ARTICLE

DOI 10.52781/cmm.a125

The Russian-Ukrainian Cyber War: Russian attacks on Ukrainian Critical Infrastructure and possible lessons for the Brazilian Army

La ciberguerra ruso-ucraniana: los ataques rusos contra las infraestructuras críticas ucranianas y las posibles lecciones para el Ejército Brasileño

Abstract: What lessons can the Brazilian Army learn about cyber defense in terms of attacks on critical infrastructures in the conflict between Russia and Ukraine? With the evolution of the use of cyberspace, there has been a significant increase in attacks aimed at affecting a State' critical infrastructures. The aim of this work is to analyze what lessons the Brazilian Army can learn from the Russian attacks on Ukrainian critical infrastructures. Thus,with exploratory methodology, the text focuses on understanding the background to the conflict, what actions are being used by Russia to affect Ukraine and how actions within the theater of operations can be related to Brazil's National Cybersecurity Strategy. Therefore, this text points out the changes in Russian strategy linked to the use and adaptation of cyber attacks critical infrastructures, addressing possible lessons that the Brazilian Army can absorb.

Keywords: russo-ukrainian war; critical infrastructures; brazilian army; cyber defense; exploratory.

Resumen: ¿Qué lecciones puede extraer el Ejército Brasileño del conflicto entre Rusia y Ucrania en materia de ciberdefensa ante ataques contra infraestructuras críticas? Con la evolución del uso del ciberespacio, se ha producido un aumento significativo de los ataques para afectar las infraestructuras críticas de un Estado. El objetivo de este trabajo es analizar qué lecciones puede extraer el Ejército Brasileño de los ataques rusos a infraestructuras críticas ucranianas. Así, por medio de una metodología exploratoria, el texto se centra en comprender cuáles fueron los antecedentes del conflicto, qué acciones está tomando Rusia para afectar a Ucrania y la manera en que las acciones en el teatro de operaciones pueden relacionarse con la estrategia nacional de ciberseguridad de Brasil. Por lo tanto, este texto señala los cambios en la estrategia rusa relacionados con el uso y la adaptación de los ciberataques a las infraestructuras críticas, abordando las posibles lecciones que el Ejército Brasileño puede extraer.

Palabras Clave: guerra ruso-ucraniana; infraestructuras críticas; ejército brasileño; ciberdefensa; exploratoria.

Rachel Camilly Soares de Souza
Universidade Estadual da Paraíba
João Pessoa, PB, Brasil
rachelcamillyss@gmail.com

Thays Felipe David de Oliveira
Centro Universitário Estácio
Recife, PE, Brasil
thaysfelipe@gmail.com

Murilo Gustavo de Paula
Centro Universitário Estácio
Goiânia, GO, Brasil
murilogdpaula@gmail.com

Received: Sep. 10, 2023
Approved: Dec. 12, 2023

COLEÇÃO MEIRA MATTOS
ISSN on-line 2316-4891 / ISSN print 2316-4833
http://ebrevistas.eb.mil.br/index.php/RMM/index

1 INTRODUCTION

What insights on Cyber Defense concerning attacks on Critical Infrastructure can be gleaned from the conflict between Russia and Ukraine for the Brazilian Army? In light of technological progress and the identification of cyberspace vulnerabilities, an uptick in attacks has been observed, posing potential threats to a State's critical infrastructures like telecommunications, energy, and finance. These services hold strategic significance as indispensable components for citizens, organizations, and the state, as they play pivotal roles in national security, sovereignty, as well as the integration and sustainable economic development of the state (Segundo, 2019).

Russia's invasion of Ukraine on February 24, 2022, instigated the most significant security crisis in Europe since World War II (Fonseca, 2023). Alongside conventional Kinetic Warfare, Russia engaged in extensive cyber operations in Ukraine before and after the conflict commenced (Schulze; Kerttunen, 2023). From the onset of the conflict, at least six distinct state-linked cracker groups executed approximately 240 cyber operations targeting Ukrainian civilian and military targets (Cerulus, 2019).

A Malware—a comprehensive term encompassing all forms of malicious *software* designed to inflict harm—was used in conjunction with malicious tools and sophisticated hacking tactics, undermining public infrastructures. The ongoing campaign involves *Advanced Persistent Threat* (APT) groups affiliated with Russian intelligence agencies as the primary actors. A cyber attacker is designated as an *Advanced Persistent Threat* (APT) when they target a network or system deliberately over an extended period, seeking to extract sensitive information, gain privileged access, or inflict significant damage. APT attacks are characterized by their stealthy nature, reliance on advanced hacking techniques and vulnerability exploitation, and the adept evasion of detection by conventional security measures. Typically, these actors are highly trained and often affiliated with or even controlled by a State (NCSC, 2018).

Despite Russia's established reputation in cyber warfare, it has fallen short in executing decisive cyber-attacks against Ukraine's Information Technology (IT) infrastructure. The attacker's methods and tools, previously effective, yielded different results this time, contrary to expectations. Additionally, the volume of Russian cyber-attacks was lower than anticipated by Cyber Defense analysts (NCSC, 2018).

Ukraine's success in defending against the Russian cyber offensive can be attributed to three elements: government preparations in the pre-war years, cyber defense assistance from the North Atlantic Treaty Organization (NATO), and European Union countries. We must highlight the involvement of private companies, such as Microsoft, Amazon, and SpaceX, which offered commercial solutions like digital cloud services and Starlink—a satellite constellation project by SpaceX, comprising thousands of small satellites in low Earth orbit, forming an interconnected network that provided critical communications infrastructure (CISA, 2022).

In summary, the research was operationalized via qualitative research methods. Furthermore, in a complementary manner, this article serves as a single-case study. The overarching objective of this work is to analyze the lessons that the Brazilian Army can derive from the Russian attacks on Ukrainian critical infrastructures in 2015.

2 HISTORICAL BACKGROUND CONCERNING RUSSIAN CYBER ATTACKS

Russia has systematically resorted to cyber-attacks against Ukraine. *Crackers*, individuals who illicitly infiltrate computers or computer systems for unlawful purposes, affiliated with the Russian secret services, have been engaged in cyber offensive operations in Ukraine at least since Russia annexed Crimea in 2014. Their targets included universities, electricity companies, the banking sector, and other critical infrastructure. Initially, Russia's objectives were to instigate public frustration and weaken political opponents within the Ukrainian political system. In some cases, attackers employed the *KillDisk* malware, making Ukraine a test bed for developing new cyberweapons (Fonseca, 2023.

In 2014, the pro-Russian hacktivist group (Greenberg, 2017) *CyberBerkut*, linked to the foreign military intelligence agency of the General Staff of the Russian Armed Forces, known as GRU, compromised the Ukrainian central electoral system by deploying the *BlackEnergy malware* to undermine confidence in the electoral process and sow political instability (Greenberg, 2017). On Election Day, *CyberBerkut* also launched a massive campaign of denial-of-service (DDoS) attacks—cyber-attacks designed to overwhelm systems, services, or networks, making them inaccessible to legitimate users. The aim was to delay the final vote count and discredit the electoral process for the population. Although the attack failed in delegitimizing the winner of the 2014 elections, it caused a two-hour delay in the final vote count (CISA, 2022).

In 2015, the APT group *Sandworm*, connected to the GRU, executed the first publicly recognized cyber-attack on an electrical grid (NCSC, 2018). Attackers successfully gained remote control of supervisory control and data acquisition (SCADA) systems at three Ukrainian energy distribution companies, leading to the disruption of power supplies. Approximately 225 thousand people experienced a six-hour power outage (Cisa, 2022). Almost a year after the attack, the Ukrainian energy network became the target of another assault. This time, the *Industroyer malware*, also known as *CrashOverride*, was employed, focusing on cyber-attacks against industrial control systems (ICS). Industroyer was specifically crafted to exploit vulnerabilities present in communication protocols used in industrial control systems, such as the *Modbus* protocol and the IEC 61850 protocol. It stands out as the most significant threat to industrial control systems since the infamous *Stuxnet* incident (Whitehead, 2017). The *malware* facilitated remote control of electrical substation switches and circuit breakers by installing a backdoor into the target system, exploiting protocols used by industrial control systems (ICS) across critical infrastructure. The cyber-attack had an impact on a significant area of Ukraine's capital and was attributed to the *Electrum APT* group, directly associated with *Sandworm* (Whitehead, 2017)..

The most severe cyber incident in Ukraine took place in 2017, when the Russian APT group *Telebots*, also linked to *Sandworm*, unleashed the destructive *NotPetya* malware against Ukraine's financial and energy sectors (Cherepanov; Lipovsky, 2017). *NotPetya* earned its name due to its resemblance to the Petya ransomware, which was active in early 2016, extorting victims for passwords to unlock their data. This time, *NotPetya* sabotaged 10% of computers in Ukraine, regardless of whether the victim paid the ransom or not (Cherepanov; Lipovsky, 2017). It spread throughout Ukraine's financial sector through a popular tax preparation program. Although the attack initially targeted companies within Ukraine, the *malware* spiraled out of control, affecting multinational companies across Europe and the United States (US). The exact impact on the Ukrainian economy remains unclear, but estimated global economic losses exceeded ten million dollars (Greenberg, 2018).

In 2018, US Cyber Command used Russia's past behavior, along with other indicators and warnings signaling that the Russians were poised to repeat its efforts, as justification for launching a pre-emptive operation against the *Internet Research Agency*, a Russian organization engaged in propaganda and influence operations, to prevent attacks during the elections. (Nakashima, 2019). More recently, Russian operations have concocted a mix of sophisticated espionage with criminal malware campaigns. Throughout most of 2020, the Russian cracker group *Cozy Bear* exploited a supply chain vulnerability in the *SolarWinds Orion* program to extract data and digital tools from an extensive list of targets (Sanger; Perlroth; Schmitt, 2020). The operation raised alarm bells, as neither the NSA nor major companies like Microsoft detected the intrusion, suggesting it likely involved a combination of human intelligence and cyber operations to inject malicious coding deep into servers.

On February 23, 2023, on the eve of the Russian invasion, a massive cyber-attack employing the *HermeticWiper malware* targeted Ukrainian government machinery and the financial, aviation, IT, and energy sectors (Greenberg, 2018). Although there is no concrete evidence directly linking the perpetrators of the attack to Russia, the timing and methodology strongly suggest such a connection. The following day, just hours after the invasion, another significant cyber-attack targeted *Viasat's KA-SAT* network, extensively used by the Ukrainian military and police (Saade, 2022). This attack combined DDoS with the *AcidRain malware*, specifically designed for targeting telecommunications equipment. As a result, most *Viasat modems* were rendered inoperable, disrupting broadband Internet service for hundreds of thousands of Ukrainians and military personnel. A secondary effect of this attack was that *AcidRain* crossed borders and impacted other European countries, much like what happened in the case of *NotPetya* (Saade, 2022).

The subsequent major incident occurred in April 2022 when Ukraine's energy infrastructure fell victim to *Industroyer II*, the successor of *Industroyer malware*, with a specific focus on high-voltage electrical substations (Viasat, 2022). The *CaddyWiper malware* was also deployed alongside Industroyer II to erase traces of the attack. It is worth noting that, unlike its predecessor, *Industroyer II* functioned as an autonomous weapon, relegating the intervention of a remote operator (CERT-UA, 2022). This led to a significant update, as such a weapon could be deployed within a corporate network, remaining inactive until the opportune moment for an attack. This behavior introduces complexity for cybersecurity professionals in executing their duties to preempt an attack. These characteristics align with the modus operandi of the Sandworm group, as observed with *Industroyer* in 2016. However, in this instance, no direct impacts on energy availability were observed. The success of the attack can be attributed to the prompt response of the Ukrainian cyber defense authorities, who have amassed considerable experience in recent years, as well as the collaborative assistance of Microsoft and ESET (Zhora, 2022).

3 COOPERATION WITH THE PRIVATE SECTOR

The Ukrainian government and military successfully overcame the initial shock of the invasion and effectively countered these non-cyber attacks. The Ukrainian Computer Emergency Response Team (CERT-UA) collaborated with private companies to mitigate the impact of Russia's cyber offensive and ensure the continuous operation of critical systems with minimal disruption. Anticipating the imminent war, a week before the invasion, the Ukrainian government expressed concerns about data security and sought ways to safeguard it. Previously, Ukrainian law mandated specific government and public sector data to be stored on servers physically located within the country. The legislation was amended, permitting the transfer of sensitive government and private sector data to cloud servers outside Ukraine (Amazon, 2022).

In the subsequent days and weeks, these companies provided assistance, support, and the necessary resources, including computer equipment and data centers outside Ukraine, for the seamless migration of data across all sectors in the country. This collaboration benefited most Ukrainian ministries, universities, and private companies (Poireault, 2022). Effectively, Ukraine traded data sovereignty for enhanced Cyber Defense against Russian attacks. This strategic decision not only allowed the Ukrainian government to function effectively to this day but also enabled the population to maintain a relatively normal online life during the war, with most public services still available. These factors significantly boosted the nation's morale and played a crucial role in sustaining Ukraine's resistance to the invasion (Poireault, 2022).

Another noteworthy aspect was CERT-UA's collaboration with private cybersecurity companies to monitor and identify potential cyber-attacks. Even before the 2022 *Industroyer II* attack, investigators from Microsoft (Poireault, 2022) and ESET (Smith, 2022) were remotely monitoring networks in Ukraine and conducting real-time data analysis to identify potential malicious activity. Additionally, before Ukraine's cyber operations, the first confirmed use of Artificial Intelligence (AI)—a technological advancement enabling systems to simulate human-like intelligence—was documented. According to Microsoft President Brad Smith, Ukraine successfully employed AI to detect, identify, and counter a Russian cyber-attack without human intervention (Papachelas, 2022).

For instance, the Ukrainian AI company Primer adapted its commercial AI-based voice transcription and translation service to process intercepted Russian communications, automatically highlighting information related to Ukrainian forces. Ukraine utilized advanced AI-based facial and image recognition software from Clearview AI to identify deceased Russians through their social media profiles, facilitating the notification of their families about their deaths and the subsequent transfer of their bodies (Mcgee-Abe, 2023).

Resilient and secure communications are imperative for any military operation. Following the cyber-attack on Viasat's satellite communications infrastructure, the Ukrainian Army lost access to satellite communications. This situation jeopardized the country's entire defense, but it was resolved by another private American company, SpaceX, which offered Ukraine free access to its Starlink satellite Internet services. Ukraine promptly adopted the service as a substitute for the compromised government's military communications system, proving both extremely beneficial and successful. The system also demonstrated resistance to signal jamming, as confirmed by SpaceX executive director Elon Musk (Papachelas, 2022).

4 CONSIDERATIONS AND RESULTS OF THE CYBER WAR BETWEEN RUSSIA AND UKRAINE

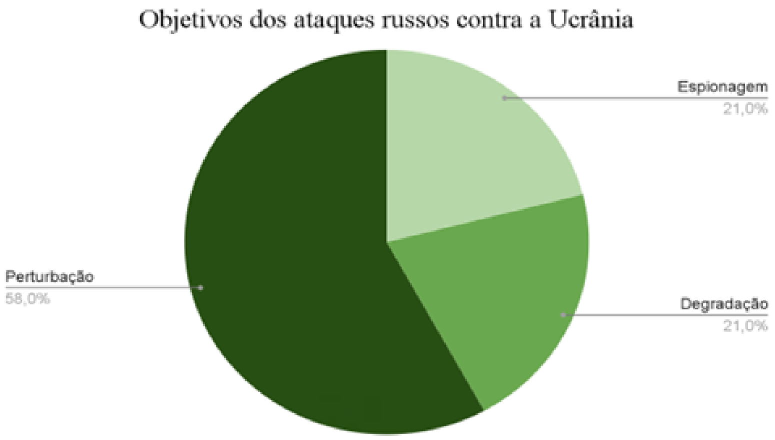
The absence of verifiable information regarding successful Russian cyber-attacks during the war complicates the overall understanding of the actual landscape. Ukraine will probably refrain from publicly disclosing the complete extent of the impacts of Russian cyber offensives on its infrastructure to prevent Russia from gaining a clear idea of the effectiveness of its cyber operations (Werner, 2023). Conversely, Russia may be holding back some of its cyber capabilities for future operations or might be covertly working on a new, undisclosed cyber offensive. In either case, Ukraine's years of preparation seem to have yielded positive results (Werner, 2023).

Data lies at the core of the information age, and events like the 2017 *NotPetya* cyber-attack underscore that cyberspace cannot be restricted to traditional borders. Collateral damage from cyber-attacks can extend well beyond the initial target, with malicious software swiftly spreading across countries and impacting government and corporate data worldwide. Both the public and private sectors cannot afford to overlook the potential damage of such a crisis. The implementation of new resilient strategies is essential to bolster resistance to this kind of attack. As the Ukrainian example illustrates, the advantages of migrating data to clouds outside the country can outweigh the disadvantages, such as the loss of data sovereignty, providing a viable solution. Another factor to consider is that large enterprise data centers providing cloud computing services pose a greater challenge for *APT* groups to compromise compared to local ones (Lewis, 2022).

When analyzing the style of Russian attacks, it is evident that Russia's cyber activity during the war has been more disruptive than degrading, aligning with its previous behavior. As depicted in Graph 1, when scrutinizing these cyber operations by type, Russia's favored cyber objectives continued to involve disruptive modeling activities and cyber espionage campaigns. In the initial months of the 2022 invasion of Ukraine, incidents of disruption accounted for 57.4% of the total actions recorded, followed by espionage at 21.3% (Muelle *et al.*, 2023).

The reliance on disruptive operations contrasts with Russia's pre-war behavior, where there was an increase in espionage. Nevertheless, for both the pre-war sample and the 2022 war sample, degrading cyber operations never constituted the majority (Mueller et al., 2023), as illustrated in Graph 1.

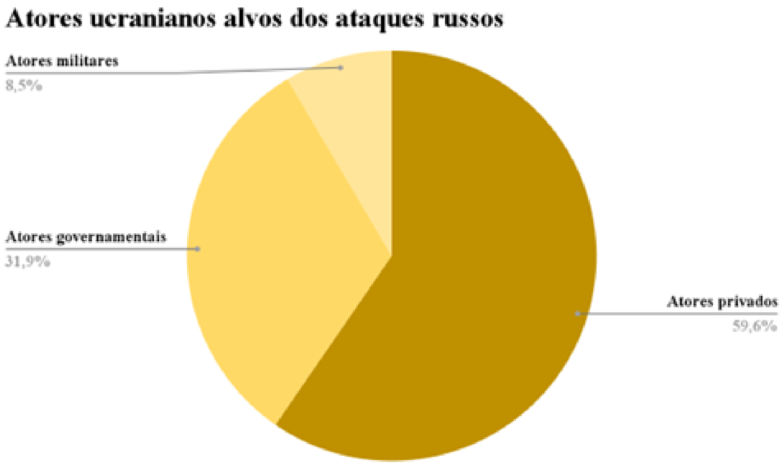
Graph 1 — Objectives of Russian attacks against Ukraine



Source: Lewis, 2022.

Examining Russian cyber-attack targets across the 47 total incidents in 2022 reveals that most (59.6%) were aimed at non-state private actors, with attacks on state and local government actors accounting for 31.9%. Only four incidents (8.5%) targeted government military actors, as depicted in Graph 2 (Mueller *et al*., 2023).

Graph 2 — Ukrainian actors targeted by Russian attacks



Source: Lewis, 2022.

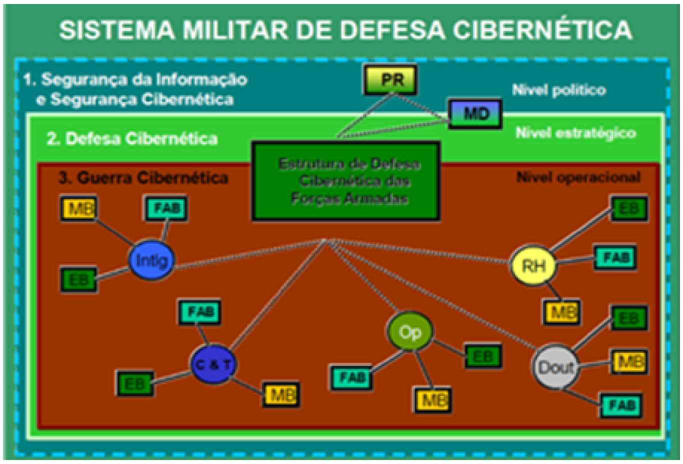
The results raise questions regarding the degree to which Russia has effectively integrated its conventional military operations with cyber effects. The coordination with conventional forces has become a focal point of discussion, with a considerable portion of the media aligning with some analysts in claiming significant coordination between cyber operations and conventional military forces (Lewis, 2022). It seems that Russian military operations face challenges in effectively integrating combined effects, particularly across different domains.

5 LESSONS FOR THE BRAZILIAN ARMY

The publication of a new National Cybersecurity Strategy – E-Ciber, in February 2020, marks a significant achievement for Brazil. Since 2008, the National Defense Strategy (*Estratégia Nacional de Defesa* – END) has defined, three sectors of strategic importance to national defense: nuclear, space, and cyber. The Brazilian Navy is responsible for managing the nuclear program, the Brazilian Air Force oversees the geospatial program, and the Brazilian Army leads cyber defense within national territory. According to END's perspective, the Cyber Sector extends beyond Cyber Security and Defense activities; it encompasses Information and Communication Technologies (ICT) and the fundamental components of the Cyber Sector for network operations. This includes the (i) command, control, communications, computing, and intelligence (C4I) structure for the operational and administrative functioning of the Armed Forces; (ii) ICT resources; and (iii) matrix architecture, facilitating the flow of information to support decision-making processes almost in real-time (Brasil, 2020a).

In light of the lessons from the Russo-Ukrainian War, cyber security and defense emerge naturally as imperatives for safeguarding critical information infrastructures associated with national critical infrastructures. In December 2020, Brazil took a significant step by establishing the Military Cyber Defense System (*Sistema Militar de Defesa Cibernética* – SMDC), with its central body being the Cyber Defense Command (*Comando de Defesa Cibernética* – ComDCiber), an operational command permanently activated and integrated by officers and enlisted personnel from the Three Armed Forces, as illustrated in Figure 1 (Brasil, 2022c).

Figure 1 – Military Cyber Defense System



Source: Instituto Militar de Engenharia, undated.

The SMDC conducts protection, exploration, and cyber-attack actions in favor of National Defense, with several benefits to society by supporting cyber security in interagency activities formed by the Armed Forces acting cooperatively with other bodies, aiming at reconciling interests, coordinating efforts, and preventing duplication of activities, dispersion of resources, and divergence of solutions, including the protection of the country's critical infrastructures. While the Brazilian Army excels in leading the structuring of Brazilian Cyber Security and Defense, it is evident that the tactics mastered by the Armed Forces are rooted in the terrestrial domain, not in cyberspace (Brasil, 2020b).

The cyber war between Russia and Ukraine, particularly the Russian attacks on Ukrainian Critical Infrastructure, has provided valuable lessons for Brazil. These events underscore the importance of preparation and capacity building to counter cyber threats targeting the country's strategic sectors.

One key lesson is the imperative to invest in cyber defense capabilities. Thus, there is a need to develop and enhance skills in protecting energy systems, communication, transport, and other critical areas of the country. This requires a comprehensive approach involving technology, cybersecurity expertise, and adequate training for the teams involved (Harknett, 2009).

The Brazilian Army is committed to the Cyber Defense of Critical Infrastructures, recognizing the importance of addressing incidents related to cyber-attacks. However, it is crucial to emphasize the continuous need for improvement and the regular implementation of exercises and simulations. The Cyber Guardian Exercise 5.0 (*Exercício Guardião Cibernético*, EGC), based at the *Escola Superior de Defesa* in Brasília (DF), embodies a significant milestone in cyber preparedness and defense for Brazil. Held annually and considered the largest event in the Southern Hemisphere dedicated to digital defense, the EGC features dynamics and simulations designed to train critical sectors of the country against cyber-attacks. Throughout the event days, these activities not only test the ability to respond to attacks but also foster collaboration between government agencies, private companies linked to the country's Critical Infrastructure, and the academic community (Padilha, 2023).

Moreover, these simulations play a crucial role in testing and strengthening the Army's cyber readiness, allowing for the identification of gaps, improvement of cyber incident response procedures, and enhanced collaboration between the teams involved (Padilha, 2023). The land armed forces can actively contribute by guiding cyber measures, such as the implementation of intrusion and detection systems, authentication policies, data protection, and the training of employees in private companies that provide essential services to the country, including banks, energy, and telecommunications companies.

Furthermore, there is a need to invest in offensive Cybersecurity resources. The Russian cyber-attacks on Ukraine underscored the necessity for a quick and effective response capacity to this type of aggression. This underscores the critical need for Brazil to possess the capability to identify, track, and neutralize hostile actors intending to inflict harm on the nation's critical infrastructure (Buchan, 2009).

Another crucial aspect to emphasize is collaboration and engagement with international partners, as Cyber War represents a transnational threat that demands concerted efforts for effective counteraction. Seeking strategic partnerships with other nations, and sharing knowledge, technologies, and experiences can enhance Brazil's response capabilities to cyber-attacks. Furthermore, collaboration with international organizations such as NATO can provide a strategic framework for addressing this threat at a global level (Samuel; Sharma, 2012).

Additionally, it is crucial to discuss the significance of Decree No. 11,200, issued on September 15, 2022, addressing the National Critical Infrastructure Security Plan (*Plano Nacional de Segurança de Infrestruturas Críticas* – Plansic). This plan encompasses a set of measures and guidelines designed to ensure the security and resilience of critical infrastructures, thereby ensuring the uninterrupted provision of essential services to the population in the event of attacks on these infrastructures. Moreover, the mentioned decree outlines the establishment of an Integrated Critical Infrastructure Security Data System, to be managed by the Institutional Security Office of the Presidency of the Republic (*Gabinete de Segurança Institucional da Presidência da República* – GSI/SP), with the purpose of monitoring and identifying threats and vulnerabilities within these critical infrastructures (Brasil, 2022a). The plan also foresees a distribution of responsibilities between ministries for the preparation of sectoral security plans for these infrastructures:

Table 1 — Responsibilities distribution between Ministries for the preparation of sectoral security plans for critical infrastructures

PRIORITY AREA	SECTOR	MINISTERIO RESPONSABLE
Water	Dams	Ministry of Regional Development
	Urban Water Supply	
Energy	Electricity	Ministry of Mines and Energy
	Petroleum, Natural Gas and Biofuels	
Transport	By land	Ministry of Infrastructure
	By Air	
	By water	
Communication	Telecommunication	Ministry of Communications
	Broadcasting	
	Postal Services	
Finance	Finance	Ministry of Economy
Biosafety and Bioprotection	Biosafety and Bioprotection	Ministry of Health
Defense	Defense	Ministry of Defense

Source: Brasil, 2022a.

The sectoral distribution of responsibility plays a crucial role in ensuring the agility and efficiency of emergency response. With ministries assigned to specific priority areas such as energy, transport, and communications, among other strategic sectors, the clear structuring of responsibilities facilitates prompt and coordinated decision-making in the face of threats or attacks on any of the country's critical infrastructure. This responsibility organization ensures an agile and effective response, adopting appropriate measures to preserve the continuity of essential services offered to the population.

We highlight that intelligence, surveillance, and recognition are pivotal in detecting and preventing cyber-attacks. The Brazilian Army must invest in cyber intelligence resources, leveraging advanced technologies such as AI and machine learning to monitor and evaluate potential threats. The ability to anticipate attacks enables a quick and effective response to protect the country's critical infrastructure (Lee, 2012).

Furthermore, it is important to highlight the cooperation between the Army's communications sector, government institutions, and sectors of civil society, including private technology companies and academic institutions. This collaboration is essential for developing comprehensive cyber defense strategies, and ensuring a coordinated and efficient response to potential cyber-attacks (Carretero; Cruz; Sempere, 2010).

The Cyber War between Russia and Ukraine provides valuable lessons for Brazil and the world. By learning from these events and implementing rapid response measures, the Army may enhance its capabilities and preparation to deal with similar challenges in the future. This ensures Brazil's security and sovereignty, protecting its Critical Infrastructures and maintaining stability in an increasingly digital and interconnected world (Alberts; Garstka, 2000).

6 FINAL CONSIDERATIONS

A nation of extensive territorial, population, and economic dimensions, such as Brazil, which aims to enhance its global engagement, must consistently extract insights from ongoing international conflicts applicable to improving sectors of its Armed Forces. It is crucial to note that instances like Russia's conflict with Ukraine underscore the significance of cyberspace as a paramount domain for modern conflict.

Despite the presence of cybernetic branches within individual forces (in Brazil, following its National Defense Strategy, the cybernetic branch of the Army holds prominence), a parallel can be drawn with the historical consolidation of air branches from Armies and Navies into the creation of the Air Forces. There is the potential to establish a new Armed Force or a dual-purpose organization comprising specialized cyber operatives, amalgamating the cyber branches from the presently existing Individual Forces.

The structure, timelines, resources, and combat tactics explored in the fifth domain of war significantly differ from their predecessors. Examining the ongoing Russian-Ukrainian war reveals that a cyber battle unfolds over a few hours, whereas land, sea, and air battles endure for days or even weeks.

Consequently, the pursuit of insights applicable to the Brazilian Army is imperative for formulating new Cyber Defense policies, alongside a more frequent revision of the National Cyber Security Strategy. Considering its international influence and the abundance of natural resources within its territory, Brazil cannot afford to neglect its defense sector and the paramount importance of advancing capabilities in the fifth domain today.

REFERENCES

ALBERTS, D. S.; GARSTKA J. J. **Network-centric warfare**: Developing and leveraging information superiority. Washington, DC: CCRP Publications, 2000.

AMAZON. Amazon Staff. Safeguarding Ukraine's data to preserve its present and build its future. **Amazon News**, [*s. l.*], 9 jun. 2022. Disponível em: https://www.aboutamazon.com/news/aws/safeguarding-ukraines-data-to-preserve-itspresent-and-build-its-future. Acesso em: 15 maio 2023.

BRASIL. Ministério da Defesa. **Estratégia Nacional de Defesa**. Versão sob apreciação do Congresso Nacional (Lei Complementar 97/1999, art. 9o, § 3o). Brasília, DF: Ministério da Defesa. 2020a.

BRASIL. **Decreto nº 11.200, de 15 de setembro de 2022**. Aprova o Plano Nacional de Segurança das Infraestruturas Críticas. Brasília, DF: Congresso Nacional, 2022a.

BRASIL. Presidência da República. **Estratégia Nacional de Segurança Cibernética – E-Ciber**. Decreto nº 10.222. Brasília, DF: Presidência da República, 2022b.

BRASIL. Ministério da Defesa. **Sistema Militar de Defesa Cibernética entra em vigor nesta terça-feira**. Brasília, DF: Presidência da República, 2022c.

BRASIL. Ministério da Defesa. **Defesa e Segurança cibernéticas**. Rio de Janeiro, RJ; Instituto Militar de Engenharia. Disponível em: http://www.defesacibernetica.ime.eb.br/. Acesso em: 20 maio 2023.

BUCHAN, J. P. Protecting national critical infrastructure against cyber threats. **Computers & Security**, [*s. l.*], v. 28, n. 3, p. 191-198, 2009.

CARRETERO, M. M.; CRUZ, A. D.; CRUZ, J. R. Strengthening International cooperation for combating cybercrime. **Computer Law & Security Review**, Amsterdam, v. 26, n. 5, p. 501-507, 2010.

CERT-UA – COMPUTER EMERGENCY RESPONSE TEAM OF UKRAINE. Cyber attack of the Sandworm group (UAC-0082) on energy facilities of Ukraine using malware INDUSTROYER2 and CADDYWIPER. **CERT-UA**, Kyiv, 12 dez. 2022. Disponível em: https://cert.gov.ua/article/39518. Acesso em: 17 jul. 2023.

CERULUS, L. How Ukraine became a test bed for cyberweaponry. **Politico**, Bruxelles, 14 fev. 2019. Disponível em: https://www.politico.eu/article/ukraine-cyber-war-frontline-russia-malware-attacks/. Acesso em: 15 jul. 2023.

CHEREPANOV, A.; LIPOVSKY, R. Industroyer: Biggest threat to industrial control systems since Stuxnet. **We Live Security**, Bratislava, 12 jun. 2017. Disponível em: https://www.

welivesecurity.com/2017/06/12/industroyer-biggest-threat-industrial-control-systems-since-stuxnet/. Acesso em: 18 jul. 2023.

CISA – CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY. Russian State-Sponsored and criminal cyber threats to critical infrastructure. **CISA**, Washington, DC, 20 abr. 2022. Disponível em: https://www.cisa.gov/uscert/ncas/alerts/aa22-110aI. Acesso em: 3 jul. 2023.

FONSECA, L. A guerra cibernética e o conflito Rússia versus Ucrânia. **Revista de Relações Exteriores**, [*s. l.*], 24 fev. 2023. Disponível em: https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/. Acesso em: 1 abr. 2023.

GREENBERG, A. Everything We Know About Russia's Election-Hacking Playbook. **Wired**, [*s. l.*], 6 set. 2017. Disponível em: https://www.wired.com/story/russia-election-hacking-playbook/. Acesso em: 16 set. 2023.

GREENBERG, A. The Untold Story of NotPetya, the Most Devastating Cyberattack in History, **Wired**, [*s. l.*], 22 ago. 2018.

HARKNETT, M. Defending cyberspace and other metaphors. **Journal of Strategic Studies**, Oxfordshire, v. 32, n. 1, p. 5-31, 2009.

LEE, R. M. Active cyber defense: Applying Air Force doctrine for cyber operations. **Air & Space Power Journal**, [*s. l.*], v. 26, n. 6, p. 50-61, 2012.

LEWIS, J. Cyber War And Ukraine. **CSIS**, [*s. l.*], 16 jun. 2022. Disponível em: https://www.csis.org/analysis/cyber-war-and-ukraine. Acesso em: 9 maio 2023.

MCGEE-ABE, J. One year on: 10 technologies used in the war in Ukraine. **Tech Informed**, [*s. l.*], 24 fev. 2023. Disponível em: https://techinformed.com/one-year-on-10-technologies-used-in-the-war-in-ukraine/. Acesso em: 9 maio 2023.

MUELLER, G. *et al*. Cyber Operations during the Russo-Ukrainian War. **CSIS**, [*s. l.*], 13 jul. 2023. Disponível em: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war. Acesso em: 24 ago 2023.

NAKASHIMA, E. U.S. Cyber Command operation disrupted Internet access of Russian troll factory on day of 2018 midterms. **The Washington Post**, Washington, DC, 27 fev. 2019. Disponível em: https://www.washingtonpost.com/world/national-security/us-cyber-command-operation-disrupted-internet-access-of-russian-troll-factory-on-day-of-2018-midterms/2019/02/26/1827fc9e-36d6-11e9-af5b-b51b7ff322e9_story.html. Acesso em: 10 ago. 2023.

NCSC – NATIONAL CYBER SECURITY CENTER. Reckless campaign of cyber attacks by Russian military intelligence service exposed. NCSC, [*s. l.*], 3 out. 2018. Disponível em: https://www.ncsc.gov.uk/news/reckless-campaign-cyber-attacks-russian-military-intelligence-service-exposed. Acesso em: 22 jul. 2023.

PADILHA, L. Exercício do Guardião Cibernético 5.0 – Forças Armadas, órgãos públicos e empresas realizam grande treinamento. **Defesa Aérea e Naval**, Brasília, DF, 6 out. 2023. Disponível em: https://www.defesaaereanaval.com.br/ciberseguranca/exercicio-guardiao-cibernetico-5-0-forcas-armadas-orgaos-publicos-e-empresas-realizam-grande-treinamento. Acesso em: 1 dez. 2023.

PAPACHELAS, A. Building defenses for cyberwarfare. **Kathimerini**, London, 14 nov. 2022. Disponível em: https://www.ekathimerini.com/opinion/interviews/1197775/building-defenses-for-cyberwarfare/. Acesso em: 30 jul. 2023.

POIREAULT, K. Interview: Microsoft Shares Its Experience of Migrating Data in Times of Cyber Warfare. **Infosecurity**, [*s. l.*], 30 set. 2022. Disponível em: https://www.infosecurity-magazine.com/interviews/interview-microsoft-migrating-data/. Acesso em: 10 jun. 2023

SAADE, J. A. G. HermeticWiper. New Destructive Malware Used In Cyber Attacks on Ukraine. **Sentinel One**, [*s. l.*], 23 fev. 2022.

SAMUEL, C.; SHARMA, M. **Securing cyberspace**: International and Asian perspectives. Washington, DC: World Scientific Publishing, 2012.

SANGER, D.; PERLTOTH, N.; SCHMITT, E. Scope of Russian Hacking Becomes Clear: Multiple U.S. agencies were hit. **New York Times**, New York, 14 dez. 2020. Disponível em: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html. Acesso em: 2 ago. 2023.

SCHULZE, M.; KERTTUNEN, M. Cyber Operations in Russia's War against Ukraine. **SWP Comment**, [*s. l.*], abr. 2023. Disponível em: https://www.swp-berlin.org/publications/products/comments/2023C23_CyberOperations_UkraineWar.pdf. Acesso em: 7 de jun. 2023.

SEGUNDO, C. B. T. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**. Brasília, DF: Escola Superior de Guerra, 2019. Disponível em: https://repositorio.esg.br/handle/123456789/1205. Acesso em: 7 maio 2023.

SMITH, B. **Defending Ukraine**: Early Lessons from the Cyber War. Blog Microsoft, [*s. l.*], 22 jun. 2022. Disponível em: https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/. Acesso em: 21 dez. 2023.

VIASAT. KA-SAT Network cyber attack overview. **Viasat**, [*s. l.*], 30 mar. 2022. Disponível em: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. Acesso em: 15 jul. 2023.

WERNER, D. Russian invasion of Ukraine exposes cybersecurity threat to commercial satellites. **Spacenews**, [*s. l.*], 14 abr. 2023. Disponível em: https://spacenews.com/russian-invasion-of-ukraine-exposes-cybersecurity-threat-to-commercial-satellites/. Acesso em: 1 jul. 2023.

WHITEHEAD, D. E. *et al*. Ukraine cyber-induced power outage: Analysis and practical mitigation strategies. *In*: ANNUAL CONFERENCE FOR PROTECTIVE RELAY ENGINEERS (CPRE), 70., 2017, Texas. **Anais** [...]. Texas, 2017.

YIN, R. **Estudo de Caso**: Planejamento e métodos. Porto Alegre: Bookman, 2015.

ZHORA, V. The potential of Russian hackers is probably overestimated. **State Service of Special Communications and Information Protection of Ukraine**, Kiev, 16 mar. 2022. Disponível em: https://cip.gov.ua/en/news/viktor-zhora-potencial-rosiiskikh-khakeriv-imovirno-pereocinenii. Acesso em: 13 jul. 2023.

ECEME