Revista ARACÊ
ISSN: 2358-2472

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/arev7n6-239

Data de submissão: 20/05/2025 **Data de publicação:** 20/06/2025

João Marcos Barbosa Oliveira
Mestrando em Ciências Militares (EsAO)
Rio de Janeiro, Rio de Janeiro - Brasil
E-mail: barbosaoliveira.joao@eb.mil.br

Carlos Henrique do Nascimento Barros
Doutor em Ciências Militares (ECEME)
Rio de Janeiro, Rio de Janeiro - Brasil
E-mail: carloshnbarros@gmail.com

Ismael Deus Marques
Mestre em Políticas Públicas e Governo (FGV)
Brasília, DF - Brasil
E-mail: ismaeldmarques@gmail.com

Jovair Pazzini de Melo Souza
Mestrando em Ciências Militares (EsAO)
Rio de Janeiro, Rio de Janeiro - Brasil
E-mail: pazzini.jovair@eb.mil.br

Eduardo Stefani
Doutorando em Informática e Gestão do Conhecimento (UNINOVE)
São Paulo, São Paulo - Brasil
E-mail: eduardo_stefani@uni9.edu.br

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.

Revista ARACÊ
ISSN: 2358-2472

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. 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.

Revista ARACÊ
ISSN: 2358-2472

1 INTRODUÇÃO

A incorporação das Tecnologias da Informação e Comunicação (TIC) ao ambiente operacional ampliou o espectro de ação das Operações Militares Terrestres, possibilitando a integração do ciberespaço como domínio de combate. No contexto do conflito russo-ucraniano (2022–2024), observou-se um uso de capacidades cibernéticas ofensivas tanto por atores de diferentes naturezas, atuando em ativos de tecnologia militares ou não, evidenciando o emprego coordenado de capacidades em múltiplos domínios, como previsto em princípios doutrinários de manobra comumente observados em forças armadas ao redor do mundo

Na doutrina militar brasileira (BRASIL, 2017, p. 18), a Guerra Cibernética (G Ciber) "[..] corresponde ao uso ofensivo e defensivo de informação e sistemas de informação para negar capacidades de C2 [Comando e Controle] ao adversário, explorá-las, corrompê-las, degradá-las ou destruí-las [...]". Constitui uma forma de conflito assimétrico com potencial de integração às ações táticas, operacionais ou estratégicas das Forças Terrestres, potencializando seus efeitos ou antecipando ações cinéticas por meio da negação, dissuasão ou paralisação de funções críticas do inimigo (BRASIL, 2023a).

Nesse contexto, o presente estudo tem como objetivo analisar, a partir de dados empíricos da base EuRepoC (*European Repository of Cyber Incidents*), de que forma a G Ciber se articula com o conflito físico tradicional no teatro de operações ucraniano. Para isso, a análise foi estruturada em três eixos principais: (1) a correlação entre intensidade cibernética e intensidade física do conflito; (2) a ocorrência de efeitos físicos em decorrência de ataques cibernéticos; e (3) a distribuição temporal dos ataques cibernéticos em relação às escaladas do conflito armado.

Autores como Rid (2012) e Valeriano, Jensen e Maness (2018) têm debatido a efetividade estratégica de operações cibernéticas em guerras interestatais. Apesar das divergências quanto à sua efetividade estratégica isolada, há concordância de que tais operações contribuem para a disrupção de fluxos logísticos, degradação de infraestrutura crítica e saturação de sistemas de C2. No caso da Ucrânia, episódios como o ataque à infraestrutura da Kyivstar, em dezembro de 2023, ilustram a possibilidade de impactos físicos concretos oriundos do domínio cibernético.

Diante disso, este artigo se propõe a contribuir com a literatura especializada de estudos de doutrina militar e cibersegurança ao combinar uma abordagem empírica, baseada em dados sistematizados de incidentes cibernéticos, tomando como referencial teórico a doutrina militar terrestre brasileira e estudos internacionais sobre G Ciber.

Revista ARACÊ
ISSN: 2358-2472

2 REFERENCIAL TEÓRICO

A G Ciber é comumente observada como uma capacidade essencial no escopo da doutrina de Operações Militares Terrestres, integrando o esforço conjunto, coordenado e simultâneo dos diversos meios de combate no campo de batalha contemporâneo através das chamadas Operações Cibernéticas (Op Ciber) (BRASIL, 2023a). Para a doutrina militar do Exército Brasileiro (BRASIL, 2017, p. 18), a G Ciber "compreende ações que envolvem as ferramentas de TIC para desestabilizar ou tirar proveito dos sistemas de informação do oponente e defender os próprios Sist Info".

Na Doutrina Militar de Defesa Cibernética do Brasil (BRASIL, 2023a), as Op Ciber podem ser classificadas em três tipos: ataque cibernético (Atq Ciber), exploração cibernética (Exp Ciber) e proteção cibernética (Ptç Ciber). Os Atq Ciber, particularmente, visam degradar, destruir ou manipular sistemas e informações adversárias, podendo ser empregadas de forma autônoma ou como parte integrante de campanhas militares mais amplas. Em conflitos armados, essas operações podem ser sincronizadas com ações cinéticas para potencializar seus efeitos, sendo executadas em apoio a ações de interdição, negação de área ou paralisia de comando (BRASIL, 2017).

No âmbito das Op Ciber Ofs, destaca-se o conceito de interdição, que consiste na execução de ações voltadas a negar a liberdade de ação do inimigo, por meio da degradação ou neutralização de suas infraestruturas críticas, fluxos de informação e capacidades de comando e controle (BRASIL, 2017). Essas ações podem anteceder ou acompanhar ofensivas convencionais, sendo planejadas para comprometer a capacidade de resposta e articulação do adversário. A interdição cibernética representa, portanto, uma forma de potencializar os efeitos de campanhas militares por meio do rompimento da coesão operacional do inimigo.

A Exp Ciber, por sua vez, compreende ações que visam obter informações sensíveis de sistemas computacionais adversários, sem necessariamente causar degradação perceptível ou imediata desses ativos. Essas ações buscam comprometer a confidencialidade da informação, conduzidas com caráter velado e prolongado, para apoiar outras operações militares por meio da coleta de inteligência (BRASIL, 2017). A distinção entre Exp Ciber e Atq Ciber reside, em essência, no pilar da segurança da informação afetado: enquanto a exploração compromete a confidencialidade, o ataque impacta a disponibilidade e/ou integridade dos sistemas.

Já a Ptç Ciber corresponde ao conjunto de medidas e capacidades voltadas à defesa ativa e passiva dos sistemas e redes das Forças Armadas, garantindo a liberdade de ação no ciberespaço, assegurando o funcionamento contínuo de suas capacidades críticas e promovendo a resiliência cibernética das infraestruturas de missão. A Ptç Ciber abrange desde o monitoramento de ativos e

Revista ARACÊ
ISSN: 2358-2472

detecção de intrusões até a contenção de ameaças e a recuperação de sistemas, sendo essencial para preservar a integridade, a disponibilidade e a confidencialidade das informações operacionais. De acordo com a doutrina brasileira, a eficácia da Ptç Ciber depende da integração entre recursos tecnológicos, pessoal qualificado e processos bem definidos, alinhados ao ciclo de gestão da segurança da informação (BRASIL, 2017).

A doutrina brasileira também ressalta a importância da sinergia entre os domínios físico e cibernético, especialmente em operações de larga escala. A capacidade de integrar ações cibernéticas com manobras terrestres, aéreas ou informacionais amplia o espectro de combate e contribui para o alcance de superioridade decisória (BRASIL, 2017). Esse alinhamento se insere no conceito de operações de convergência, no qual ações cibernéticas e convencionais atuam de forma coordenada para maximizar os efeitos militares (BRASIL, 2023b). Nesse contexto, a proteção da infraestrutura crítica nacional assume papel estratégico, sendo considerada um dos principais objetivos das ações de Ptç Ciber. A continuidade dos serviços essenciais e a preservação dos ativos tecnológicos das Forças Armadas são condições indispensáveis para garantir a liberdade de ação no ciberespaço, elemento central da operacionalidade no século XXI.

No plano internacional, autores como Thomas Rid (2012) argumentam que as Op Ciber, diferentemente de outras dimensões da guerras convencional, raramente produzem mortes ou destruição física imediata, sendo caracterizadas, majoritariamente, como ações de efeitos limitados, voltadas à desorganização, sabotagem ou espionagem. Entretanto, estudos mais recentes indicam que, quando integradas a campanhas militares, tais operações podem assumir características estratégicas, como evidenciado em ataques à infraestrutura crítica, ao comando e controle e às redes de comunicação dos oponentes (VALERIANO; JENSEN; MANESS, 2018). Corroborando essa perspectiva, Marini, Pederneiras e Moita (2024) destacam que a rápida evolução tecnológica e o protagonismo do ciberespaço têm tornado cada vez mais recorrente o emprego de G Ciber como instrumento para alcançar objetivos militares e políticos, inclusive promovendo impactos significativos sobre infraestruturas críticas estatais. O caso Stuxnet, analisado pelos autores, evidencia que Op Ciber podem ser caracterizadas como atos de guerra quando empregadas com o propósito de compelir a vontade do oponente e atingir finalidades estratégicas.

A literatura também enfatiza o papel da G Ciber em conflitos híbridos, nos quais ações irregulares, desinformação, influência política e operações cibernéticas são empregadas de forma coordenada. Segundo Kello (2013), a G Ciber desafia as fronteiras tradicionais entre paz e guerra, criando um estado contínuo de hostilidade ambígua, típico dos chamados conflitos em zona cinzenta, no qual Atq Ciber ou Exp Ciber precedem, acompanham ou substituem confrontos físicos.

Revista ARACÊ
ISSN: 2358-2472

Do ponto de vista doutrinário, a G Ciber pode ainda apoiar o conceito de Manobra Militar, ao atuar sobre os vetores de tempo, espaço e informação, contribuindo para o rompimento da coesão inimiga e para a superioridade decisória das forças amigas (BRASIL, 2017). Essa capacidade torna-se particularmente relevante em operações ofensivas, defensivas e de estabilização, como observado em diversas campanhas modernas, inclusive no contexto do conflito entre Rússia e Ucrânia. Com isso, coloca-se a pergunta estudada nesse artigo: a forma com que a guerra cibernética observada em contextos em que há manobra militar corrobora com o que é descrito pela doutrina militar brasileira, isto é, de coordenação das ações físicas e cibernéticas?

3 METODOLOGIA

Este estudo adota uma abordagem qualitativa e quantitativa, com base na análise de dados empíricos provenientes da base EuRepoC – *European Repository of Cyber Incidents*, concentrando-se no período de janeiro de 2022 a dezembro de 2024, correspondente a dois anos do conflito russo-ucraniano. O objetivo da metodologia é identificar padrões e correlações entre o emprego da G Ciber e observações na manobra militar.

Metodologicamente os ataques cibernéticos foram classificados com base no país afetado pelo ataque cibernético. Essa escolha se justifica devido à dificuldade de identificar a origem dos Atq e Exp Ciber, isto é, grupos estatais e não estatais podem camuflar a origem de suas ações, porém o país alvo é mais facilmente identificado.

A pesquisa está estruturada em três eixos analíticos:

- Análise da correlação entre intensidade cibernética e intensidade do conflito físico;
- Identificação de ataques cibernéticos com efeitos físicos diretos ou indiretos;
- Observação da cronologia dos ataques cibernéticos em relação a momentos de escalada ou de retração do conflito armado.

A base de dados utilizada contém 198 registros únicos, categorizando incidentes cibernéticos por atributos como data de ocorrência, país alvo (*receiver_main_country*), tipo de operação (*attack_type*), intensidade cibernética (*weighted_cyber_intensity*), existência de impactos físicos (*physical_impact*), e associação com eventos militares (*offline_conflict_intensity*). As análises foram realizadas com uso da linguagem R, com apoio dos pacotes *tidyverse*, *lubridate* e *ggplot2* para manipulação, limpeza e visualização dos dados.

Para a análise do primeiro eixo, os registros foram segmentados por país alvo e classificados conforme a intensidade do conflito físico associada ("*Yes*", "*Unknown*" ou "*Not available*"),

Revista ARACÊ
ISSN: 2358-2472

permitindo a construção de *boxplots* comparativos. Já no segundo eixo, foram filtrados os eventos que apresentaram a variável *physical_impact* marcada como verdadeira. O terceiro eixo consistiu na agregação dos incidentes ao longo do tempo e na comparação visual com indicadores de escalada do conflito físico, observando possíveis correlações temporais. Foi adotado o termo Operação Cibernética Ofensiva (Op Ciber Ofs) para abranger tanto ações de Atq Ciber quanto Exp Ciber, tendo em vista que originalmente a base da EuRepoC não faz essa distinção.

Além da abordagem quantitativa, o artigo também incorpora um estudo de caso ilustrativo, centrado no ataque cibernético contra a infraestrutura da operadora Kyivstar, ocorrido em dezembro de 2023. Este incidente foi selecionado por apresentar elevada intensidade cibernética e impactos físicos relevantes, além de ampla repercussão na mídia e em fontes especializadas, sendo cruzado com informações externas a partir de fontes abertas e acadêmicas.

A escolha metodológica pela base EuRepoC deve-se à sua ênfase em ataques atribuídos e documentados, com curadoria acadêmica, o que a torna adequada para estudos de correlação entre ações cibernéticas e fenômenos geopolíticos. Contudo, reconhece-se como limitação a dependência de dados abertos e a possível subnotificação de incidentes, especialmente em ambientes com menor transparência informacional.

4 RESULTADOS

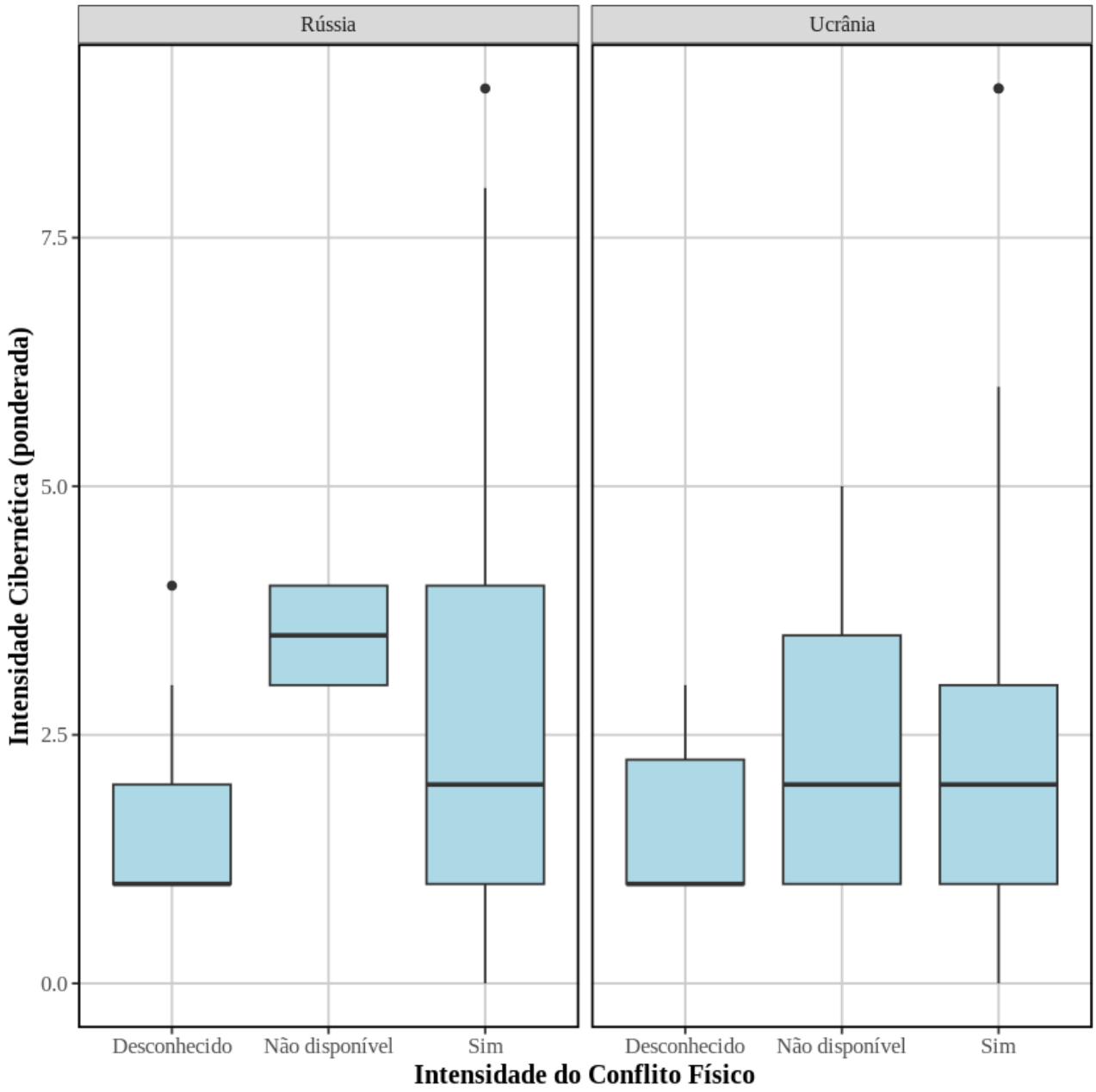
Esta seção apresenta os resultados obtidos a partir da análise dos incidentes cibernéticos ocorridos entre 2022 e 2024, com ênfase na relação entre a G Ciber e o conflito físico tradicional no contexto da guerra russo-ucraniana. Os dados analisados, extraídos da base EuRepoC, foram organizados e visualizados em gráficos que permitem compreender as possíveis correlações entre intensidade cibernética, efeitos físicos e momentos de escalada do conflito armado. A discussão dos resultados é estruturada em torno dos três tópicos investigativos delineados na metodologia, com atenção especial aos pontos que dialogam diretamente com os conceitos e orientações contidas no Manual de Doutrina Militar de Defesa Cibernética (BRASIL, 2017).

4.1 CORRELAÇÃO ENTRE A INTENSIDADE DO CONFLITO FÍSICO E A INTENSIDADE CIBERNÉTICA

A Figura 1 apresenta um boxplot comparando a intensidade cibernética ponderada (*weighted_cyber_intensity*) com a variável de intensidade do conflito físico (*offline_conflict_intensity*), segmentada pelo país alvo (Ucrânia e Rússia).

Revista ARACÊ
ISSN: 2358-2472

Figura 1 – Intensidade Cibernética vs Conflito Físico por País Alvo (2022–2024)



Fonte: Os autores, com dados da EuRepoC (2024)

A análise do gráfico revela que, no caso da Rússia como país alvo, há uma maior concentração de Op Ciber Ofs com elevado grau de complexidade e sofisticação, mesmo em registros classificados como de "baixa ou desconhecida intensidade" do conflito físico. Esse achado sugere que, no caso russo, há uma maior flexibilidade no emprego das Op Ciber Ofs, mesmo fora do escopo das ações cinéticas, ampliando as possibilidades previstas na doutrina brasileira quanto à sincronização entre domínios. Em contraste, os incidentes direcionados à Ucrânia apresentam distribuição mais uniforme

Revista ARACÊ
ISSN: 2358-2472

entre os diferentes níveis de intensidade física, com uma leve tendência de aumento de intensidade cibernética em eventos associados a combates mais intensos.

Esse resultado oferece um contraponto relevante à doutrina brasileira, que postula que as Op Ciber Ofs tendem a ser sincronizados com ações cinéticas, como forma de potencializar os efeitos das operações (BRASIL, 2017). No caso russo, observa-se um número significativo de Op Ciber Ofs de alta intensidade mesmo em contextos sem associação direta com escaladas físicas, sugerindo que, nesse contexto específico, a G Ciber pode operar com relativa independência das ações convencionais, servindo, por exemplo, a propósitos de sabotagem, pressão estratégica ou dissuasão.

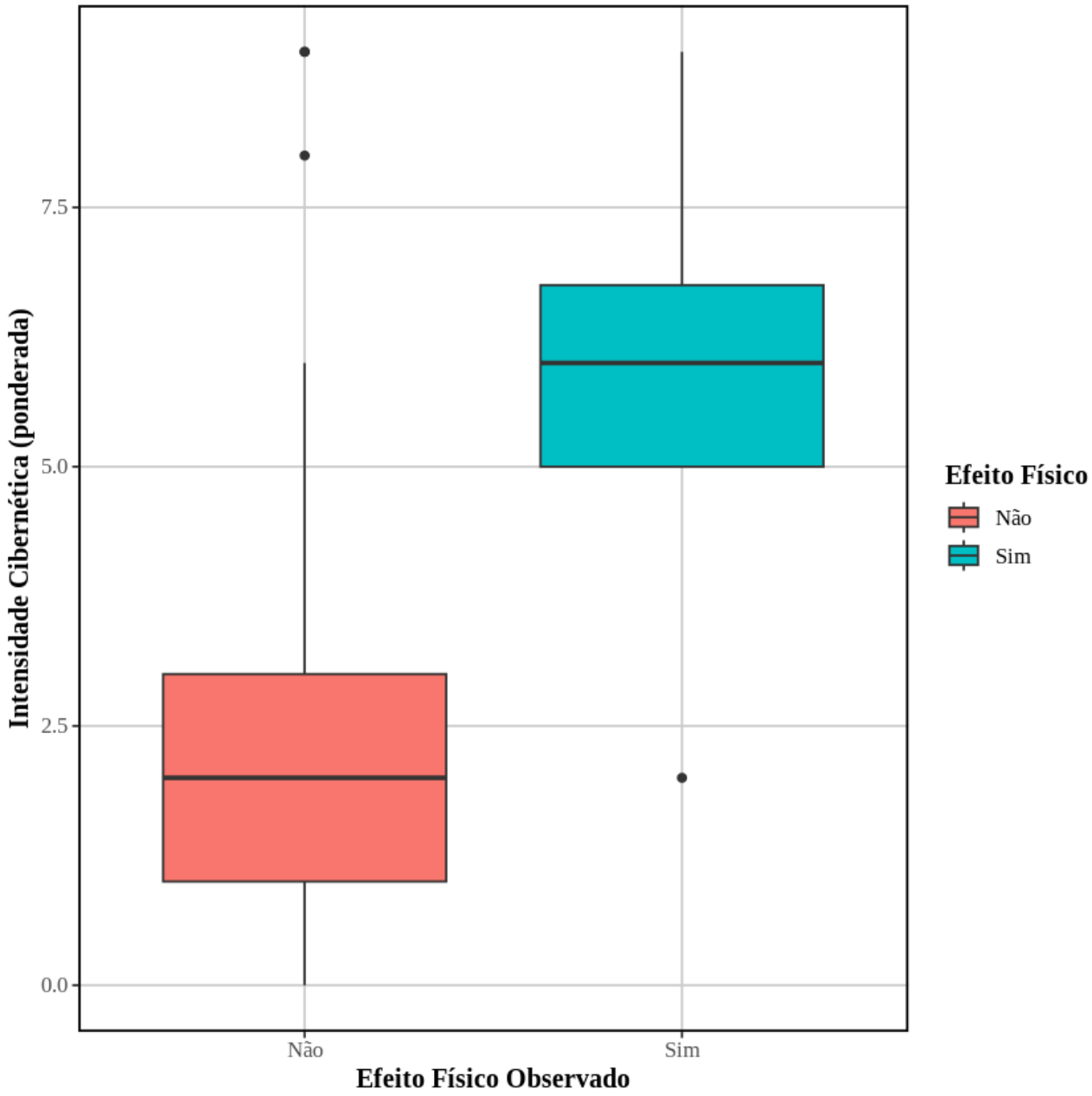
No caso da Ucrânia, a maior coerência entre as intensidades sugere uma integração mais próxima entre os domínios físico e cibernético, alinhada ao que a doutrina brasileira define como emprego coordenado de capacidades para obter superioridade decisória e romper a coesão inimiga (BRASIL, 2017).

4.2 INTENSIDADE CIBERNÉTICA POR OCORRÊNCIA DE EFEITOS FÍSICOS

A Figura 2 apresenta a distribuição da intensidade cibernética ponderada (*weighted_cyber_intensity*) conforme a ocorrência ou não de efeitos físicos observáveis em decorrência dos ataques. A análise evidencia uma distinção clara: as poucas Op Ciber Ofs que geraram efeitos físicos (“Sim”) apresentam medianas significativamente mais altas, com predominância de pontuação entre 6 e 8 no índice de intensidade ponderada. Já as Op Ciber Ofs que não geraram tais efeitos (“Não”) se concentram entre 1 e 4 pontos, com dispersão e presença de *outliers* de intensidade baixa.

Revista ARACÊ
ISSN: 2358-2472

Figura 2 – Intensidade Cibernética por Ocorrência de Efeitos Físicos



Fonte: Os autores, com dados da EuRepoC (2024)

Esse padrão reforça a doutrina brasileira ao indicar que quanto maior a intensidade da Op Ciber Ofs, nesse caso, Atq Ciber, maior o potencial de geração de efeitos físicos concretos, como disrupção de serviços, degradação de infraestruturas críticas ou comprometimento de sistemas de comando e controle (BRASIL, 2017). Ainda que a amostra de ataques com efeitos físicos seja pequena, o desvio entre os grupos é nítido e visualmente consistente.

Revista ARACÊ
ISSN: 2358-2472

Do ponto de vista doutrinário, esse resultado corrobora a premissa de que a G Ciber, quando aplicada com suficiente escala, sofisticação e tempo de persistência, é capaz de gerar efeitos físicos comparáveis aos da guerra convencional, principalmente sobre alvos civis e infraestruturas críticas. Ainda segundo o manual de Doutrina Militar de Defesa Cibernética (BRASIL, 2023a), tais Atq Ciber tendem a ser empregados em apoio a campanhas ofensivas, de interdição ou para paralisação de comando, o que reforça a relevância tática da G Ciber.

4.3 CRONOLOGIA DOS ATAQUES CIBERNÉTICOS E MOMENTOS DE ESCALADA

Na Figura 3, observa-se a linha do tempo dos ataques cibernéticos classificados por intensidade e país alvo, com coloração indicando a intensidade do conflito físico segundo o sistema HIIK (quando disponível). Os pontos se distribuem de maneira relativamente equilibrada entre Ucrânia e Rússia, mas com diferenças qualitativas importantes.

A sigla HIIK refere-se ao *Heidelberg Institute for International Conflict Research*, um centro de pesquisa vinculado à Universidade de Heidelberg, na Alemanha. Esse instituto é responsável pela produção do *Conflict Barometer*, um relatório anual que documenta e classifica os conflitos políticos em todo o mundo com base em critérios de intensidade, atores envolvidos e dinâmica do confronto.

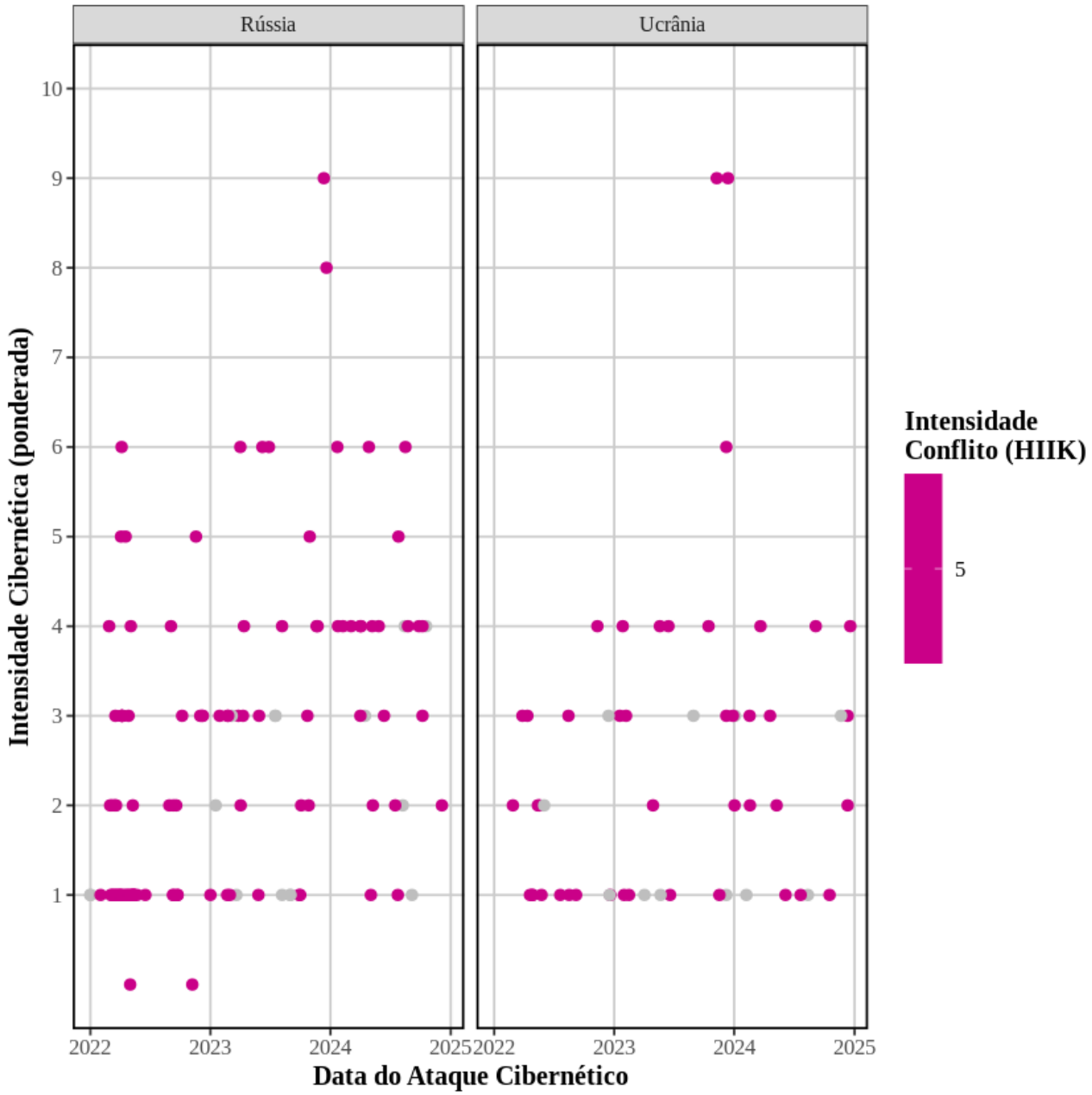
O sistema HIIK utiliza uma escala ordinal de 1 a 5 para classificar a intensidade de conflitos, sendo:

- Nível 1: Disputa latente
- Nível 2: Conflito manifesto
- Nível 3: Crise
- Nível 4: Conflito severo
- Nível 5: Guerra

Essa classificação leva em conta variáveis como o uso da força, número de vítimas, danos estruturais e duração do enfrentamento. No contexto deste artigo, a variável *offline_conflict_intensity_subcode* da base EuRepoC associa cada incidente cibernético, quando possível, a um nível de intensidade HIIK, permitindo cruzar os eventos no ciberespaço com momentos de escalada no conflito físico convencional.

Revista ARACÊ
ISSN: 2358-2472

Figura 3 – Linha do Tempo: Intensidade Cibernética e Escalada do Conflito Físico (por País Alvo)



Fonte: Os autores, com dados da EuRepoC (2024).

Para a Rússia como país alvo, há uma maior densidade de ataques ao longo do tempo, com intensidades moderadas e altas (acima de 4) distribuídas de forma relativamente constante. Isso sugere a existência de uma campanha cibernética prolongada, possivelmente associada a operações de desgaste, desinformação e sabotagem em períodos distintos do conflito.

No caso da Ucrânia, por outro lado, os ataques de maior intensidade estão mais concentrados em momentos críticos — como o final de 2023 — e se alinham visualmente com a presença do maior

Revista ARACÊ
ISSN: 2358-2472

número de registros de conflito físico intenso (HIIK 5). Em especial, em 29 de dezembro de 2023, a Rússia realizou o maior ataque aéreo desde o início da guerra, empregando 158 mísseis e drones contra cidades como Kyiv, Kharkiv, Dnipro e Lviv, resultando em pelo menos 31 mortes e danos severos a infraestruturas civis (NPR, 2023). Além disso, na noite de 20 para 21 de dezembro, múltiplos ataques com drones *Shahed* também foram lançados de diferentes frentes, intensificando os combates em regiões como Dnipropetrovsk, Sumy e Poltava (BASMAT, 2023). Esse sincronismo reforça a hipótese de que, neste teatro, a G Ciber foi empregada como vetor de apoio direto às operações militares convencionais, conforme preconizado pela doutrina brasileira (BRASIL, 2017), atuando como multiplicador de efeitos em campanhas ofensivas.

Visualmente, essa integração entre domínios no caso ucraniano evidencia o uso da G Ciber como meio de desorganização e negação de capacidades, sobretudo em momentos de escalada. Já no caso russo, sua função parece mais dispersa e contínua, o que sugere diferenças doutrinárias e operacionais entre os beligerantes no tocante ao emprego da G Ciber como vetor tático ou estratégico. Esses achados ilustram, na prática, a aplicação do conceito de operações de convergência, previsto na doutrina militar brasileira (BRASIL, 2023b).

4.4 ESTUDO DE CASO: ATAQUE À KYIVSTAR (2023)

Entre os incidentes registrados na base EuRepoC com intensidade cibernética máxima (9/10), destaca-se o ataque realizado contra a Kyivstar, maior operadora de telecomunicações da Ucrânia, ocorrido em dezembro de 2023. O evento, atribuído ao grupo *Sandworm*, vinculado ao serviço de inteligência militar russo (GRU), foi classificado com efeitos físicos confirmados e associado a um momento de conflito físico de alta intensidade (HIIK 5), sendo um exemplo emblemático da sinergia entre operações cibernéticas e ações convencionais no teatro ucraniano.

Segundo o próprio chefe da inteligência cibernética da Ucrânia, os atacantes permaneceram infiltrados na rede da Kyivstar por vários meses antes de iniciar o ataque de destruição (BALMFORTH, 2024). Esse padrão evidencia a relação direta entre as etapas de Exp Ciber — caracterizadas pelo acesso furtivo, coleta de informações e mapeamento de vulnerabilidades — e a execução posterior do Atq Ciber, responsável pela degradação substancial da infraestrutura crítica. A integração entre Exp Ciber e Atq Ciber no caso Kyivstar demonstra que operações ofensivas bem-sucedidas, especialmente aquelas com impactos físicos e sociais relevantes, dependem do prolongado reconhecimento e preparação realizados de forma velada. O episódio também destaca como a ausência de detecção precoce das atividades exploratórias pode potencializar os danos causados na fase destrutiva do ataque.

Revista ARACÊ
ISSN: 2358-2472

A ofensiva resultou na desativação de serviços móveis e internet para milhões de civis, impactando diretamente os sistemas de alerta aéreo em cidades como Kyiv e Sumy, considerados essenciais para a defesa antiaérea durante bombardeios russos. Além disso, relatórios técnicos indicam a destruição de mais de 10 mil servidores e 4 mil estações de trabalho, caracterizando degradação substancial da infraestrutura crítica nacional, com impactos sobre a continuidade dos serviços essenciais e sobre a resiliência operacional do Estado (BALMFORTH, 2024).

A partir da perspectiva doutrinária nacional, este ataque pode ser interpretado como uma ação de interdição cibernética, cuja finalidade foi negar liberdade de ação ao inimigo por meio da degradação de infraestrutura crítica, conforme descrito no Manual de Doutrina Militar de Defesa Cibernética (BRASIL, 2017). O episódio demonstra a efetividade da G Ciber quando atuando como vetor de negação de capacidades de C2, tanto na esfera militar quanto na infraestrutura civil crítica, tanto na dimensão terrestre, quanto aérea.

Além disso, o ataque à Kyivstar evidencia o risco de alvos civis serem empregados como vetores estratégicos na G Ciber. O impacto sobre a população e sobre sistemas de comunicação civil reforça o argumento de que as fronteiras entre o ciberespaço e o ambiente operacional físico estão cada vez mais difusas, como já alertado por Kello (2013) ao caracterizar a G Ciber como um vetor de "hostilidade ambígua".

O incidente também destaca a centralidade da proteção cibernética (Ptç Ciber) como atividade de natureza interagências. No contexto ucraniano, a maior parte das infraestruturas críticas – telecomunicações, energia, transportes – pertence ao setor civil ou opera sob regime misto, tornando a defesa cibernética uma responsabilidade compartilhada entre órgãos militares, agências de governo, empresas privadas e organizações internacionais. O ataque à Kyivstar evidenciou como falhas ou limitações na articulação entre esses atores podem comprometer a resiliência do sistema como um todo, impactando diretamente a sociedade civil, os serviços essenciais e, por consequência, as próprias operações militares. Assim, a resposta a esse tipo de ameaça demanda não apenas capacidades técnicas, mas também cooperação, troca de informações e construção de confiança entre diferentes setores, incluindo mecanismos de resposta rápida, planos de contingência integrados e políticas públicas de segurança cibernética.

Em termos práticos, a resposta ao ataque mobilizou não apenas a equipe interna da Kyivstar, mas também autoridades ucranianas de defesa cibernética e parceiros internacionais. Apesar dos esforços, a restauração completa dos serviços foi lenta, evidenciando desafios relacionados à detecção precoce, isolamento de sistemas comprometidos e recuperação da infraestrutura (EUREPOC, 2024). A experiência indica que, diante de ataques persistentes e sofisticados, mesmo medidas robustas de

Revista ARACÊ
ISSN: 2358-2472

proteção podem ser insuficientes sem uma abordagem integrada, contínua e adaptativa de cibersegurança. Isso reforça a necessidade de investimentos em treinamento, tecnologia e, sobretudo, em processos colaborativos entre atores públicos e privados.

A repercussão internacional do caso, aliada à sua complexidade técnica, elevou o incidente à condição de marco simbólico da G Ciber no conflito russo-ucraniano, sendo citado por diversos especialistas como um dos ataques mais impactantes contra infraestrutura civil em zona de guerra ativa (Wired, 2024). Como estudo de caso, ele sintetiza as dimensões tática e operacional da G Ciber.

5 CONCLUSÃO

Os resultados apresentados neste estudo evidenciam a amplitude do emprego da G Ciber como vetor de combate no contexto do conflito russo-ucraniano (2022–2024), revelando tanto pontos de convergência quanto de tensão em relação à doutrina militar brasileira, especialmente conforme delineada no Manual de Guerra Cibernética.

Um primeiro aspecto relevante diz respeito à sincronização entre Atq Ciber e escaladas do conflito físico, como abordado na subseção 4.3. A doutrina nacional postula que os Atq Ciber devem ser conduzidos, preferencialmente, em apoio a campanhas militares convencionais, seja para ampliar seus efeitos, seja para paralisar capacidades do inimigo. Esse princípio encontra respaldo na análise dos dados da Ucrânia como país alvo, onde observou-se maior frequência de ataques intensos em períodos classificados como HIIK 5. Já no caso russo, o padrão mais difuso e constante dos ataques sugere um emprego cibernético com características menos integradas ao ciclo operacional militar, o que sinaliza a possibilidade de linhas de ação cibernéticas independentes da manobra convencional, configurando-se como formas de desgaste, dissuasão ou sabotagem estratégica prolongada.

Outro ponto de confronto reside na associação entre intensidade cibernética e ocorrência de efeitos físicos, discutido na subseção 4.2. A doutrina reconhece que operações cibernéticas ofensivas podem gerar efeitos físicos concretos, principalmente quando aplicadas contra sistemas industriais, energéticos e de comunicações. Os dados da EuRepoC corroboram essa concepção ao indicar que os poucos ataques que causaram efeitos físicos verificáveis foram justamente os de maior intensidade ponderada, corroborando o entendimento doutrinário de que a eficácia das Op Ciber Ofs decorre da combinação entre persistência, superioridade informacional e elevado grau de coordenação técnica sobre alvos de valor tático ou estratégico.

Por outro lado, a reduzida quantidade de eventos com efeitos físicos — apenas três em toda a amostra — levanta uma questão importante que não é suficientemente abordada pela doutrina brasileira: a baixa frequência e a limitada visibilidade dos efeitos físicos no campo de batalha

Revista ARACÊ
ISSN: 2358-2472

cibernético real. A G Ciber, como alertado por Rid (2012) e Valeriano et al. (2018), nem sempre se traduz em destruição material imediata, mas pode ser empregada como ferramenta de guerra informacional, visando comprometer a coesão interna, degradar a confiança institucional e manipular percepções adversárias.

O estudo de caso do ataque à Kyivstar reforça as premissas doutrinárias da G Ciber como vetor de interdição e paralisação. O Atq Ciber exemplifica com clareza o emprego coordenado de capacidades técnicas cibernéticas para comprometer a disponibilidade de comunicações e, por consequência, a capacidade de resposta e mobilização da população civil e das forças armadas. A doutrina brasileira prevê esse tipo de operação como parte das Op Ciber ofensivas, e a atuação do grupo Sandworm exemplifica, de forma empírica, a concepção doutrinária de ações de interdição cibernética, voltadas à degradação de infraestrutura crítica e à negação da liberdade de ação do inimigo. Assim, o conflito russo-ucraniano confirma a importância das operações de convergência como paradigma para a integração de capacidades em futuros conflitos.

Por fim, é relevante destacar que a doutrina nacional, embora estruturada com base em fundamentos consolidados de emprego militar, ainda apresenta oportunidades de atualização quanto à integração plena entre domínios físico e cibernético. O estudo aqui apresentado reforça a utilidade de análises empíricas sistemáticas — como as proporcionadas pela base EuRepoC — como insumo relevante para a atualização doutrinária contínua, especialmente no que diz respeito à caracterização de efeitos, atribuição de autoria, e integração entre domínios operacional e cibernético.

Faz-se necessário reconhecer, entretanto, as limitações deste estudo. Em primeiro lugar, a análise foi restrita aos dados disponíveis na base EuRepoC, que dependem de registros abertos e, portanto, podem sofrer de subnotificação e viés de atribuição, sobretudo em ambientes de baixa transparência informacional. Além disso, a impossibilidade de distinguir, de maneira sistemática, entre ataques e explorações cibernéticas nas bases analisadas restringe a compreensão detalhada sobre o papel de cada modalidade no desenrolar dos eventos. Outra limitação está na ausência de dados sistematizados sobre ações de proteção cibernética (Ptç Ciber), aspecto que se mostrou relevante especialmente no estudo de caso, onde a defesa das infraestruturas críticas envolve forte articulação entre agências civis, militares e privadas. Futuras pesquisas podem explorar metodologias de análise mista, incorporar entrevistas com especialistas e examinar em maior detalhe tanto os mecanismos de proteção quanto o ciclo completo das operações cibernéticas, ampliando a compreensão sobre sua integração e impacto em cenários de conflito real.

Revista ARACÊ
ISSN: 2358-2472

REFERÊNCIAS

BALMFORTH, Tom. Exclusive: Russian hackers were inside Ukraine telecoms giant for months. Reuters, 4 jan. 2024. Disponível em: https://www.reuters.com/world/europe/russian-hackers-were-inside-ukraine-telecoms-giant-months-cyber-spy-chief-2024-01-04/. Acesso em: 06 jun. 2025.

BASMAT, Dmytro. Ukraine downs 34 of 35 Russian Shahed drones in latest overnight attack. 21 dez. 2023. Disponível em: https://kyivindependent.com/air-force-ukraine-downs-34-of-35-drones-launched-by-russia-overnight/. The Kyiv Independent. Acesso em: 16 jun. 2025.

BRASIL. Ministério da Defesa. Exército Brasileiro. Comando de Operações Terrestres. Guerra Cibernética – EB70-MC-10.232. 1. ed. Brasília: 2017.

_____. _____. Estado Maior Conjunto das Forças Armadas. Doutrina Militar de Defesa Cibernética – MD31-M-07. 2. ed. Brasília: 2023a.

_____ . Exército Brasileiro. Estado-Maior do Exército. Manual de Fundamentos Conceito Operacional do Exército Brasileiro – Operações de Convergência 2040 - EB20-MF-07.101. 1. ed. Brasília: EME, 2023b.

EUROPOLITICS. European Repository of Cyber Incidents (EuRepoC). Heidelberg: Heidelberg University, 2024. Disponível em: https://eurepoc.eu/. Acesso em: 06 jun. 2025.

HEIDELBERG INSTITUTE FOR INTERNATIONAL CONFLICT RESEARCH (HIIK). Conflict Barometer 2023. Heidelberg: HIIK, 2024. Disponível em: https://hiik.de/wp-content/uploads/2024/12/coba23_v3.pdf. Acesso em: 06 jun. 2025.

MARINI, Amanda Neves Leal; PEDERNEIRAS, Lucas Chrystello; MOITA, Sandro Teixeira. A guerra cibernética sob a ótica de Clausewitz: um estudo de caso sobre o Stuxnet. Malala, Revista Internacional de Estudos sobre o Oriente Médio e Mundo Muçulmano, v. 12, n. 15, p. 159-178, 2024.

NPR. Russia launches massive air assault across Ukraine, killing at least 31. National Public Radio, 29 dez. 2023. Disponível em: https://www.npr.org/2023/12/29/1222099484/russia-launches-aerial-attacks-against-ukraine. NPR. Acesso em: 16 jun. 2025.

KELLO, Lucas. The meaning of the cyber revolution: Perils to theory and statecraft. International Security, v. 38, n. 2, p. 7–40, 2013.

RID, Thomas. Cyber war will not take place. Journal of Strategic Studies, v. 35, n. 1, p. 5–32, 2012.

VALERIANO, Brandon; JENSEN, Benjamin; MANESS, Ryan C. Cyber strategy: The evolving character of power and coercion. Oxford: Oxford University Press, 2018.

Revista ARACÊ
ISSN: 2358-2472

WIRED. Hacker group linked to Russian military claims credit for cyberattack on Ukrainian telecom. Wired, 13 dez. 2023. Disponível em: https://www.wired.com/story/ukraine-kyivstar-solntsepek-sandworm-gru/. Acesso em: 06 jun. 2025.