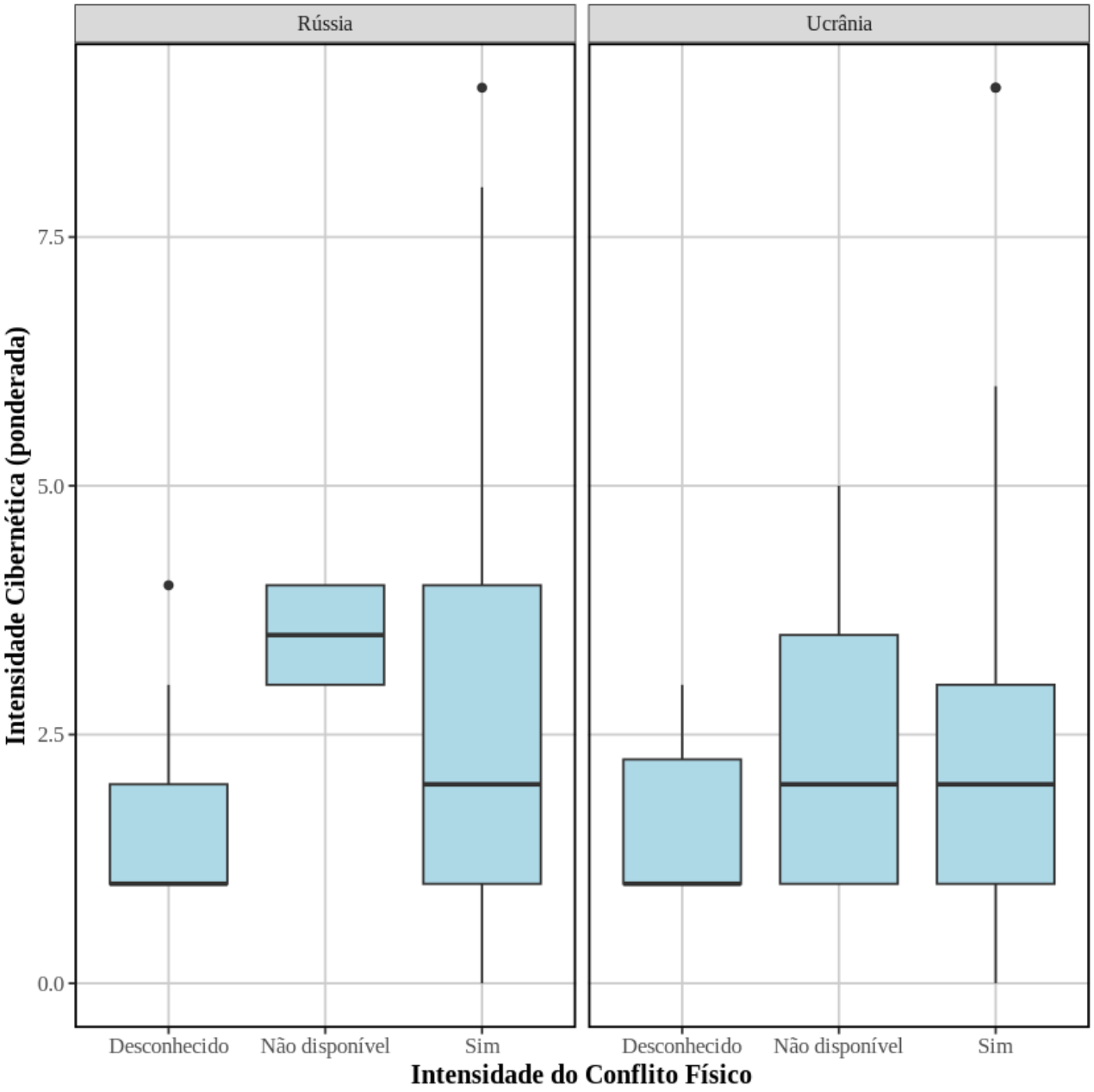
RESULTS

This section presents the results obtained from the analysis of cyber incidents that occurred between 2022 and 2024, with an emphasis on the relationship between G Ciber and the traditional physical conflict in the context of the Russian-Ukrainian war. The data analyzed, extracted from the EuRepoC database, were organized and visualized in graphs that allow us to understand the possible correlations between cyber intensity, physical effects, and moments of escalation of the armed conflict. The discussion of the results is structured around the three investigative topics outlined in the methodology, with special attention to the points that dialogue directly with the concepts and guidelines contained in the Manual of Military Doctrine for Cyber Defense (BRASIL, 2017).

CORRELATION BETWEEN THE INTENSITY OF PHYSICAL CONFLICT AND CYBERNETIC INTENSITY

Figure 1 presents a boxplot comparing the weighted cyber intensity (*weighted_cyber_intensity*) with the physical conflict intensity variable (*offline_conflict_intensity*), segmented by the target country (Ukraine and Russia).

Figure 1 – Cyber Intensity vs Physical Conflict by Target Country (2022–2024)



Source: The authors, with data from EuRepoC (2024)

The analysis of the graph reveals that, in the case of Russia as a target country, there is a greater concentration of Cyber Ofs Op with a high degree of complexity and sophistication, even in records classified as of "low or unknown intensity" of the physical conflict. This finding suggests that, in the Russian case, there is greater flexibility in the use of Cyber Ofs, even outside the scope of kinetic actions, expanding the possibilities provided for in the Brazilian doctrine regarding synchronization between domains. In contrast,

incidents targeting Ukraine have a more even distribution across different levels of physical intensity, with a slight trend of increased cyber intensity in events associated with more intense fighting.

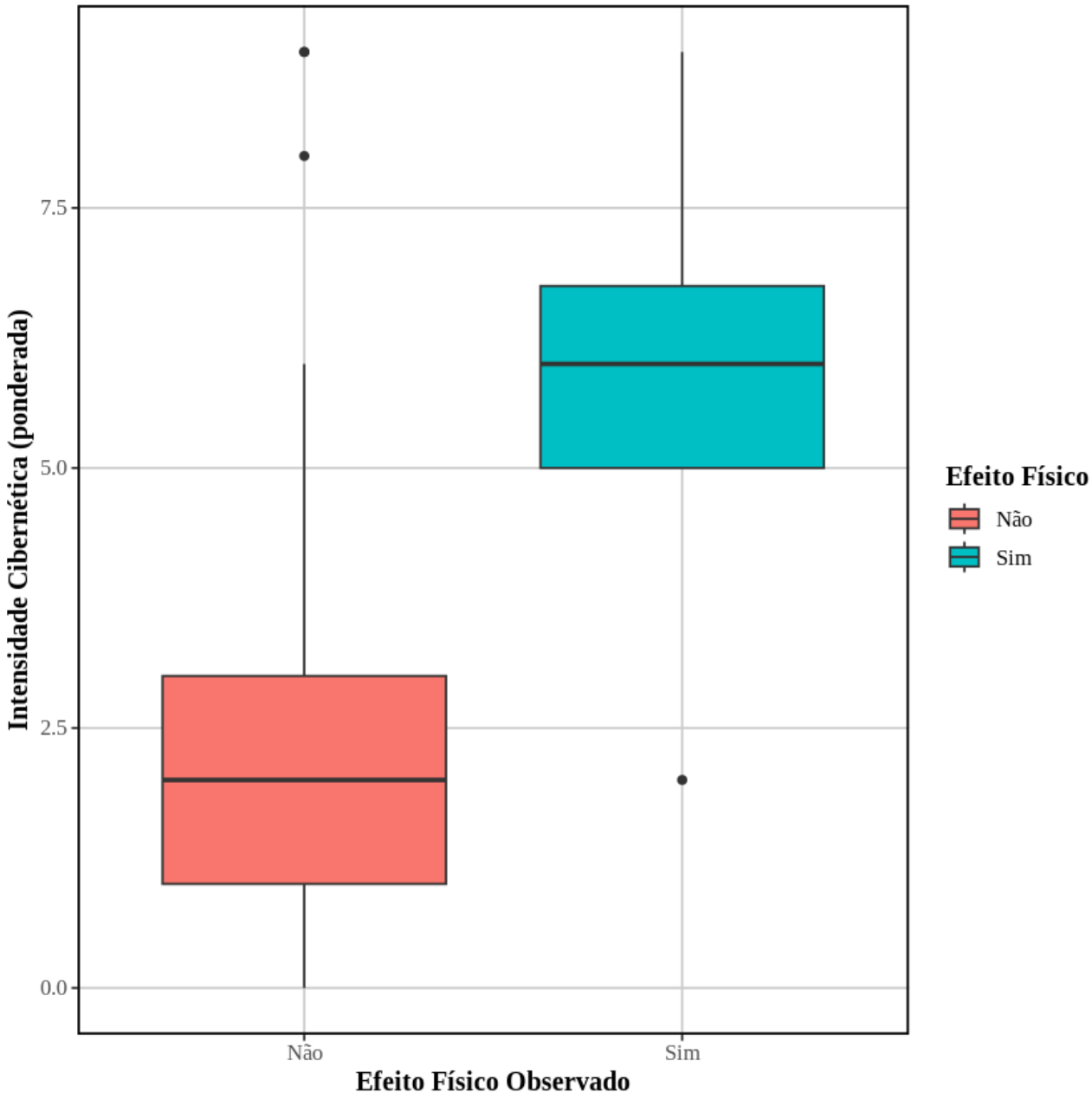
This result offers a relevant counterpoint to the Brazilian doctrine, which postulates that Cyber Ofs tend to be synchronized with kinetic actions, as a way to enhance the effects of operations (BRASIL, 2017). In the Russian case, a significant number of high-intensity Cyber Ofs Op is observed even in contexts without direct association with physical escalations, suggesting that, in this specific context, G Ciber can operate relatively independently of conventional actions, serving, for example, sabotage, strategic pressure or deterrence purposes.

In the case of Ukraine, the greater coherence between the intensities suggests a closer integration between the physical and cyber domains, in line with what the Brazilian doctrine defines as the coordinated use of capabilities to obtain decision-making superiority and break enemy cohesion (BRASIL, 2017).

CYBERNETIC INTENSITY DUE TO THE OCCURRENCE OF PHYSICAL EFFECTS

Figure 2 shows the distribution of weighted cyber intensity (*weighted_cyber_intensity*) according to the occurrence or absence of observable physical effects as a result of the attacks. The analysis shows a clear distinction: the few Cyber Ofs that generated physical effects ("Yes") have significantly higher medians, with a predominance of scores between 6 and 8 on the weighted intensity index. On the other hand, the Cyber Ofs that did not generate such effects ("No") are concentrated between 1 and 4 points, with dispersion and presence of *low-intensity* outliers.

Figure 2 – Cybernetic Intensity by Occurrence of Physical Effects



Source: The authors, with data from EuRepoC (2024)

This pattern reinforces the Brazilian doctrine by indicating that the greater the intensity of the Cyber Ofs Operation, in this case, Cyber Atk, the greater the potential for generating concrete physical effects, such as disruption of services, degradation of critical infrastructures or compromise of command and control systems (BRASIL, 2017). Although the sample of attacks with physical effects is small, the deviation between groups is clear and visually consistent.

From a doctrinal point of view, this result corroborates the premise that G Ciber, when applied with sufficient scale, sophistication and persistence time, is capable of

generating physical effects comparable to those of conventional warfare, especially on civilian targets and critical infrastructures. Also according to the Military Doctrine of Cyber Defense manual (BRASIL, 2023a), such Cyber Atks tend to be used in support of offensive campaigns, interdiction, or command paralysis, which reinforces the tactical relevance of G Ciber.

4.3 TIMELINE OF CYBERATTACKS AND MOMENTS OF ESCALATION

Figure 3 shows the timeline of cyberattacks classified by intensity and target country, with coloring indicating the intensity of the physical conflict according to the HIIK system (when available). The points are relatively evenly distributed between Ukraine and Russia, but with important qualitative differences.

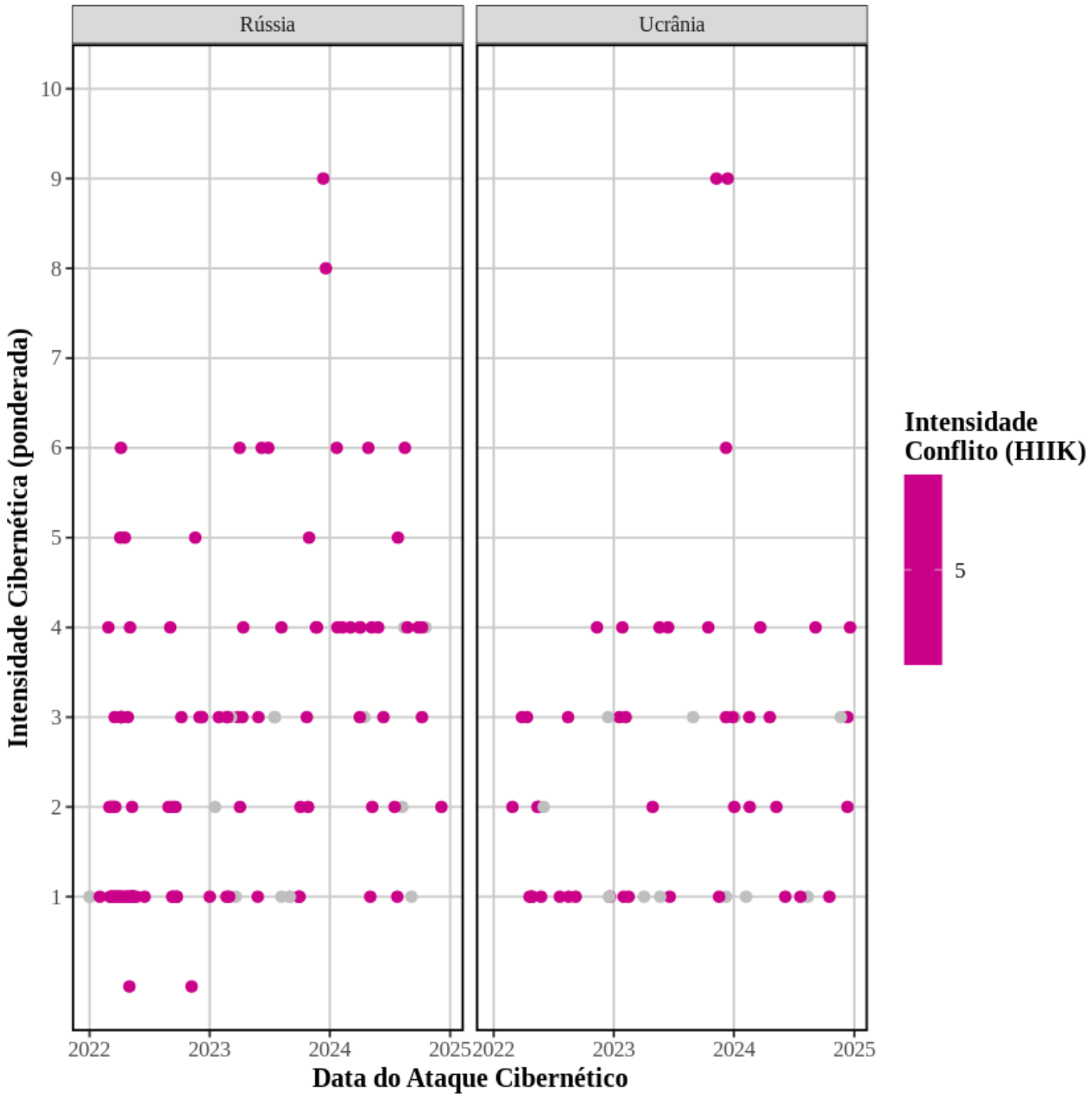
The acronym HIIK refers to the *Heidelberg Institute for International Conflict Research*, a research center linked to the University of Heidelberg, in Germany. This institute is responsible for producing the *Conflict Barometer*, an annual report that documents and classifies political conflicts around the world based on criteria of intensity, actors involved, and dynamics of the confrontation.

The HIIK system uses an ordinal scale from 1 to 5 to classify the intensity of conflicts, being:

- Level 1: Latent Dispute
- Level 2: Manifest Conflict
- Level 3: Crisis
- Level 4: Severe Conflict
- Level 5: War

This classification takes into account variables such as the use of force, number of victims, structural damage, and duration of confrontation. In the context of this article, the *offline_conflict_intensity_subcode* variable of the EuRepoC database associates each cyber incident, when possible, with a HIIK intensity level, allowing to cross events in cyberspace with moments of escalation in conventional physical conflict.

Figure 3 – Timeline: Cyber Intensity and Escalation of Physical Conflict (by Target Country)



Source: The authors, with data from EuRepoC (2024).

For Russia as a target country, there is a higher density of attacks over time, with moderate and high intensities (above 4) distributed relatively constantly. This suggests the existence of a prolonged cyber campaign, possibly associated with attrition, disinformation, and sabotage operations in different periods of the conflict.

In the case of Ukraine, on the other hand, the highest-intensity attacks are more concentrated at critical moments — such as the end of 2023 — and visually align with the presence of the highest number of records of intense physical conflict (HIIK 5). In particular, on 29 December 2023, Russia carried out the largest airstrike since the start of the war,

employing 158 missiles and drones against cities such as Kyiv, Kharkiv, Dnipro, and Lviv, resulting in at least 31 deaths and severe damage to civilian infrastructure (NPR, 2023). In addition, on the night of December 20-21, multiple *Shahed drone* strikes were also launched from different fronts, intensifying fighting in regions such as Dnipropetrovsk, Sumy, and Poltava (BASMAT, 2023). This synchronism reinforces the hypothesis that, in this theater, G Ciber was used as a vector of direct support to conventional military operations, as recommended by the Brazilian doctrine (BRASIL, 2017), acting as a multiplier of effects in offensive campaigns.

Visually, this integration between domains in the Ukrainian case highlights the use of G Ciber as a means of disorganization and denial of capabilities, especially in times of escalation. In the Russian case, its function seems more dispersed and continuous, which suggests doctrinal and operational differences between the belligerents regarding the use of G Ciber as a tactical or strategic vector. These findings illustrate, in practice, the application of the concept of convergence operations, provided for in Brazilian military doctrine (BRASIL, 2023b).

CASE STUDY: ATTACK ON KYIVSTAR (2023)

Among the incidents recorded in the EuRepoC base with maximum cyber intensity (9/10), the attack carried out against Kyivstar, Ukraine's largest telecommunications operator, which took place in December 2023, stands out. The event, attributed to the *Sandworm group*, linked to the Russian military intelligence service (GRU), was classified with confirmed physical effects and associated with a moment of high-intensity physical conflict (HIIK 5), being an emblematic example of the synergy between cyber operations and conventional actions in the Ukrainian theater.

According to Ukraine's own cyber intelligence chief, the attackers remained infiltrated in Kyivstar's network for several months before launching the destructive attack (BALMFORTH, 2024). This pattern highlights the direct relationship between the stages of Cyber Exp — characterized by stealth access, information collection, and vulnerability mapping — and the subsequent execution of Cyber Atk, responsible for the substantial degradation of critical infrastructure. The integration between Exp Ciber and Atk Ciber in the Kyivstar case demonstrates that successful offensive operations, especially those with relevant physical and social impacts, depend on prolonged reconnaissance and preparation carried out in a veiled manner. The episode also highlights how the absence of early detection of exploratory activities can enhance the damage caused in the destructive phase of the attack.

The offensive resulted in the disabling of mobile services and internet for millions of civilians, directly impacting air warning systems in cities such as Kyiv and Sumy, considered essential for anti-aircraft defense during Russian bombardments. In addition, technical reports indicate the destruction of more than 10 thousand servers and 4 thousand workstations, characterizing substantial degradation of the national critical infrastructure, with impacts on the continuity of essential services and on the operational resilience of the State (BALMFORTH, 2024).

From the national doctrinal perspective, this attack can be interpreted as a cyber interdiction action, whose purpose was to deny freedom of action to the enemy through the degradation of critical infrastructure, as described in the Manual of Military Doctrine of Cyber Defense (BRASIL, 2017). The episode demonstrates the effectiveness of G Ciber when acting as a vector for the denial of C2 capabilities, both in the military sphere and in critical civilian infrastructure, both in the ground and air dimensions.

In addition, the attack on Kyivstar highlights the risk of civilian targets being employed as strategic vectors in G Ciber. The impact on the population and on civil communication systems reinforces the argument that the boundaries between cyberspace and the physical operating environment are increasingly blurred, as already warned by Kello (2013) when he characterized G Ciber as a vector of "ambiguous hostility".

The incident also highlights the centrality of cyber protection (Ptç Ciber) as an activity of an interagency nature. In the Ukrainian context, most critical infrastructure – telecommunications, energy, transport – belongs to the civilian sector or operates under a mixed regime, making cyber defense a shared responsibility between military bodies, government agencies, private companies, and international organizations. The attack on Kyivstar highlighted how failures or limitations in the articulation between these actors can compromise the resilience of the system as a whole, directly impacting civil society, essential services and, consequently, military operations themselves. Thus, the response to this type of threat requires not only technical capabilities, but also cooperation, information exchange, and trust-building between different sectors, including rapid response mechanisms, integrated contingency plans, and public cybersecurity policies.

In practical terms, the response to the attack mobilized not only Kyivstar's internal team, but also Ukrainian cyber defense officials and international partners. Despite efforts, the full restoration of services was slow, highlighting challenges related to early detection, isolation of compromised systems, and infrastructure recovery (EUREPOC, 2024). Experience indicates that, in the face of persistent and sophisticated attacks, even robust protection measures can be insufficient without an integrated, continuous, and adaptive

approach to cybersecurity. This reinforces the need for investments in training, technology and, above all, in collaborative processes between public and private actors.

The international repercussion of the case, combined with its technical complexity, elevated the incident to the status of a symbolic milestone for G Ciber in the Russian-Ukrainian conflict, being cited by several experts as one of the most impactful attacks against civilian infrastructure in an active war zone (Wired, 2024). As a case study, it synthesizes the tactical and operational dimensions of G Ciber.

CONCLUSION

The results presented in this study show the breadth of the use of G Ciber as a combat vector in the context of the Russian-Ukrainian conflict (2022–2024), revealing both points of convergence and tension in relation to Brazilian military doctrine, especially as outlined in the Cyber Warfare Manual.

A first relevant aspect concerns the synchronization between Cyber Atk and physical conflict escalations, as discussed in subsection 4.3. The national doctrine postulates that Cyber Atk should be conducted, preferably, in support of conventional military campaigns, either to amplify their effects or to paralyze the enemy's capabilities. This principle is supported by the analysis of data from Ukraine as a target country, where a higher frequency of intense attacks was observed in periods classified as HIIK 5. In the Russian case, the more diffuse and constant pattern of attacks suggests a cybernetic use with characteristics less integrated into the military operational cycle, which signals the possibility of cyber lines of action independent of conventional maneuvers, configuring themselves as forms of attrition, deterrence, or prolonged strategic sabotage.

Another point of confrontation lies in the association between cybernetic intensity and the occurrence of physical effects, discussed in subsection 4.2. The doctrine recognizes that offensive cyber operations can generate concrete physical effects, especially when applied against industrial, energy, and communications systems. The EuRepoC data corroborate this conception by indicating that the few attacks that caused verifiable physical effects were precisely those of greater weighted intensity, corroborating the doctrinal understanding that the effectiveness of Cyber Ofs Op stems from the combination of persistence, informational superiority and a high degree of technical coordination on targets of tactical or strategic value.

On the other hand, the small number of events with physical effects — only three in the entire sample — raises an important issue that is not sufficiently addressed by Brazilian doctrine: the low frequency and limited visibility of physical effects on the real cyber

battlefield. G Ciber, as warned by Rid (2012) and Valeriano et al. (2018), does not always translate into immediate material destruction, but can be used as a tool of informational warfare, aiming to compromise internal cohesion, degrade institutional trust, and manipulate adversarial perceptions.

The case study of the attack on Kyivstar reinforces the doctrinal premises of G Ciber as a vector of interdiction and paralysis. Atk Ciber clearly exemplifies the coordinated use of cyber technical capabilities to compromise the availability of communications and, consequently, the response and mobilization capacity of the civilian population and the armed forces. Brazilian doctrine provides for this type of operation as part of offensive Cyber Operations, and the actions of the Sandworm group empirically exemplify the doctrinal conception of cyber interdiction actions, aimed at degrading critical infrastructure and denying the enemy's freedom of action. Thus, the Russian-Ukrainian conflict confirms the importance of convergence operations as a paradigm for the integration of capabilities in future conflicts.

Finally, it is relevant to highlight that the national doctrine, although structured based on consolidated foundations of military use, still presents opportunities for updating regarding the full integration between physical and cyber domains. The study presented here reinforces the usefulness of systematic empirical analyses — such as those provided by the EuRepoC database — as a relevant input for continuous doctrinal updating, especially with regard to the characterization of effects, attribution of authorship, and integration between operational and cyber domains.

It is necessary to recognize, however, the limitations of this study. First, the analysis was restricted to the data available in the EuRepoC database, which depend on open registries and, therefore, may suffer from underreporting and attribution bias, especially in environments with low informational transparency. In addition, the impossibility of systematically distinguishing between cyber attacks and exploits in the analyzed databases restricts the detailed understanding of the role of each modality in the unfolding of events. Another limitation is the absence of systematized data on cyber protection actions (Ptç Ciber), an aspect that proved to be relevant especially in the case study, where the defense of critical infrastructures involves strong articulation between civilian, military, and private agencies. Future research can explore mixed-analysis methodologies, incorporate expert interviews, and examine in greater detail both protection mechanisms and the full cycle of cyber operations, broadening understanding of their integration and impact in real-world conflict scenarios.

REFERENCES

1. Balmforth, T. (2024, January 4). Exclusive: Russian hackers were inside Ukraine telecoms giant for months. Reuters. https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/

2. Basmat, D. (2023, December 21). Ukraine downs 34 of 35 Russian Shahed drones in latest overnight attack. *The Kyiv Independent*. https://kyivindependent.com/air-force-ukraine-downs-34-of-35-drones-launched-by-russia-overnight/

3. Brazil, Ministry of Defense, Brazilian Army, Land Operations Command. (2017). *Cyber warfare – EB70-MC-10.232* (1st ed.). Brasília.

4. Brazil, Ministry of Defense, Joint Chiefs of Staff of the Armed Forces. (2023a). *Military doctrine of cyber defense – MD31-M-07* (2nd ed.). Brasília.

5. Brazil, Brazilian Army, Army General Staff. (2023b). Manual of fundamentals operational concept of the Brazilian Army – Convergence operations 2040 – EB20-MF-07.101 (1st ed.). Brasília: EME.

6. Europolitics. (2024). *European repository of cyber incidents (EuRepoC)*. Heidelberg University. https://eurepoc.eu/

7. Heidelberg Institute for International Conflict Research. (2024). *Conflict barometer 2023*. HIIK. https://hiik.de/wp-content/uploads/2024/12/coba23_v3.pdf

8. Kello, L. (2013). The meaning of the cyber revolution: Perils to theory and statecraft. *International Security, 38*(2), 7–40. https://doi.org/10.1162/ISEC_a_00138

9. Marini, A. N. L., Pederneiras, L. C., & Moita, S. T. (2024). Cyberwarfare from Clausewitz's perspective: A case study on Stuxnet. *Malala, International Journal of Middle East and Muslim World Studies, 12*(15), 159–178.

10. National Public Radio. (2023, December 29). Russia launches massive air assault across Ukraine, killing at least 31. *NPR*. https://www.npr.org/2023/12/29/1222099484/russia-launches-aerial-attacks-against-ukraine

11. Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies, 35*(1), 5–32. https://doi.org/10.1080/01402390.2011.608939

12. Valeriano, B., Jensen, B., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.

13. Wired. (2023, December 13). Hacker group linked to Russian military claims credit for cyberattack on Ukrainian telecom. *Wired*. https://www.wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru/

.