ARTIGO DOI 10.52781/cmm.a125

A Guerra Cibernética Russo-Ucraniana: os ataques russos às Infraestruturas Críticas ucranianas e possíveis lições para o Exército Brasileiro

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

Resumo: Quais lições sobre defesa cibernética no que tange aos ataques às infraestruturas críticas podem ser retiradas do conflito entre Rússia e Ucrânia para o Exército Brasileiro? Com a evolução do uso do ciberespaço, houve um aumento significativo de ataques que visam afetar as infraestruturas críticas de um Estado. O objetivo deste trabalho é analisar quais lições que o Exército Brasileiro pode obter a partir dos ataques russos às infraestruturas críticas ucranianas. Desse modo, através da metodologia exploratória, o texto concentra-se em entender quais foram os antecedentes do conflito, quais ações estão sendo usadas pela Rússia para afetar a Ucrânia e como as ações dentro do teatro de operações podem ser relacionadas com a estratégia nacional de segurança cibernética do Brasil. Portanto, este texto aponta as mudanças na estratégia russa ligadas ao uso e à adaptação dos ataques cibernéticos às infraestruturas críticas, abordando, possíveis lições que o Exército Brasileiro pode absorver.

Palavras-Chave: guerra russo-ucraniana; infraestruturas críticas; exército brasileiro; defesa cibernética; exploratória.

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.

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

Recebido: 10 set. 2023
Aprovado: 12 dez. 2023

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

1 INTRODUÇÃO

Quais lições sobre Defesa Cibernética no que tange aos ataques às Infraestruturas Críticas podem ser retiradas do conflito entre Rússia e Ucrânia para o Exército Brasileiro? Com o avanço tecnológico e a demonstração da fragilidade do espaço cibernético, mais ataques estão ocorrendo nesse local, podendo afetar as infraestruturas críticas de um Estado, tais quais telecomunicações, energia, finanças etc. Os serviços prestados por essas infraestruturas apresentam dimensão estratégica, pois são essenciais para cidadãos, organizações e para o Estado, visto que desempenham um papel imprescindível tanto para a segurança e soberania nacional como para a integração e o desenvolvimento econômico sustentável do Estado (Segundo, 2019).

A invasão da Ucrânia pela Rússia, em 24 de fevereiro de 2022, desencadeou a crise de segurança mais importante na Europa desde a Segunda Guerra Mundial (Fonseca, 2023). Para além da Guerra Cinética tradicional, a Rússia conduziu operações cibernéticas em grande escala na Ucrânia antes e depois do início do conflito (Schulze; Kerttunen, 2023). Desde o início desse conflito, pelo menos seis grupos diferentes de *crackers* ligados ao Estado executaram cerca de 240 operações cibernéticas contra alvos civis e militares ucranianos (Cerulus, 2019).

Empregou-se um *malware* – termo amplo usado para classificar todos os tipos de *softwares* maliciosos usados para causar danos – em conjunto com ferramentas maliciosas e táticas sofisticadas de *hacking* em detrimento das infraestruturas públicas. Os grupos de *Advanced Persistent Threat* (APT) ligados às agências de informação russas são os atores que estão presentes nessa campanha em curso. Um ciberatacante é designado como APT, quando há o ataque a uma rede ou um sistema de forma direcionada durante um longo período, com o objetivo de extrair informações sensíveis, obter acesso privilegiado ou causar danos significativos. Os ataques APT são caracterizados por sua natureza furtiva, persistência ao uso de técnicas avançadas de invasão e exploração de vulnerabilidades, bem como pela capacidade de evadir a detecção das medidas de segurança tradicionais. Normalmente, esse ator é bem treinado e frequentemente ligado a um Estado ou mesmo controlado por ele (NCSC, 2018).

Apesar da sua reputação em matéria de ciberguerra, a Rússia não conseguiu desferir ciberataques decisivos contra as infraestruturas de Tecnologias da Informação (TI) da Ucrânia. Os métodos e as ferramentas do atacante eram anteriormente eficazes, mas dessa vez o resultado foi diferente do que muitos esperavam. Para além da reduzida eficácia, o volume dos ciberataques russos foi inferior ao que os analistas em Defesa Cibernética esperavam (NCSC, 2018).

O sucesso da Ucrânia até agora na defesa contra a ofensiva cibernética russa pode ser atribuído a três elementos: os preparativos do governo nos anos anteriores à guerra, a assistência à ciberdefesa da Organização do Tratado Atlântico Norte (Otan) e dos países da União Europeia. Além disso, é válido destacar o envolvimento de empresas privadas, por exemplo, a Microsoft, a Amazon e a SpaceX, que ofereceram soluções comerciais como serviços digitais em nuvem e a Starlink – um projeto de constelação de satélites desenvolvido pela empresa privada SpaceX, que consiste em milhares de pequenos satélites em órbita baixa da Terra, formando uma rede interconectada, que forneceu infraestruturas de comunicações críticas (CISA, 2022).

Em suma, para operacionalizar esta pesquisa, foi feita uma pesquisa qualitativa. Além disso, de forma complementar, este artigo representa um estudo de caso único. Assim,

o objetivo deste trabalho é analisar quais lições o Exército Brasileiro pode obter a partir dos ataques russos às infraestruturas críticas ucranianas 2015).

2 ANTECEDENTES HISTÓRICOS EM RELAÇÃO AOS CIBERATAQUES RUSSOS

A Rússia tem recorrido sistematicamente a ciberataques contra a Ucrânia. Os *crackers*, indivíduos que invadem computadores ou sistemas computacionais com propósitos ilegais, ligados aos serviços secretos russos, têm conduzido operações de ciberofensiva na Ucrânia, pelo menos desde a anexação da Crimeia pela Rússia em 2014. Os seus alvos incluíam universidades, empresas de eletricidade, o setor bancário e outras infraestruturas críticas. Inicialmente, a Rússia pretendia causar frustração pública e enfraquecer os seus adversários políticos no sistema político ucraniano. Em alguns casos, os atacantes usaram o *malware KillDisk*, fazendo da Ucrânia um banco de ensaio para o desenvolvimento de novas armas cibernéticas (Fonseca, 2023).

A partir de 2014, o grupo hacktivista pró-russo (Greenberg, 2017) *CyberBerkut*, ligado à agência de informações militares estrangeiras do Estado-Maior General das Forças Armadas russas, conhecida como GRU, comprometeu o sistema eleitoral central ucraniano instalando um *malware BlackEnergy* no sistema para minar a confiança no processo eleitoral e causar instabilidade política (Greenberg, 2017). Além disso, no dia das eleições, o *CyberBerkut* lançou uma campanha maciça de ataques de negação de serviço (DDoS) – ataque cibernético projetado para sobrecarregar um sistema, serviço ou rede, tornando-o inacessível para usuários legítimos – para atrasar a contagem final das eleições e descredibilizar o processo eleitoral para a população. O ataque não foi bem-sucedido, uma vez que não deslegitimou o vencedor das eleições em 2014. No entanto, a contagem final dos votos foi adiada por duas horas (CISA, 2022).

Em 2015, o *Sandworm*, um grupo APT ligado ao GRU, conseguiu efetuar o primeiro ciberataque de sempre reconhecido publicamente a uma rede elétrica (NCSC, 2018). Os atacantes conseguiram obter remotamente o controle dos sistemas de controle de supervisão e de aquisição de dados (SCADA) em três empresas ucranianas de distribuição de energia e interromper o fornecimento de energia. Cerca de 225 mil pessoas ficaram sem eletricidade durante seis horas (Cisa, 2022). Assim, quase um ano após o ataque supracitado, a rede de energia ucraniana foi novamente alvo de ataques. Dessa vez, foi usado o *malware Industroyer*, também conhecido como *CrashOverride*, que é voltado para ataques cibernéticos contra sistemas de controle industrial (ICS). O *Industroyer* foi projetado para explorar vulnerabilidades específicas encontradas em protocolos de comunicação usados em sistemas de controle industrial, tal qual o protocolo *Modbus* e o protocolo IEC 61850, ele se tornou a maior ameaça aos sistemas de controle industrial desde o *Stuxnet* (Whitehead, 2017). Esse *malware* foi usado para obter remotamente o controle de interruptores e disjuntores de subestações de eletricidade, instalando uma porta traseira no sistema alvo que explorava os protocolos usados pelos sistemas de controle industrial (ICS) em toda a infraestrutura crítica. Este ciberataque afetou uma grande parte da capital da Ucrânia e foi atribuído ao grupo *Electrum APT*, que está diretamente associado ao *Sandworm* (Whitehead, 2017).

O pior incidente cibernético na Ucrânia ocorreu em 2017, quando o grupo APT russo *Telebots*, também ligado ao *Sandworm*, implantou o *malware* destrutivo *NotPetya* contra os setores financeiro e energético da Ucrânia (Cherepanov; Lipovsky, 2017). O *NotPetya* recebeu o seu

nome devido à sua semelhança com o *ransomware Petya*, que atacou no início de 2016 e extorquiu as vítimas para obter a chave para desbloquear os seus dados. Dessa vez, o *NotPetya*, independentemente da vítima pagar ou não, sabotou 10% dos computadores na Ucrânia (Cherepanov; Lipovsky, 2017). Espalhou-se por todo o setor financeiro da Ucrânia por meio de um popular programa de preparação de impostos. Embora o ataque visasse empresas dentro da Ucrânia, o *malware* ficou fora de controle e afetou empresas multinacionais em toda a Europa e nos Estados Unidos (EUA). O impacto exato na economia ucraniana não é claro, mas as perdas econômicas globais estimadas excederam os dez milhões de dólares (Greenberg, 2018).

Em 2018, o Comando Cibernético dos EUA usou o comportamento anterior da Rússia, bem como outros indicadores e avisos de que o Estado russo estava prestes a repetir os seus esforços, como justificativa para lançar uma operação preventiva contra a *Internet Research Agency*, uma empresa russa de propaganda e de operações de influência, concebida para evitar ataques durante as eleições (Nakashima, 2019). Mais recentemente, as operações russas combinaram uma mistura de espionagem sofisticada e campanhas criminosas de *malware*. Durante a maior parte de 2020, o grupo de *crackers* russos, *Cozy Bear*, explorou uma vulnerabilidade da cadeia de abastecimento no programa *SolarWinds Orion* para retirar dados e ferramentas digitais de uma extensa lista de alvos (Sanger; Perlroth; Schmitt, 2020). A operação fez soar o alarme, uma vez que nem a NSA nem grandes empresas como a Microsoft detectaram a intrusão e porque provavelmente envolveu uma combinação de inteligência humana e operações cibernéticas para inserir código malicioso profundamente nos servidores.

No dia 23 de fevereiro de 2023, véspera da invasão russa, foi lançado um ciberataque maciço usando o *malware HermeticWiper* nas máquinas do governo ucraniano e nos setores financeiros, da aviação, das TI e da energia (Greenberg, 2018). Embora não existam provas concretas que liguem os autores desse ataque à Rússia, o momento e a metodologia usada sugerem fortemente essa ligação. No dia seguinte, poucas horas depois da invasão, houve outro ciberataque significativo contra a rede *KA-SAT* da *Viasat*, amplamente usadas pelas forças armadas e pela polícia ucraniana (Saade, 2022). O ataque combinou ataques DDoS com o *malware AcidRain*, especialmente concebido contra equipamento de telecomunicações. Como resultado, a maioria dos *modems Viasat* ficou inoperacional e o serviço de Internet de banda larga para centenas de milhares de ucranianos e militares foi interrompido. Um efeito secundário desse ataque foi o fato de o *AcidRain* ter atravessado fronteiras e ter afetado outros países europeus, tal qual no caso do *NotPetya* (Saade, 2022).

O seguinte grande incidente foi registrado em abril de 2022, quando a infraestrutura energética da Ucrânia foi atacada pelo *malware Industroyer II*, o sucessor do *Industroyer*, visando especificamente subestações elétricas de alta tensão (Viasat, 2022). O *malware CaddyWiper* foi também implantado juntamente com o *Industroyer II* para apagar os vestígios do ataque. É preciso salientar que, ao contrário do seu antecessor, o *Industroyer II* foi usado como uma arma autônoma, não necessitando da intervenção de um operador remoto (CERT-UA, 2022). Trata-se de uma atualização significativa porque uma arma desse tipo poderia ser implantada numa rede empresarial e ficar inativa, à espera do momento certo para atacar. Esse comportamento gera complexidade para os profissionais de cibersegurança no desempenho de suas funções de prevenir um ataque. Exibindo assim, características consistentes com as atividades do grupo *Sandworm*, o que também foi

feito com o *Industroyer* em 2016, mas, dessa vez, não foram observados impactos diretos na disponibilidade de energia. O êxito do ataque deveu-se à resposta imediata das autoridades ucranianas de ciberdefesa, que adquiriram uma experiência significativa nos últimos anos e à assistência da Microsoft e da ESET (Zhora, 2022).

3 COOPERAÇÃO COM O SETOR PRIVADO

O governo e as forças armadas ucranianas ultrapassaram o choque inicial da invasão e enfrentaram com êxito esses ataques não cibernéticos. A Equipe de Resposta a Emergências Informáticas da Ucrânia (CERT-UA) trabalhou com empresas privadas para minimizar os efeitos da ofensiva cibernética da Rússia e manter todos os sistemas críticos em operação com o mínimo de interrupções. Uma semana antes da invasão, quando a guerra parecia iminente, o governo ucraniano ficou preocupado com a segurança dos seus dados e procurou formas de protegê-los. Até então, a lei ucraniana exigia que os dados específicos do governo e do setor público fossem armazenados em servidores localizados fisicamente no país. O governo alterou a legislação, permitindo que os dados sensíveis do governo e do setor privado fossem transferidos para servidores em nuvem fora do país (Amazon, 2022).

Nos dias e semanas seguintes, essas empresas forneceram ajuda, apoio e os meios (equipamentos de informática e centros de dados fora da Ucrânia) para a migração de dados de todos os setores da Ucrânia. A maioria dos ministérios, universidades e empresas privadas ucranianas se beneficiaram dessa colaboração (Poireault, 2022). Com efeito, a Ucrânia trocou a soberania dos dados por uma melhor Defesa Cibernética contra os ataques russos. Devido a essa estratégia, não só o governo ucraniano conseguiu funcionar corretamente até hoje, como também a população pôde continuar a ter uma vida em linha relativamente normal durante a guerra: a maior parte dos serviços públicos estavam disponíveis. Todos esses fatores tiveram um impacto significativo na moral da nação e ajudaram certamente a manter a resistência da Ucrânia à invasão (Poireault, 2022).

Outro aspecto interessante foi a cooperação do CERT-UA com empresas privadas de cibersegurança para monitorar e identificar potenciais ciberataques. Mesmo antes do ataque *Industroyer II* de 2022, investigadores da Microsoft (Poireault, 2022) e da *ESET* (Smith, 2022) monitoravam remotamente as redes na Ucrânia e efetuavam análises de dados em tempo real para identificar potenciais atividades maliciosas. Além disso, durante as operações cibernéticas da Ucrânia, foi registrada a primeira utilização confirmada de Inteligência Artificial (IA) – avanço tecnológico que permite que sistemas simulem uma inteligência similar à humana –. De acordo com o presidente da Microsoft, Brad Smith, a Ucrânia usou com êxito a IA para detectar, identificar e derrotar um ciberataque russo sem intervenção humana (Papachelas, 2022).

Por exemplo, a empresa ucraniana de IA Primer modificou o seu serviço comercial de transcrição e tradução de voz com base em IA para que pudesse processar as comunicações russas interceptadas e destacar automaticamente as informações relativas às forças ucranianas. A Ucrânia também usou um *software* avançado de reconhecimento facial e de imagem baseado em IA da Clearview AI para identificar russos falecidos através dos seus perfis nas redes sociais, a fim de notificar os seus familiares das suas mortes e transferir os seus corpos para as famílias (Mcgee-Abe, 2023).

Comunicações resilientes e seguras são essenciais para qualquer operação militar. Após o ciberataque contra a infraestrutura de comunicações por satélite da Viasat, o Exército ucraniano ficou sem comunicações por satélite. Essa situação comprometeu toda a Defesa do país, sendo assim solucionada por outra empresa privada americana, a SpaceX, que ofereceu à Ucrânia acesso gratuito aos seus serviços de Internet por satélite Starlink. A Ucrânia adotou rapidamente o serviço como substituto do sistema de comunicações militares do governo, que se encontrava comprometido, o que se revelou extremamente útil e bem-sucedido. O sistema provou também a sua resistência ao empastelamento de sinais, conforme afirmou recentemente o diretor-executivo da SpaceX, Elon Musk (Papachelas, 2022).

4 CONSIDERAÇÕES E RESULTADOS ACERCA GUERRA CIBERNÉTICA ENTRE RÚSSIA E UCRÂNIA

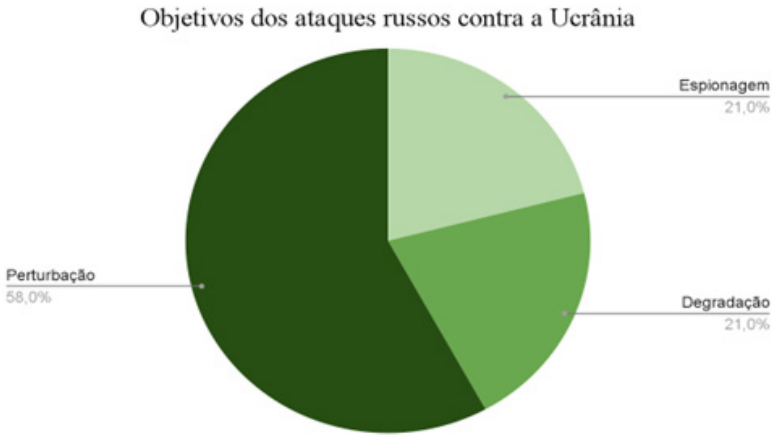
A falta de informações verificáveis sobre os ciberataques russos bem-sucedidos durante a guerra complica o cenário. É provável que a Ucrânia não revele publicamente toda a extensão dos impactos das ofensivas cibernéticas russas nas suas infraestruturas para que a Rússia não tenha uma ideia clara da eficácia das suas operações cibernéticas (Werner, 2023). Por outro lado, a Rússia poderá manter algumas das suas capacidades cibernéticas em reserva para operações futuras ou já está trabalhando numa nova ofensiva cibernética ainda não revelada. Em qualquer um dos casos, os anos de preparação da Ucrânia parecem ter dado frutos (Werner, 2023).

Os dados estão no centro da era da informação, e eventos como o ciberataque NotPetya de 2017 mostraram que o ciberespaço não respeita as fronteiras tradicionais. Os danos colaterais dos ciberataques podem ocorrer muito para além do alvo original. O *software* malicioso pode espalhar-se rapidamente pelos países e afetar dados governamentais e empresariais em todo o mundo. Os setores público e privado não podem ignorar os danos potenciais de uma crise desse tipo. Devem ser implementadas novas estratégias suscetíveis para aumentar a resistência a esse tipo de ataque. Conforme mostra o exemplo ucraniano, os benefícios da migração de dados para nuvens fora do país podem superar desvantagens como a perda de soberania dos dados e podem ser uma solução. Outro aspecto a ter em conta é o fato dos grandes centros de dados empresariais que fornecem serviços de computação em nuvem serem mais difíceis de comprometer por grupos *APT* do que os locais (Lewis, 2022).

Analisando o estilo dos ataques russos, observa-se que a atividade cibernética da Rússia durante a guerra tem sido mais perturbadora do que degradante, o que é coerente com o seu comportamento anterior. Como se pode ver no gráfico 1, quando se analisam estas operações cibernéticas por tipo, os objetivos cibernéticos preferidos da Rússia continuaram a ser as atividades de modelação perturbadoras e as campanhas de ciberespionagem. Durante os primeiros meses da sua invasão da Ucrânia em 2022, os incidentes de perturbação representaram 57,4% do total de incidentes, seguidos da espionagem, 21,3% (Mueller *et al*., 2023).

A confiança em operações disruptivas contrasta com o comportamento da Rússia antes da guerra, que acentuou a espionagem. Dito isso, tanto para a amostra do pré-guerra como para a amostra da guerra de 2022, as operações cibernéticas degradantes nunca foram a maioria (Mueller *et al*., 2023) conforme pode ser observado no Gráfico 1.

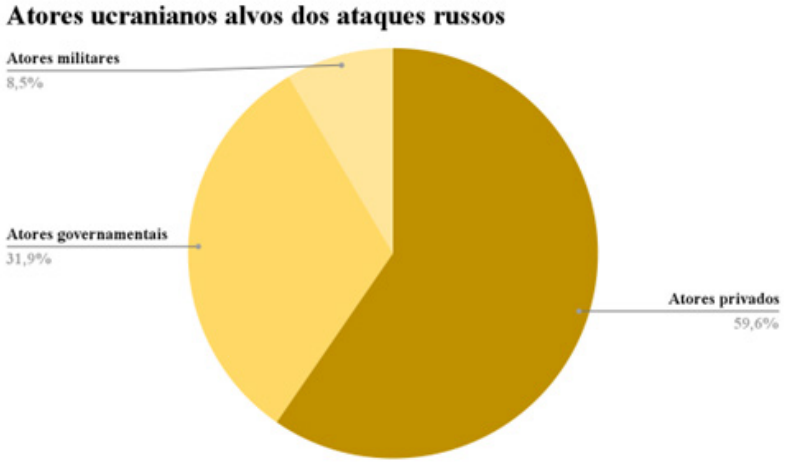
Gráfico 1 – Objetivos dos ataques russos contra a Ucrânia



Fonte: Lewis, 2022.

Olhando para os alvos de ciberataques russos no total dos 47 incidentes em 2022, a maioria (59,6%) visava atores privados não estatais, seguidos de ataques que visavam atores governamentais estatais e locais (31,9%). Apenas quatro (ou 8,5%) visaram atores militares governamentais, como pode ser observado no Gráfico 2 (Mueller *et al*., 2023).

Gráfico 2 – Atores ucranianos alvos dos ataques russos



Fonte: Lewis, 2022.

Esses resultados lançam dúvidas sobre a medida em que a Rússia conseguiu integrar com êxito as suas operações militares convencionais nos efeitos cibernéticos. A coordenação com as forças convencionais tornou-se um importante ponto de discussão, com um grande segmento dos meios de comunicação social a seguir alguns analistas na afirmação de que houve uma

coordenação significativa entre as ciber-operações e as forças militares convencionais (Lewis, 2022). As operações militares russas parecem ter dificuldade em integrar efeitos combinados, especialmente entre domínios.

5 LIÇÕES PARA O EXÉRCITO BRASILEIRO

A publicação de uma nova Estratégia Nacional de Segurança Cibernética – E-Ciber, em fevereiro de 2020, é uma importante conquista para o Brasil. A Estratégia Nacional de Defesa (END) define, desde 2008, três setores de importância estratégica à defesa nacional: o nuclear, o espacial e o cibernético, cabendo à Marinha do Brasil a gerência do programa nuclear; à Força Aérea Brasileira, o programa geoespacial; e, ao Exército Brasileiro, a liderança da defesa cibernética em território nacional. Verifica-se que o Setor Cibernético, na visão da END, não se restringe às atividades de Segurança e Defesa Cibernética, pois inclui, também, as Tecnologias de Informação e comunicação (TIC) e os componentes básicos do Setor Cibernético à atuação em rede: (i) estrutura de comando, controle, comunicações, computação e inteligência (C4I) para atuação operacional e funcionamento administrativo das Forças Armadas; (ii) recursos de TIC; e (iii) arquitetura matricial, que viabiliza trânsito de informações em apoio ao processo decisório, em tempo quase real (Brasil, 2020a).

Diante das lições da Guerra Russo-Ucraniana, a segurança e a defesa cibernéticas surgem naturalmente como imperativos de proteção das infraestruturas críticas da informação, associadas às infraestruturas críticas nacionais. Em dezembro de 2020, o Brasil deu grande passo ao criar o Sistema Militar de Defesa Cibernética (SMDC), que tem como órgão central o Comando de Defesa Cibernética (ComDCiber), um comando operacional permanentemente ativado e integrado por oficiais e praças das Três Forças Armadas, conforme na Figura 1 (Brasil, 2022c).

Figura 1 – Sistema militar de Defesa Cibernética

Fonte: Instituto Militar de Engenharia, sem ano.

O SMDC conduz ações de proteção, exploração e ataques cibernéticos em prol da Defesa Nacional, com diversos benefícios à sociedade, em apoio à segurança cibernética em atividades

interagências que se forma na atuação das Forças Armadas de forma cooperativa com outros órgãos, conciliando assim, interesses e coordenando esforços, no intuito de evitar a duplicidade de atividades, a dispersão de recursos e a divergência de soluções, incluindo a proteção de infraestruturas críticas do País. Embora o Exército Brasileiro faça um excepcional trabalho ao liderar a estruturação de Segurança e Defesa Cibernéticas brasileiras, é evidente que as táticas que as Forças Armadas dominam são baseadas no domínio terrestre, e não no ciberespaço (Brasil, 2020b).

A guerra cibernética entre Rússia e Ucrânia, especificamente os ataques russos à Infraestrutura Crítica ucraniana, ofereceu uma série de lições valiosas para o Brasil, esses eventos destacam a importância da preparação e capacitação para enfrentar ameaças cibernéticas direcionadas a setores estratégicos do país.

Uma das principais lições é a necessidade de investir em capacidades de ciberdefesa. Havendo, assim, a necessidade de desenvolver e aprimorar suas habilidades na proteção de sistemas de energia, comunicação, transporte e outras áreas estratégicas do país. Isso requer uma abordagem abrangente que envolva tecnologia tecnológica, especialização em cibersegurança e treinamento adequado para suas equipes (Harknett, 2009).

O Exército Brasileiro tem se empenhado na Defesa Cibernética de Infraestruturas Críticas, reconhecendo a importância de enfrentar os incidentes relacionados a ataques cibernéticos. No entanto, é fundamental destacar a necessidade contínua de aprimoramento e implementação regular de exercícios e simulações, o Exercício Guardião Cibernético 5.0 (EGC), sediado na Escola Superior de Defesa, em Brasília (DF), representa um marco significativo na preparação e defesa cibernética do Brasil. Realizado anualmente e considerado o maior evento do Hemisfério Sul dedicado à defesa digital, ao longo dos dias de evento, o EGC apresenta dinâmicas e simulações desenhadas para treinar setores críticos do país contra ataques cibernéticos. Essas atividades não só testam a capacidade de resposta contra esses ataques, mas também promovem a colaboração entre agências governamentais, empresas privadas ligadas às Infraestrutura Críticas do país e a comunidade acadêmica (Padilha, 2023).

Além disso, desempenham um papel crucial ao testar e fortalecer a prontidão cibernética do Exército, permitindo identificar lacunas, aperfeiçoar procedimentos de respostas a incidentes cibernéticos e aprimorar a colaboração entre as equipes envolvidas (Padilha, 2023). A força armada terrestre pode desempenhar um papel ativo em fornecer um orientações sobre medidas cibernéticas, como a implementação de sistema de detecção e intrusão, políticas de autenticação, proteção de dados e treinamento de funcionários de empresas privadas que fornecem serviços essenciais para o país, tais quais bancos, empresas energéticas e telecomunicações.

Além disso, é fundamental investir em recursos ofensivos de Segurança Cibernética. Os ciberataques russos à Ucrânia exigiram uma capacidade de resposta rápida e eficaz a esse tipo de agressão. Demonstrando para o Brasil a relevância de ter a capacidade de identificar, rastrear e neutralizar atores hostis que buscam prejudicar a infraestrutura crítica do país (Buchan, 2009).

Outro ponto a ser destacado é a cooperação e intercâmbio com parceiros internacionais, pois, a Guerra Cibernética é uma ameaça transnacional que requer esforços definidos para combatê-la. Devendo assim, buscar parcerias estratégicas com outras nações, compartilhando conhecimentos, tecnologias e experiências para fortalecer os recursos de resposta a ataques cibernéticos para o Brasil. Além disso, a colaboração com organizações internacionais, como a Otan, pode fornecer um quadro estratégico para lidar com essa ameaça a nível global (Samuel; Sharma, 2012).

Outrossim, precisamos discorrer sobre a importância do decreto nº 11.200, datado de 15 de setembro de 2022, que versa sobre o Plano Nacional de Segurança de Infraestruturas Críticas (Plansic), que é uma iniciativa de extrema relevância para o país. Esse plano consiste em uma série de medidas e orientações que visam garantir a segurança e resiliência das infraestruturas críticas, assegurando uma continuidade dos serviços essenciais oferecidos à população em caso de ataques a essas infraestruturas. Além disso, o decreto supracitado prevê a criação de um Sistema Integrado de Dados de Segurança de Infraestruturas Críticas, que será gerido pelo Gabinete de Segurança Institucional da Presidência da República (GSI/SP), com a finalidade de monitorar e identificar ameaças e vulnerabilidades nessas infraestruturas (Brasil, 2022a). O plano, ainda, prevê uma distribuição das responsabilidades entre ministérios para elaboração de planos setoriais de segurança a essas infraestruturas:

Tabela 1 – Distribuição das responsabilidades entre os Ministérios para a elaboração dos planos setoriais de segurança das infraestruturas críticas

ÁREA PRIORITÁRIA	SETOR	MINISTÉRIO RESPONSÁVEL
Águas	Barragens	Ministério do Desenvolvimento Regional
	Abastecimento Urbano de Águas	
Energia	Energia Elétrica	Ministério de Minas e Energia
	Peganbio	
Transporte	Terrestre	Ministério da Infraestrutura
	Aéreo	
	Aquaviário	
Comunicações	Telecomunicações	Ministério das Comunicações
	Radiodifusão	
	Serviços Postais	
Finanças	Finanças	Ministério da Economia
Biossegurança e Bioproteção	Biossegurança e Bioproteção	Ministério da Saúde
Defesa	Defesa	Ministério da Defesa

Fonte: Brasil, 2022a.

A distribuição setorial de responsabilidade desempenha papel crucial na agilidade e eficiência da resposta em emergências. Com ministérios designados para áreas prioritárias específicas, como energia, transportes, comunicações, entre outros setores estratégicos, a estruturação clara das responsabilidades facilita a tomada de decisões rápidas e coordenadas em caso de ameaças ou ataques a alguma infraestrutura crítica do país. Essa divisão de responsabilidade proporciona uma resposta ágil e efetiva, assegurando que medidas adequadas sejam adotadas para preservar a continuidade dos serviços essenciais oferecidos à população.

Outro ponto que merece destaque é a inteligência, vigilância e reconhecimento cumprem um papel crucial na detecção e prevenção de ataques cibernéticos. O Exército Brasileiro deve investir em recursos de inteligência cibernética, usando tecnologias avançadas, por exemplo, a IA e a aprendizagem de máquina para monitorar e avaliar possíveis ameaças. Essa capacidade de antecipar ataques permitirá uma resposta rápida e eficaz para proteger a infraestrutura crítica do país (Lee, 2012).

Por fim, é importante ressaltar a cooperação entre o setor de comunicações do Exército, instituições governamentais e setores da sociedade civil, como empresas privadas de tecnologia e instituições acadêmicas, para desenvolver estratégias abrangentes de defesa cibernética. Essa colaboração permitirá uma resposta coordenada e eficiente a ataques cibernéticos em potencial (Carretero; Cruz; Sempere, 2010).

A Guerra Cibernética entre Rússia e Ucrânia fornece lições valiosas para o Brasil e para o mundo. Ao aprender com esses eventos e implementar medidas de resposta rápida, o Exército pode fortalecer suas capacidades de estar preparado para enfrentar desafios semelhantes no futuro. Isso garantirá a segurança e soberania do Brasil, protegendo suas Infraestruturas Críticas e mantendo a estabilidade em um mundo cada vez mais digital e interconectado (Alberts; Garstka, 2000).

6 CONSIDERAÇÕES FINAIS

Um país de grandes proporções territoriais, populacionais e econômicas, como o Brasil, que busca uma crescente inserção internacional, deve constantemente buscar lições a partir de conflitos internacionais em curso aplicáveis à melhoria dos setores de suas Forças Armadas, tendo em vista que o caso da guerra da Rússia na Ucrânia, por exemplo, demonstra que a relevância de espaço cibernético sendo um dos meios mais importantes de condução de um conflito na atualidade.

Apesar da existência dos ramos cibernéticos nas forças singulares (no Brasil, pela END, predomina o ramo cibernético do Exército), a exemplo do que ocorreu com os antigos ramos aéreos dos Exércitos e da Marinhas, que foram unidos para a criação das Forças Aéreas, há uma possibilidade da construção de uma nova Força Armada, ou organização de emprego dual, composta por cibercombatentes especializados, advindos da junção dos ramos cibernéticos das Forças Singulares hoje existentes.

Afinal, a organização, os tempos, os meios e as táticas de combate exploradas no quinto domínio da guerra são bem distintos dos anteriores. Observa-se o que ocorre na guerra russo-ucraniana, em que uma batalha cibernética dura poucas horas, enquanto batalhas terrestres, marítimas e aéreas duram dias ou semanas.

Logo, a busca por lições aplicáveis ao Exército Brasileiro é imprescindível para o desenvolvimento de novas políticas de Defesa Cibernética além de uma atualização mais frequente da Estratégia Nacional de Segurança Cibernética, pois o Brasil, levando em consideração suas potencialidades internacionais e a quantidade de recursos naturais integrados ao território, não pode negligenciar seu segmento de defesa e a importância do desenvolvimento do quinto domínio na atualidade.

REFERÊNCIAS

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