UNIVERSIDADE ESTADUAL DA PARAÍBA
CENTRO DE CIÊNCIAS BIOLÓGICAS E SOCIAIS APLICADAS
DEPARTAMENTO DE RELAÇÕES INTERNACIONAIS
CURSO DE RELAÇÕES INTERNACIONAIS

RACHEL CAMILLY SOARES DE SOUZA

A GUERRA CIBERNÉTICA RUSSO-UCRANIANA: UMA ANÁLISE DOS ATAQUES CIBERNÉTICOS RUSSOS CONTRA AS INFRAESTRUTURAS CRÍTICAS UCRANIANAS

JOÃO PESSOA
2024

RACHEL CAMILLY SOARES DE SOUZA

A GUERRA CIBERNÉTICA RUSSO-UCRANIANA: UMA ANÁLISE DOS ATAQUES CIBERNÉTICOS RUSSOS CONTRA AS INFRAESTRUTURAS CRÍTICAS UCRANIANAS

Trabalho de Conclusão de Curso (Artigo) apresentado ao Programa de Graduação em Relações Internacionais da Universidade Estadual da Paraíba, como requisito parcial à obtenção do título de graduado em Relações Internacionais.

Área de concentração: Segurança Cibernética, Defesa Cibernética e Relações Internacionais.

Orientador: Prof. Dr. Fábio Rodrigo Ferreira Nobre.

Coorientadora: Profa. Dra. Thays Felipe David de Oliveira.

JOÃO PESSOA
2024

S729g Souza, Rachel Camilly Soares de.

A guerra cibernética Russo-Ucraniana [manuscrito] : uma análise dos ataques cibernéticos russos contra as infraestruturas Ucranianas / Rachel Camilly Soares de Souza. - 2024.

37 p. : il. colorido.

Digitado.

Trabalho de Conclusão de Curso (Graduação em Relações Internacionais) - Universidade Estadual da Paraíba, Centro de Ciências Biológicas e Sociais Aplicadas, 2024.

"Orientação : Prof. Dr. Fábio Rodrigo Ferreira Nobre, Coordenação do Curso de Relações Internacionais - CCBSA. "

"Coorientação: Profa. Dra. Thays Felipe David de Oliveira , UFPB - Universidade Federal da Paraíba "

1. Guerra Russo-ucraniana. 2. Defesa Cibernética. 3. Infraestruturas Críticas. I. Título

21. ed. CDD 327.16

Elaborada por Danielle H. da S. Moreno - CRB - 15/042 BSEAD/UEPB

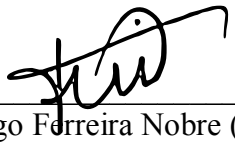
RACHEL CAMILLY SOARES DE SOUZA

A GUERRA CIBERNÉTICA RUSSO-UCRANIANA: UMA ANÁLISE DOS ATAQUES CIBERNÉTICOS RUSSOS CONTRA AS INFRAESTRUTURAS CRÍTICAS UCRANIANAS

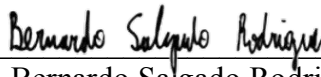
Trabalho de Conclusão de Curso apresentado ao Curso de Relações Internacionais da Universidade Estadual da Paraíba como requisito parcial à obtenção do título de bacharel em Relações Internacionais.

Aprovado em: 13 03 2024.

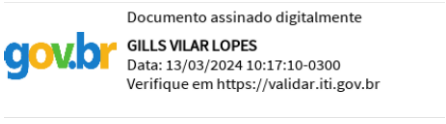
BANCA EXAMINADORA



Fábio Rodrigo Ferreira Nobre (Orientador)
Universidade Estadual da Paraíba (UEPB)



Bernardo Salgado Rodrigues
Universidade Estadual da Paraíba (UEPB)



Gills Vilar Lopes
Universidade da Força Aérea (UNIFA)

Dedico este trabalho aos meus avós maternos, Coronel Jodelmir Pereira de Souza e Eunice Maria Soares de Souza (*in memoriam*). Obrigada por sempre me apoiarem fazendo o possível e o impossível para que eu pudesse alcançar meus sonhos. Minha gratidão eterna aos senhores.

LISTA DE GRÁFICOS

LISTA DE SIGLAS E ABREVIATURAS

APT - *Advanced persistent threat*

CERT-UA - *Computer Emergency Response Team of Ukraine*

C3I - Comando, Comunicação, Controle e Inteligência

DDoS - Ataque de negação de serviço distribuída

EUA - Estados Unidos da América

EPCIP - Programa Europeu de Proteção das Infraestruturas Críticas

IC - Infraestruturas Críticas

ICT - Tecnologias de Informação e Comunicação

ISPs - Provedores de Serviços de Internet

GUAM - Organização para a Democracia e o Desenvolvimento Econômico

GRU - Departamento Central de Inteligência da Rússia.

NISAC - Centro Nacional de Proteção das Infraestruturas de Simulação e Análise de Infraestruturas

NSA - Agência de Segurança Nacional dos Estados Unidos da América

OTAN - Organização do Tratado do Atlântico Norte

SIC - Sistemas de Infraestruturas Críticas

UE - União Europeia

SUMÁRIO

A GUERRA CIBERNÉTICA RUSSO-UCRANIANA: UMA ANÁLISE DOS ATAQUES CIBERNÉTICOS RUSSOS CONTRA AS INFRAESTRUTURAS CRÍTICAS UCRANIANAS

THE RUSSIAN-UKRAINIAN CYBERWAR: AN ANALYSIS OF RUSSIAN CYBERATTACKS AGAINST UKRAINIAN CRITICAL INFRASTRUCTURE

Rachel Camilly Soares de Souza[1]

RESUMO

De que maneira a Rússia utiliza os ataques cibernéticos de forma precursora em relação aos ataques cinéticos no conflito russo-ucraniano? A Rússia e a Ucrânia têm mantido relações tensas desde 2014 durante a Guerra da Crimeia em que ataques cibernéticos contra às Infraestruturas Críticas promovidos pela Rússia já podiam ser observados buscando gerar instabilidade no sistema político ucraniano e no financeiro, que se mantiveram até a eclosão da Guerra em 24 de fevereiro de 2022. Um dia antes do início do conflito a Rússia realizou um ataque cibernético contra o satélite KA-SAT da empresa *Viasat* visando desestabilizar o Estado ucraniano gerando um aumento significativo na escalada do conflito cibernético. Com base no calendário das Guerras e dos ataques cibernéticos contra as Infraestruturas Críticas da Ucrânia, o objetivo deste trabalho é analisar os ataques cibernéticos promovidos pela Rússia contra as Infraestruturas Críticas ucranianas no teatro de operações da Guerra Cibernética entre os Estados. Desse modo, utilizando-se do metodologia qualitativa através do método exploratório sendo um estudo de caso único, o texto concentra-se em compreender o debate teórico acerca da Guerra Cibernética, apontar a visão russa e ucraniana acerca da Defesa Cibernética no que tange às Infraestruturas Críticas, descrever e analisar os ataques cibernéticos russos contra a Ucrânia. Portanto, conclui-se que a Rússia utiliza os ataques cibernéticos de forma precursora visando desestabilizar o Estado ucraniano frente aos ataques cinéticos, no entanto, estes não possuem um impacto efetivo fazendo com que a Rússia busque mudanças estratégicas no teatro de operações.

Palavras-chave: Guerra Russo-ucraniana. Defesa Cibernética. Infraestruturas Críticas.

ABSTRACT

How has Russia used cyber attacks as a precursor to kinetic attacks in the Russian-Ukrainian conflict? Russia and Ukraine have had tense relations since 2014, during the Crimean War, when Russian cyberattacks against critical infrastructure could already be observed, seeking to generate instability in the Ukrainian political and financial systems, which continued until the outbreak of the war on February 24, 2022. A day before the start of the conflict, Russia carried out a cyber-attack against the KA-SAT satellite of the Viasat company with the aim of

[1]Graduanda em Relações Internacionais pela Universidade Estadual da Paraíba (UEPB). Atualmente é integrante do Núcleo de Estudos em Processos Cibernéticos nas Relações Internacionais (NEPCRI). Área de interesse: Estudos para a Guerra e para a Paz. Subárea: Segurança Internacional, Defesa e Segurança Cibernética.

destabilizing the Ukrainian state, generating a significant increase in the escalation of the cyber-conflict. Based on the calendar of wars and cyberattacks against Ukraine's critical infrastructure, the aim of this paper is to analyze the cyberattacks carried out by Russia against Ukrainian critical infrastructure in the theater of operations of the cyberwar between states. Thus, using qualitative methodology through the exploratory method and a single case study, the text focuses on understanding the theoretical debate on Cyber Warfare, pointing out the Russian and Ukrainian vision of Cyber Defense with regard to Critical Infrastructures, pointing out and analyzing Russian cyber attacks against Ukraine. Therefore, it is concluded that Russia uses cyber attacks as a precursor to destabilize the Ukrainian state in the face of kinetic attacks, however, these do not have an effective impact, causing Russia to seek strategic changes in the theater of operations.

Keywords: Russo-Ukrainian War. Cyber Defense. Critical Infrastructures.

1 CONSIDERAÇÕES INICIAIS

A difusão e a evolução das tecnologias vêm transformando o mundo e a sociedade, tornando-os cada vez mais conectados e integrados ao ciberespaço. Perante esta realidade, as ameaças cibernéticas estão entre os maiores riscos globais de acordo com o Relatório de Riscos Globais 2022, desenvolvido pelo Fórum Econômico Mundial e os conflitos entre os países já se estenderam para a seara digital (World Economic Forum, 2022). Neste contexto, as guerras também se modificaram e ganharam novos formatos, modernas armas tecnológicas e um novo campo de batalha – o ciberespaço, ou espaço cibernético (Lobato e Kenkel, 2015). Na esfera militar, o ciberespaço foi integrado às políticas e estratégias bélicas, sendo denominado de “quinto domínio” (Teixeira Júnior, Lopes e Freitas, 2017).

A Guerra Cibernética Russo-ucraniana é o maior conflito militar da era cibernética e o primeiro a incorporar níveis tão significativos de operações cibernéticas de todos os lados. Para os acadêmicos, teóricos e profissionais do ciberconflito (e do combate em geral), esta Guerra fornece um material precioso para estudo (Willett, 2023). Em 2014, a Rússia foi acusada de bloquear o serviço da companhia telefônica Ukrtelecom na Crimeia. Em 2015, a Ucrânia foi vítima do vírus *BlackEnergy* da Rússia, que causou quedas de energia em milhares de residências e acredita-se ser o primeiro ataque bem-sucedido à rede elétrica do mundo. No dia 23 fevereiro de 2022, véspera da invasão cinética, o satélite KA-SAT da *Viasat* foi atacado deixando civis e militares sem *wi-fi* (Fonseca, 2023). Com isso, aponta-se a importância deste projeto que busca a construção de um estudo de caso pautado na Guerra Cibernética entre Rússia e Ucrânia, porque é um dos principais objetos de estudo que representam um conflito em que Guerra Cibernética e usada como um instrumento precursor através dos ataques às Infraestruturas Críticas.

Assim, o presente artigo tem como pergunta norteadora: De que maneira a Rússia utiliza os ataques cibernéticos de forma precursora em relação aos ataques cinéticos no conflito russo-ucraniano? A partir da pergunta têm-se como objetivos compreender o debate teórico acerca da Guerra Cibernética, apontar a visão russa e ucraniana acerca da Defesa Cibernética no que tange às Infraestruturas Críticas, descrever e analisar os ataques cibernéticos russos contra a Ucrânia.

Esta pesquisa apresenta um estudo exploratório visando analisar os ataques cibernéticos contra as Infraestruturas Críticas da Ucrânia entre 2022 e 2023, levando em consideração que a Guerra ainda está em processo entende-se como um estudo inicial que pode gerar pesquisas conclusivas com o fim do conflito. Ademais, quanto à natureza está pesquisa foi desenvolvida com uma Metodologia qualitativa e quantitativa, visto que nos primeiros tópicos focou-se no qualitativo trazendo uma pesquisa bibliográfica pertinente à

temática com teóricos acerca de espaço cibernético e Guerra Cibernética e no último tópico que foca na análise o método quantitativo através de gráficos visando comparar o aumento de ataques às Infraestruturas essenciais, os setores mais afetados, os tipos de ataques utilizados entre 2022 e 2023 (Marconi e Lakatos, 1996). Segundo Yin (2001), o estudo de caso é caracterizado pelo estudo profundo e exaustivo dos fatos objetos de investigação, permitindo um amplo e pormenorizado conhecimento da realidade e dos fenômenos pesquisados. Sendo assim, esta pesquisa representa um estudo de caso, pois promove uma análise do quinto domínio da Guerra tendo como recorte o conflito russo-ucraniano com recorte temporal entre fevereiro de 2022 a julho de 2023 utilizando-se fontes primárias e secundárias.

O artigo é dividido em quatro seções. A primeira aborda sobre o debate teórico que envolve os conceitos de espaço cibernético, Guerra Cibernética e Infraestruturas Críticas. Na segunda seção, é trabalhada a visão russo-ucraniana sob a perspectiva cibernética. Na terceira seção busca realizar um contexto histórico cibernético dos ataques contra às Infraestruturas Críticas ucranianas promovidos pela Rússia. Por último, busca-se analisar os ataques cibernéticos trazendo uma linha do tempo comparativa entre os ataques cinéticos e os cibernéticos buscando comprovar a hipótese que a Rússia utiliza a Guerra Cibernética como uma estratégia precursora frente a Guerra Cinética.

2 O ESPAÇO CIBERNÉTICO

No ano de 1948, Norbert Wiener[2] desenvolveu o termo *Cibernética,* buscando unir o conjunto formado pela Teoria da Comunicação e a Teoria do Controle. Com isso, a colaboração do autor tornou possível a criação de um ambiente intelectual em que o funcionamento e o controle de computadores, sistemas de comunicação e controle, comandos eletromagnéticos, transmissões eletrônicas nas máquinas de calcular e um salto de desenvolvimento surgiu. O processo de criação do termo foi o pontapé inicial para que William Gibson[3] cunhasse, em sua obra *Neuromancer* de 1982, a palavra *ciberespaço*, sendo responsável por designar uma rede de computadores, roteadores, chaves e pessoas, que estava em constante mutação.

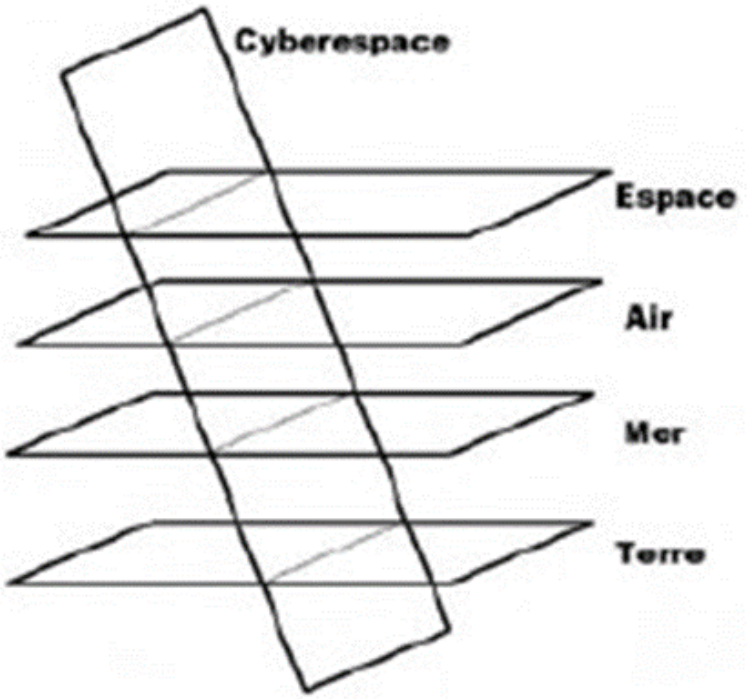
O espaço cibernético percorreu um longo caminho desde o seu nascimento como um conceito de ficção científica no início dos anos 1980. Em três décadas, ele foi definido na doutrina militar como um novo domínio de conflito e, em termos sociais mais amplos, atualmente considerado como o substrato informacional no qual crescem ecossistemas econômicos e setores inteiros. Nos países desenvolvidos, ela afeta a maioria dos aspectos da vida dos cidadãos, desde a forma como ganham dinheiro e são governados até a maneira como constroem e mantêm relações sociais e encontram sustento espiritual e intelectual (Betz e Stevens, 2011). Além disso, o espaço cibernético é compartilhado por governos, organizações, empresas e indivíduos. Nele, as decisões de alguns dos atores citados interferem nas ações dos demais (Brasil, 2012).

Os Estados e demais atores se articulam para tentarem garantir suas soberanias e seus interesses, sendo assim o espaço cibernético já passou a integrar a agenda de segurança de muitos Estados e, no meio militar, foi incorporado aos domínios da guerra: terrestre, marítimo, aéreo, espacial e cibernético (Teixeira Júnior, Lopes e Freitas, 2017). Sendo chamado de “quinto domínio” e tem, como característica, o fato de transpassar todos os demais, conforme ilustrado na Figura 1 abaixo:

Figura 1 - Dimensão transversal do ciberespaço

---

[2] WIENER, Norbert. Cybernetics. **Scientific American**, v. 179, n. 5, p. 14-19, 1948.
[3] GIBSON, William. Neuromancer (1984). In: **Crime and Media**. Routledge, 2019. p. 86-94.



Fonte: Ventre, 2012.

Para Libicki (2010), o espaço cibernético possui três camadas: a primeira camada é física, composta por *hardware*, cabos, satélites, roteadores e outros componentes infraestruturais. A segunda camada é a sintática, consistindo o código/*software* que formata, instrui e controla a informação. A terceira camada, a semântica que se refere a interface ciberespaço-humana em que a informação é dotada de significado/sentido para seres humanos. Ademais, vem tendo destaque no cenário internacional por estar se configurando como um novo campo de batalha nos conflitos entre os Estados (Bousquet, 2009).

Richard Clarke (2010), define o espaço cibernético como toda a rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles não podendo ser confundido com a conceituação de *Internet*, pois esse é o conjunto de redes menores e equipamentos conectados a ela. Assim, o conceito de espaço cibernético é mais abrangente, pois, além da *Internet*, ele também engloba todos os demais computadores não conectados e também seus equipamentos.

Sob uma perspectiva brasileira, Taquary Segundo (2019) aponta que, o espaço cibernético é um espaço virtual formado por dispositivos computacionais que podem estar conectados a uma rede ou não, no qual transitam, processam-se e armazenam-se informações, sendo necessárias para garantir o funcionamento dos sistemas. Ademais, para o autor, a natureza dinâmica do espaço é baseada na conectividade, visto que diferente dos outros domínios, que são concretos, o quinto domínio apresenta uma dimensão virtual da realidade sendo criado pelo próprio ser humano buscando atender as demandas e necessidades dos indivíduos. Portanto, o espaço cibernético não é natural como, por exemplo, os espaços terrestre e aéreo, mas um espaço criado e desenvolvido pelo ser humano. Por ser um produto da ação humana desde sua origem, o ciberespaço já surge territorializado. Essa territorialização é realizada através da rede de computadores do mundo e todas as coisas conectadas a esses aparelhos ou submetidas aos seus controles.

2.1 O Conflito Cibernético e o quinto domínio

A Guerra Cibernética refere-se à condução e à preparação para conduzir operações militares de acordo com princípios relacionados à informação, ou seja, é interromper, se não destruir, os sistemas de informação e comunicação, definidos de forma ampla para incluir até mesmo a cultura militar, nos quais o adversário se baseia para "conhecer" a si mesmo: quem é, onde está, o que pode fazer e quando, por que está lutando, quais ameaças combater primeiro etc. Significa tentar saber tudo sobre um adversário e, ao mesmo tempo, evitar que ele saiba muito sobre nós mesmos (Tzu, 2015). Sendo assim, virar o "equilíbrio de informações e conhecimento" a seu favor, especialmente se o equilíbrio de forças não estiver usando o conhecimento para que menos capital e trabalho tenham de ser gastos (Arquilla e Ronfeldt, 1993).

Nye (2012), observa que a Guerra Cibernética corresponde a uma ação hostil no ciberespaço, cujo efeito é intensificador ou semelhante à violência física. Também destaca que os Estados com recursos tecnológicos e humanos bem organizados podem destruir fisicamente alvos militares e civis por meio de ataques cibernéticos, além de causar grandes transtornos. Para o autor, o termo é utilizado buscando abranger uma ampla gama de comportamentos, refletindo as definições de guerra do dicionário que vão desde conflitos armados a qualquer concurso hostil. Contrapondo uma definição mais restrita, por exemplo, a de Rid (2011) que consiste unicamente em conflito eletrônico no espaço cibernético, no entanto, evita-se as ligações entre as camadas físicas e virtuais que pode ser desafiada pelo caso do vírus *Stuxnet*, que sabotou o programa nuclear iraniano, demonstrou, os ataques aos *software* podem ter muitos efeitos físicos reais.

Em seu artigo *The Cyber War will not take place*, 2011, Thomas Rid retoma a definição de Clausewitz (1984) acerca da Guerra como uma aplicação de força, que configure em letalidade, por meio de um ato de violência e com objetivos políticos (Rid, 2011). De acordo com o autor, ao não preencher adequadamente estes três conceitos, a Guerra Cibernética se torna uma contradição em termos. Por outro lado, John Stone (2013) adota uma visão mais abrangente de guerra em seu livro *Cyber War Will Take Place!*, apresentando uma interpretação dos conceitos de guerra de Clausewitz (1984), afirma que a guerra cibernética acontecerá, pois, um ato de violência não precisa ser letal para se configurar um ato de guerra.

Por essa linha de análise, os exemplos de conflitos cibernéticos à nossa disposição ainda são muito escassos e limitados para que possam ser analisados pela lente Clausewitziana, motivando sua exclusão da categoria “Guerra”. Para Kaldor (2013), o desenvolvimento de uma fronteira inevitável que separa as “velhas” das “novas” guerras teria sido ultrapassada, havendo assim a necessidade de nova abordagem desvencilhada de conceitos, entendimentos e métodos que foram úteis no passado.

Apesar dos debates acerca dos conceitos de Guerra Cibernética e a sua existência, aclara-se que há a ocorrência de ataques cibernéticos contra as Infraestruturas Críticas promovidos por Estados com fins políticos, econômicos e militares. A preocupação fez-se presente mediante o atual conflito entre Rússia e Ucrânia, que culminou em fevereiro de 2022 e se estende até os dias atuais, sendo caracterizada pelo grande número de ataques cibernéticos entre os países envolvidos.

Para Clarke e Knake (2012), a Guerra Cibernética é real, está acontecendo de forma rápida, além disso, é global e desafia o campo de batalha cinético que conhecemos. Sendo assim, uma penetração não autorizada, em nome ou até mesmo o apoio de um governo, podendo acontecer em um computador ou rede de outro Estado, cujo objetivo seja adicionar, alterar, falsificar dados ou causar a interrupção ou dano de um computador. Ademais, a inserção da Guerra Cibernética como temática de segurança internacional foi impulsionada por ataques cibernéticos, atribuídos à Rússia, responsáveis pelos ataques às Infraestruturas Críticas de Comunicação da Estônia, em 2007, e da Geórgia, em 2008.

O uso de ataques cibernéticos pela Rússia parece estar fortemente correlacionado e, por vezes, diretamente sincronizado com as suas operações militares cinéticas que visam serviços e instituições cruciais para os civis (Microsoft, 2022). Por exemplo, um ator russo lançou ataques cibernéticos contra uma grande empresa de radiodifusão no dia 1 de Março de 2022, o mesmo dia em que os militares russos anunciaram a sua intenção de destruir alvos de "desinformação" ucranianos e dirigiram um ataque com mísseis contra uma torre de televisão em Kiev. No dia 13 de Março de 2022, durante a terceira semana da invasão, um outro interveniente russo roubou dados de uma organização de segurança nuclear estatal chamada *Energoatom* semanas depois de unidades militares russas terem começado a capturar centrais nucleares, suscitando preocupações sobre a exposição à radiação e acidentes catastróficos (Microsoft, 2022).

Os ataques destrutivos – num número próximo de 40, visando centenas de sistemas – foram especialmente preocupantes: 32% dos ataques destrutivos tendo como alvo direto organizações governamentais ucranianas a nível nacional, regional e municipal. Mais de 40% dos ataques destrutivos visaram organizações em setores de infraestruturas críticas que poderiam ter efeitos negativos de segunda ordem sobre o governo, os militares, a economia e os civis ucranianos. Os intervenientes nestes ataques utilizam uma variedade de técnicas para obter acesso inicial aos seus alvos, incluindo *phishing*, utilização de vulnerabilidades não corrigidas e comprometimento de prestadores de serviços de TI a montante (Microsoft, 2022).

Na presente pesquisa, será utilizada a visão trazida por John Stone (2013), visto que o autor desenvolve uma análise mais ampla sobre as Guerras Cibernéticas se desprendendo dos três conceitos trazidos por Thomas Rid (2011) que limitam o entendimento acerca da guerra cibernética. Ademais, Stone (2013) traz no seu exemplo a ideia de ataques às Infraestruturas Críticas que são o foco deste trabalho no conflito cibernético entre a Rússia e a Ucrânia.

2.2 As Infraestruturas Críticas

Com o advento da sociedade da informação, em que as Tecnologias de Informação e Comunicação (ICT) têm papel preponderante nas infraestruturas de uma nação e na interação entre elas, que são consideradas críticas porque não podem sofrer solução de continuidade. Se elas param, a sociedade da informação também para, com graves consequências para a sociedade real (Mandarino Júnior, 2010). Devido às suas características, estarem acessíveis e utilizáveis pela sociedade, não cabe apenas aos indivíduos, às empresas ou ao governo protegê-las de forma individualizada e descentralizada, pois se trata de um bem comum.

Para Mandarino Júnior (2010, p. 38), as "Infraestruturas Críticas são instalações, serviços, bens e sistemas que, se forem interrompidos ou destruídos, provocarão sério impacto social, econômico, político, internacional e à segurança do Estado e da sociedade". No contexto do conflito cibernético entre Rússia e Ucrânia, em outubro de 2014, pouco antes da realização das eleições parlamentares ucranianas, um grupo hacktivista chamado pró-russo *CyberBerkut*, foi supostamente o responsável pelo ataque ao sistema eleitoral parlamentar da Ucrânia (Greenberg, 2017). Quatro dias antes da votação nacional, o sistema eleitoral central ucraniano foi comprometido e arquivos essenciais foram excluídos, tornando o sistema de contagem de votos inoperante; três dias antes da votação nacional, o *CyberBerkut* divulgou dados exfiltrados na Internet como prova do sucesso da operação. Foi instalado um *malware* que retrataria o candidato ultranacionalista Dmytro Yarosh como vencedor com 37% dos votos e o candidato Petro Poroshenko como tendo 29% dos votos (Greenberg, 2017).

Pouco depois do fechamento das urnas, o site da Comissão Eleitoral Central da Ucrânia, que organizou as eleições, foi desativado. As autoridades de segurança ucranianas caracterizaram a operação como um ataque de negação de serviço distribuído (DDoS), que pode reduzir a velocidade ou desativar uma rede inundando-a com solicitações de comunicação (Clayton, 2014). O sistema de contagem de votos foi restaurado, usando

backups, três dias antes da votação nacional. A equipe de Defesa Cibernética ucraniana conseguiu remover o *malware* 40 minutos antes da publicação dos resultados da eleição, impedindo a divulgação de resultados errôneos. Os resultados da eleição foram bloqueados por duas horas e a contagem final foi adiada. No entanto, as autoridades ucranianas anunciaram que haviam se preparado para a possibilidade de um ataque DDoS e usaram um backup para restaurar todo o sistema (Clayton, 2014).

Antes de "Infraestruturas Críticas" se tornar um termo de interesse no debate sobre terrorismo e da segurança interna, o termo "infraestrutura", aparentemente semelhante, era um assunto debatido pelos responsáveis políticos públicos. Sem uma definição padrão ou consensual, o conceito. Em termos políticos, o conceito tem sido fluido, como parece ser atualmente, incluindo sistemas públicos e privados, serviços e até comodidades. Há cerca de 20 anos, as infraestruturas foram debatidas devido à preocupação de que as infraestruturas de obras públicas do país estavam sofrendo graves problemas de deterioração, obsolescência tecnológica e capacidade insuficiente para servir o crescimento futuro (Moteff *et al*., 2003).

Ao contrário do que acontece atualmente segurança contra ataques físicos ou cibernéticos aos sistemas, o foco do debate nessa altura era a natureza, a extensão e a gravidade das más condições físicas, da e capacidade dos sistemas de obras públicas e sobre as decisões do governo a todos os níveis a todos os níveis sobre as prioridades de despesa para satisfazer as necessidades físicas e de gestão (Moteff *et al*., 2003).

A economia de uma nação e o bem-estar dos seus cidadãos dependem do funcionamento contínuo e fiável dos sistemas de infraestruturas. De acordo com o relatório da Comissão do Presidente dos Estados Unidos para a Proteção das Infraestruturas Críticas (EUA, 1997), um sistema de infraestruturas é definido como uma rede de sistemas e processos independentes, na sua maioria privados, criados pelo homem, que funcionam de forma colaborativa e sinergicamente para produzir e distribuir um fluxo contínuo de bens e serviços essenciais. Entre todos os sistemas de infraestruturas, os sistemas cuja incapacidade ou destruição teriam um impacto debilitante na defesa e na segurança econômica são considerados críticos (EUA, 1997).

A primeira definição formal sobre Infraestrutura Crítica foi desenvolvida em 1996 quando o Presidente estadunidense Clinton assinou a ordem executiva 13010, que estabelece a comissão nacional de Infraestruturas Críticas (EUA, 2017). Dessa forma, a Estratégia Nacional de Segurança Interna dos EUA considera que estes 13 setores são as Infraestruturas Críticas (EUA, 2002, p. 30), agricultura, banco e finanças, indústria química, base industrial de defesa, serviços de emergência, energia, alimentação, governo, informação e telecomunicações, correios e navegação, saúde pública, transportes e água.

Segundo Rinaldi, Peerenboom e Kelly (2001), os diferentes países têm listas ligeiramente diferentes que detalham os seus Sistemas de Infraestruturas Críticas (SIC), mas a maioria contém os seguintes sistemas: telecomunicações, sistemas de energia elétrica, gás natural e petróleo, bancos e finanças, transportes, sistemas de abastecimento de água, serviços governamentais e serviços de emergência. Os SIC não estão isolados, mas altamente interligados e mutuamente interdependentes (Rinaldi, Peerenboom, Kelly, 2001). Por exemplo, os sistemas de água e de telecomunicações necessitam de um abastecimento constante de energia elétrica para manter o seu funcionamento normal, enquanto os sistemas de energia elétrica de água e de vários serviços de telecomunicações para a geração e fornecimento de energia (Rinaldi, Peerenboom, Kelly, 2001).

As interdependências podem melhorar a eficiência operacional das infraestruturas, mas os acontecimentos mundiais como a tempestade de 1998 no Canadá, o ataque ao *World Trade Center* em 2001 o apagão norte-americano de 2003, a época de furacões de 2004 na Flórida, as inundações de 2007 no Reino Unido e os terramotos de 2010 no Chile e de 2011 no Japão 2011 no Japão mostraram que as interdependências podem aumentar a

vulnerabilidade do sistema. Os danos num SIC podem produzir falhas em cascata, provocando efeitos em cascata à escala regional ou nacional (Ouyang, 2014).

Assim, a modelização e a simulação de SIC interdependentes tornaram-se um um domínio fundamental da investigação e do estudo contemporâneos. Os governos de diferentes países também reconhecem a importância crescente dos SIC e das suas interdependências. Em 1996, o Presidente Clinton dos EUA criou a Comissão Presidencial para a Proteção das Infraestruturas Críticas (EUA, 1997). Esta comissão analisou exaustivamente e recomendou muitas políticas nacionais de proteção das IC para assegurar a continuidade das suas operações, tendo o relatório final sido publicado em outubro de 1997 (EUA, 1997).

Desde então, foram criadas e alteradas várias instituições e departamentos foram fundados e alterados para proteger os SIC nos EUA, o Centro Nacional de Proteção das Infraestruturas de Simulação e Análise de Infraestruturas (NISAC) e o Departamento de Segurança Interna (Ouyang, 2014). De igual modo, outros países e regiões também fizeram alguns esforços para proteger, tais como o Programa Europeu de Proteção das Infraestruturas Críticas (EPCIP), o Programa de Modelação e Análise de Infraestruturas Críticas na Austrália, o Programa Nacional de Garantia das Infraestruturas Críticas no Canadá, o Programa de Resiliência das Infraestruturas Críticas no Reino Unido e o Plano de Implementação da Proteção das Infraestruturas Críticas na Alemanha (Ouyang, 2014).

Com o conflito cibernético Russo-Ucraniano e os ataques russos contra às Infraestruturas Críticas ucranianas, aponta-se que estrutura institucional da Ucrânia concentra-se nas preocupações com a segurança e a defesa nacionais, em detrimento da visão da Defesa Cibernética como fundamental para o bem-estar e a prosperidade nacionais. Esse foco reflete a influência da guerra cibernética e de informações híbridas em andamento contra a Ucrânia por atores estrangeiros mal-intencionados e uma estrutura de segurança tradicionalmente rígida (USAID, 2021).

Os desafios enfrentados pela estrutura legal de Defesa Cibernética são variados e incluem aplicação fraca, funções e autoridades pouco claras entre as entidades governamentais e falta de capacidade para implementar efetivamente as leis e os regulamentos de segurança cibernética. A estrutura regulatória da Ucrânia inclui leis e regulamentações, decretos presidenciais, resoluções do Gabinete de Ministros e ordens emitidas pelas partes interessadas em Defesa Cibernética. Infelizmente, as lacunas nessa estrutura legal, as orientações contraditórias e a terminologia vaga enfraqueceram o ambiente propício para o desenvolvimento da defesa (USAID, 2021). A lei que abarca os ataques cibernéticos na Ucrânia é derivada da Constituição, da Lei de Segurança Nacional (2018), da Estratégia de Segurança Nacional (2020) e da Estratégia de Segurança Cibernética (2021).

A Estratégia de Segurança Nacional da Ucrânia define uma política externa e interna para garantir a segurança dos interesses nacionais, incluindo a Defesa Cibernética. O foco da estratégia é impedir a agressão armada, fortalecer a resiliência às ameaças à segurança nacional e envolver os principais parceiros internacionais, por exemplo, União Europeia, Estados Unidos e a Organização do Tratado do Atlântico Norte (OTAN). Ademais, a estratégia exige o estabelecimento de um sistema de segurança de Infraestruturas Críticas eficaz e resiliente com base em uma articulação clara das responsabilidades das partes interessadas, inclusive em parcerias público-privadas (USAID, 2021).

As ameaças cibernéticas à Segurança Nacional ucraniana vão muito além dos alvos militares e afetam todas as áreas da sociedade. Tanto *hackers* como governos estrangeiros são cada vez mais capazes de lançar sofisticados ataques de intrusão sobre redes e sistemas que controlam Infraestruturas Críticas. Tendo em conta a natureza integrada do ciberespaço, as falhas induzidas por meios informáticos nas redes energéticas, de transporte ou financeiras, podem provocar significativos danos físicos e rupturas econômicas no país sendo necessária uma resposta rápida e efetiva contra ataques inimigos em conflitos (Clarke e Olcott, 2012).

3 A CIBERNÉTICA SOB A ÓTICA RUSSO-UCRANIANA

A conceituação russa do *информационное пространство борства* (confronto da informação), que traz a ideia no significado de contramedida ou contra-ação, e do papel do ciberespaço no seu âmbito é delineada em documentos de política estratégica, como a Estratégia de Segurança Nacional (2015), o Conceito de Política Externa (2016), a Doutrina de Segurança da Informação (2016), a Doutrina Militar (2014), os conceitos sobre a Atividade das Forças Armadas no Espaço de Informação (2016), bem como a pesquisa de pensadores russos militares (Kukkola *et al*., 2020). Na perspetiva russa, a ciberguerra ou o equivalente russo "guerra de informação e tecnologia" é apenas uma parte do conceito abrangente de confronto de informação (*информационное пространство борства*). O Ministério da Defesa russo descreve o confronto de informações como o choque de interesses e ideias nacionais, em que a superioridade é procurada visando a infraestrutura de informação do adversário, protegendo simultaneamente os seus próprios materiais de uma influência similar (Rússia, 2011).

O confronto inclui um mandato psicológico significativo, através do qual um ator tenta afetar os recursos informacionais (documentos em sistemas de informação), bem como as mentes do pessoal militar do adversário e da população em geral (Giles, 2016). Em última análise, as operações cibernéticas (ou meios técnicos de informação) são um dos muitos métodos utilizados para ganhar superioridade no confronto de informação. A Rússia, e particularmente o regime do Presidente Vladimir Putin, vê o confronto de informação como uma competição geopolítica constante de soma zero entre grandes potências, sistemas políticos, econômicos e civilizações (Kukkola, Ristolainen e Nikkarila, 2017). À vista disso, observa-se que o aumento do uso de computadores, seus equipamentos de interconexão, sistemas de Comando, Controle, Comunicações e Informação (C3I) e sistemas de apoio à decisão que compõem o espaço cibernético se tornou fundamental nos conflitos, em decorrência da grande importância militar dos computadores e de suas redes para a circulação de ordens ou informações.

3.1 A Estratégia Nacional Cibernética da Ucrânia

Em resposta aos ataques generalizados às suas infraestruturas críticas nos últimos anos, a Ucrânia adotou uma Estratégia Nacional de Segurança Cibernética em 2016 e continua a implementá-la. A criação do Centro Nacional de Coordenação de Segurança Cibernética em 2016 e a proposta de atualização da legislação sobre crimes cibernéticos para atender aos requisitos da Convenção de Budapeste e às melhores práticas, são dois passos fundamentais para melhorar a situação cibernética no Estado. Estas atividades são complementadas por uma forte colaboração com parceiros internacionais em toda a esfera cibernética, incluindo a criminalidade cibernética e a ciberdefesa (Ucrânia, 2021; Beecroft, 2022).

A crescente digitalização dos serviços e a dependência da Internet levaram à evolução do ciberespaço, que também coloca desafios de segurança significativos aos governos de todo o mundo em relação a crimes contra e através de sistemas informáticos. Na Ucrânia, isto ficou mais evidente nos ataques cibernéticos em grande escala contra empresas de energia ucranianas, em Dezembro de 2015, após ataques aos principais canais de televisão ucranianos, dois meses antes, no dia das eleições locais (Ucrânia, 2021; Beecroft, 2022).

Estes incidentes enquadram-se numa tendência geral que a Ucrânia tem testemunhado nos últimos anos, com o aumento da utilização de ataques DDoS, bem como vulnerabilidades utilizadas para penetrar e comprometer Infraestruturas Críticas. A análise do cenário de ameaças também aponta para ataques direcionados a diplomatas, agências de aplicação da lei, agentes de defesa, empresas estatais, meios de comunicação de massa, bem como políticos e

figuras públicas, campanhas de desinformação *on-line*, dentre outros. O impacto desses ataques pode ser significativo, pois podem danificar infraestruturas essenciais e impedir o funcionamento eficaz das autoridades nacionais (Ucrânia, 2021; Spînu, 2020).

Em resposta a esses desafios, a Ucrânia adotou, por decreto presidencial, sua Estratégia Nacional de Segurança Cibernética em 15 de fevereiro de 2016. A estratégia, que está associada a um plano de ação anual para sua implementação, tem como objetivo geral criar as condições que garantam a segurança do espaço cibernético e seu uso no interesse dos indivíduos, da sociedade e do governo. O sistema nacional de cibersegurança implementado pela estratégia garante a cooperação entre todas as agências governamentais, autoridades locais, unidades militares, agências de aplicação da lei, instituições de ensino e investigação, grupos cívicos, empresas e organizações, independentemente da sua forma de propriedade, que lidam com comunicações eletrônicas. e segurança da informação ou possuir infraestrutura de informação crítica (Ucrânia, 2021; Spînu, 2020).

Um passo fundamental na implementação da Estratégia foi a criação do Centro Nacional de Coordenação de Segurança Cibernética em junho de 2016, que é um órgão de trabalho do Conselho Nacional de Segurança e Defesa. O centro tem um papel de supervisão e executa tarefas relacionadas com a análise do estado da segurança cibernética nacional e a sua preparação para combater ameaças cibernéticas, bem como a previsão e detecção de ameaças potenciais e reais relevantes. Ele também participará na organização e ministração de treinamento internacional e interdepartamental na área de segurança cibernética (Ucrânia, 2021; Spînu, 2020).

Além disso, a Ucrânia, como parte da Convenção de Budapeste sobre o Cibercrime, esforça-se pela plena implementação desta convenção. Um projeto de lei foi preparado e está atualmente em debate no Parlamento, que inclui o fortalecimento da responsabilidade pelo crime cibernético e a definição de terminologia importante e a atualização das obrigações dos Provedores de Serviços de Internet (ISPs) de acordo com a Convenção (Ucrânia, 2021).

3.2 Cooperação internacional e desenvolvimento de capacidades da Ucrânia

Ao reconhecer a necessidade de uma forte cooperação internacional e de capacitação para atender às necessidades e ameaças cibernéticas, também destacadas na nova estratégia, a Ucrânia tem colaborado com vários parceiros em todo o domínio cibernético buscando neutralizar os frequentes ataques às Infraestruturas Críticas que têm sido promovidos por grupos hacktivistas pró-russos em todo o seu território (Tkachenko, 2017; Beecroft, 2022).

A Ucrânia está trabalhando com a Defesa Cibernética da OTAN para aprimorar as capacidades técnicas do país no combate às ameaças cibernéticas. A assistência inclui a criação de um Centro de Gerenciamento de Incidentes para monitorar eventos de segurança cibernética, bem como laboratórios para investigar incidentes cibernéticos, além de treinamento para empregar essa tecnologia e esses equipamentos. Juntamente com os parceiros da OTAN, a Ucrânia realizou exercícios e treinamentos de Defesa Cibernética em que todas as partes interessadas nacionais relevantes foram treinadas sobre como reagir a grandes ataques cibernéticos as Infraestruturas Críticas (Tkachenko, 2017; Beecroft, 2022).

O Estado ucraniano não está apenas participando das iniciativas internacionais na esfera de combate às ameaças cibernéticas, mas também contribuindo para o desenvolvimento de iniciativas regionais. Com uma iniciativa liderada pela Ucrânia, foi criado um grupo de trabalho sobre Defesa Cibernética na estrutura da Organização para Democracia e Desenvolvimento Econômico (GUAM), que tem como Estados membros Azerbaijão, Geórgia, Moldávia e Ucrânia. O grupo agora está discutindo o desenvolvimento de um Memorando de Entendimento para ser adotado por seus governos, enquanto já implementou um sistema de comunicação protegido que permite, entre outras coisas, a troca segura de dados *on-line* e a realização de videoconferências (Tkachenko, 2017).

Diante disso, a experiência ucraniana dentro da Guerra Cibernética contra a Rússia demonstra que, para lidar com ameaças e ataques cibernéticos graves e persistentes, é necessário aumentar a colaboração em vários níveis, entre as autoridades nacionais, com o setor privado e com parceiros internacionais, a fim de desenvolver as capacidades necessárias, visando assim responder com eficácia a essas ameaças.

4 OS ATAQUES CIBERNÉTICOS RUSSOS CONTRA ÀS INFRAESTRUTURAS CRÍTICAS UCRANIANAS

Antes de 2014, as campanhas da Rússia tendiam a se concentrar em guerra política e espionagem. As operações na Estônia e na Geórgia foram as mais proeminentes. Operações maciças de negação de serviço (DDoS) buscaram punir a Estônia em 2007, depois que o país moveu o monumento russo conhecido como Soldado de Bronze. O monumento foi construído em 1947 como uma homenagem aos soldados do Exército Vermelho, que foram mortos em combate contra a Alemanha, apesar disso, muitos estonianos afirmam que o monumento é uma lembrança do período difícil vivido pelo país durante os quase 50 anos de ocupação soviética (Mueller *et al.*, 2013).

Durante o conflito russo-georgiano de 2008, em que *hackers* russos promoveram ataques DDoS para sobrecarregar sites e servidores da Geórgia nas semanas que antecederam a invasão militar russa. Na época, o governo da Geórgia afirmou que a Rússia estava por trás dos ataques DDoS, mas o país negou a acusação, alegando que os ataques poderiam ter sido realizados por qualquer pessoa, dentro ou de fora da Rússia (Mueller *et al*., 2013). Segundo Handler (2012), as operações de informação da Rússia visavam influenciar, interromper, corromper ou usurpar a tomada de decisões de adversários e adversários em potencial, enquanto protegiam as suas próprias.

Em um prenúncio de sua campanha militar para destruir as Infraestruturas Críticas ucranianas, a Rússia usou operações cibernéticas para atacar o fornecimento de energia da Ucrânia. Após a anexação ilegal da Crimeia em 2014, grupos de ameaças persistentes avançadas (APT), como o *Sandworm*, foram implicados na campanha *BlackEnergy* de 2015, que tinha como alvo a geração e distribuição de energia ucraniana (Symantec, 2016). No dia 23 de dezembro, a rede elétrica foi alvo de *crackers*, os mais afetados foram os consumidores da empresa *Prykarpattyaoblenergo*, que serve o distrito de Ivano-Frankivsk, tendo sido desligadas 30 subestações (7 subestações de 110 kv e 23 subestações de 35 kv) e cerca de 230.000 pessoas ficaram sem eletricidade durante um período de 1 a 6 horas (Zetter, 2016). Ao mesmo tempo, os consumidores de duas outras empresas de distribuição de energia, a *Chernivtsioblenergo* (distrito de Chernivtsi) e a *Kyivoblenergo* (distrito de Kyiv) foram também afetados por um ciberataque, mas em menor escala. Este é considerado o primeiro ciberataque bem sucedido reconhecido publicamente a uma rede elétrica (ICS-CERT, 2016).

Em outubro de 2014, um grupo hacktivista pró-russo chamado *CyberBerkut*, com supostas ligações ao grupo de hackers GRU conhecido como APT 28 (ou Fancy Bear), foi alegadamente responsável pelos ataques (Greenberg, 2017). Quatro dias antes da votação nacional, o sistema eleitoral central ucraniano foi comprometido e foram eliminados ficheiros críticos, tornando o sistema de contagem de votos inoperacional; três dias antes da votação nacional, o *CyberBerkut* divulgou na Internet dados exfiltrados como prova do êxito da operação (Greenberg, 2017; Clayton, 2014).

Foi instalado um *malware* que teria apresentado o candidato ultranacionalista Dmytro Yarosh como vencedor com 37% dos votos e o candidato Petro Poroshenko como tendo 29% dos votos. Pouco depois do encerramento das urnas, o sítio Web da Comissão Eleitoral Central da Ucrânia, que organizou as eleições, foi encerrado. As autoridades de segurança ucranianas caracterizaram a operação como um ataque distribuído de negação de serviço

(DDoS), que pode abrandar ou desativar uma rede inundando-a com pedidos de comunicação (Clayton, 2014).

O sistema de contagem de votos foi restaurado, utilizando cópias de segurança, três dias antes da votação nacional. Os funcionários ucranianos anunciaram que se tinham preparado para a possibilidade de um ataque DDoS e que tinham utilizado uma cópia de segurança para restaurar todo o sistema. Os meios de comunicação russos anunciaram que Dmytro Yarosh tinha vencido com 37% dos votos e que Petro Poroshenko tinha obtido 29% dos votos, apesar de esses resultados errôneos nunca terem sido divulgados publicamente pelas autoridades ucranianas (Clayton, 2014; Greenberg, 2017).

Nos dias 27 e 28 de junho de 2017, grupos ligados à Rússia lançaram a campanha *NotPetya*, que produziu efeitos que se espalharam dos alvos pretendidos, as empresas ucranianas, para afetar a logística global (Nakashima, 2018). O *malware NotPetya* foi propagado através de uma atualização centralizada do *software* de contabilidade fiscal *MeDoc*, utilizado por muitas empresas ucranianas. O *malware* usa o *exploit EternalBlue*, possivelmente desenvolvido pela NSA, divulgado por um grupo de *crackers* que se intitula *Shadow Brokers* e reaproveitado pelo GRU (Polityuk, 2017).

Era esperado que se propagasse apenas através de redes internas, provavelmente para ser mais direcionado; no entanto, as empresas transnacionais que tinham escritórios na Ucrânia viram as suas redes internas infetadas a nível mundial. Principalmente causando perdas econômicas a autoridades ucranianas através da encriptação irreversível dos seus dados. Estima-se que as perdas econômicas globais excedam os 10 mil milhões de dólares, além disso, o sistema de monitorização da radiação na central nuclear de Chernobyl, na Ucrânia, ficou *offline* (Auchard, Stubbs, Prentice, 2017).

Em 24 de fevereiro de 2022, o satélite *KA-SAT* da *Viasat*, amplamente utilizado pelas forças armadas e pela polícia ucraniana (Viasat, 2022), foi alvo de um ataque combinou ataques DDoS com o *malware AcidRain*, especialmente concebido contra equipamento de telecomunicações (Saade e Amerongen, 2022). Em 30 de março de 2022, a *Viasat* emitiu uma declaração sobre o ataque e afirmou que se tratava de um incidente em duas fases: (i) um ataque de negação de serviço direcionado a partir de modems e equipamento associado nas instalações do cliente localizado na Ucrânia, que deixou vários *modems offline*; e (ii) o declínio gradual dos *modems* ligados no sistema (Viasat, 2022).

A *Viasat* declarou que os atacantes exploraram uma "configuração incorreta num aparelho VPN" para obter acesso remoto a um segmento de gestão da rede terrestre e, em seguida, deslocaram-se lateralmente para um segmento utilizado para operar a rede e executaram "comandos de gestão legítimos e direcionados num grande número de modems residenciais em simultâneo", substituindo dados essenciais na memória *flash* dos *modems* (Viasat, 2022).

O ataque visava interromper o serviço, inutilizando os modems de uma parcela inteira de clientes, mas não comprometendo o satélite KA-SAT em si, nem a infraestrutura terrestre de apoio, e não havendo provas de acesso aos dados ou equipamentos pessoais dos utilizadores (Burgess, 2022). A este respeito, os peritos afirmaram que a rede da *Viasat* também fornecia serviços de comunicações às forças militares e de segurança ucranianas e que o ataque poderia ter visado atingir "aspectos do comando e controle militar na Ucrânia" (Blinken, 2022). Esta avaliação foi reiterada nas declarações dos EUA e do Reino Unido (UK, 2022), enquanto o Conselho da UE se referiu à "facilitação da ação militar" (UE, 2022).

O ataque tornou inoperacionais milhares de modems de banda larga por satélite *Viasat KA-SAT* na Ucrânia, incluindo os utilizados por militares e outras agências governamentais, causando uma grande perda de comunicação com a Internet. O ataque também afetou dezenas de milhares de clientes em toda a Europa, incluindo utilizadores de Internet por satélite da Polônia, Alemanha, Reino Unido, França e República Tcheca (Burgess, 2022). As alegadas

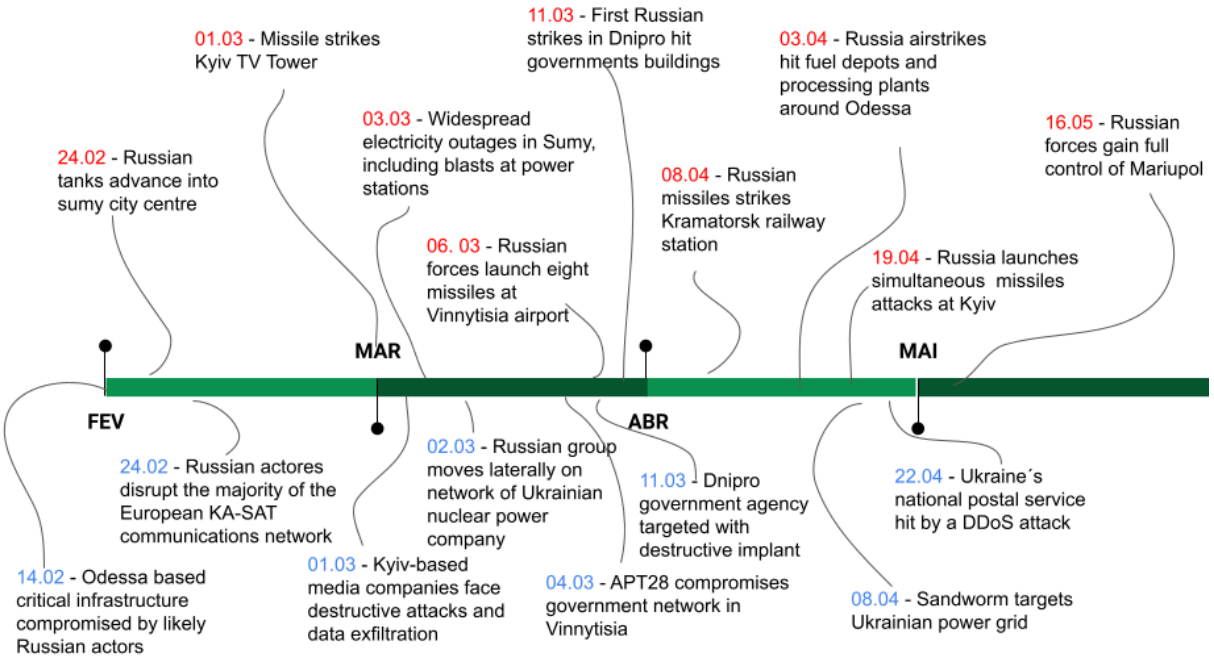
repercussões do ataque incluíram a interrupção da monitorização e controles remotos de 5.800 turbinas eólicas na Alemanha, exploradas pela Enercon, que ficaram *offline* durante várias semanas (Reuters, 2022).

Apesar disso, o ataque não comprometeu os utilizadores de outras redes da *Viasat* em todo o mundo, incluindo companhias aéreas ou outros utilizadores governamentais da rede de satélites KA-SAT, nem danificou o próprio satélite nem a infraestrutura da rede (Corera, 2022). Também não foi comunicado qualquer impacto nos componentes físicos ou elétricos dos modems e não há provas de impacto nos dados dos utilizadores nem de acesso ao equipamento pessoal dos clientes (Greig, 2022).

5 ANÁLISE DOS OBJETIVOS RUSSOS NA GUERRA CIBERNÉTICA

A Rússia não aplica uma estratégia uniforme de ataque cibernético em todos os alvos, apesar disso tem crescido na adaptabilidade e exploração das oportunidades através da vulnerabilidade dos Estados, buscando assim gerar danos e perturbações para desestabilizar um Estado alvo a partir das Infraestruturas Críticas (Pernik, 2018). Os incidentes mostrados acima, que no caso da Ucrânia aparecem desde a Guerra da Crimeia em 2014, sugerem que as operações cibernéticas têm sido usadas com um aspecto precursor, visto que a Rússia comete ataques dias ou até mesmo horas antes de um ataque cinético gerando instabilidade na Ucrânia, assim como é o caso das ações contra o satélite KA-SAT da empresa *Viasat* (Viasat, 2022). Na figura 2 abaixo pode-se observar uma linha do tempo que compara as datas entre os ataques cinéticos (em vermelho) e os cibernéticos (em azul) de fevereiro de 2022 a maio de 2022 comprovando o caráter precursor das operações cibernéticas russas visando gerar instabilidade.

Figura 2 - Linha do tempo comparativa entre os ataques cinéticos e cibernéticos entre fevereiro e maio de 2022.



Fonte: Canadian Centre for Cybersecurity, 2022

Além disso, aponta-se que o Estado russo utiliza operações cibernéticas tanto para apoiar ações militares, por exemplo no caso da Geórgia em 2008 e da Ucrânia (2014-atual), como contra adversários tradicionais e alvos de atividades de influência, por exemplo os Estados Unidos que atribui o incidente Colonial Pipeline a Rússia e a Organização do Tratado Atlântico Norte em que os *hackers* russos tiveram como alvo principalmente computadores governamentais de países membros visando gerar danos e perturbações como no caso dos ataques às Infraestruturas Críticas (Schulze e Kerttunen, 2023).

Na Guerra Cibernética Russo-ucraniana, analisa-se que a Rússia evitou uma escalada evidente ao limitar suas atividades cibernéticas à geração de efeitos atualmente considerados abaixo do limiar de desencadeamento de uma resposta armada convencional, pelo menos no caso das operações identificadas atualmente no corte temporal desta pesquisa (Mueller *et al*., 2023). Esse estilo de ataque é um paradigma ocidental de focar em operações cibernéticas ofensivas e destrutivas em Infraestruturas Críticas, cujo pico teórico trazido por Clarke e Knake (2012) muitas vezes é chamado de "*Pearl Harbor* cibernético" que seria representado por severos ataques digitais, por exemplo, a rede elétrica poderia ser desligada, a infraestrutura essencial destruída e economias inteiras paralisadas, tudo isso sem a necessidade de força militar física. Em suma, esperava-se que as operações cibernéticas alterassem o equilíbrio de poder no sistema internacional porque eram consideradas superiores à força convencional.

Entretanto, dois fatores podem alterar o cálculo estratégico da Rússia com as operações cibernéticas. O primeiro diz respeito ao seu conceito de dissuasão estratégica, segundo o qual a Rússia decidiria intensificar o uso de meios de meios informativos juntamente com outras outras ferramentas em uma tentativa de diminuir a escalada de um confronto geopolítico ou de encerrar uma uma Guerra total em termos aceitáveis para a Rússia. O segundo fator é o Estado da soberania russa na *Internet*, que, se for bem-sucedida sucesso, diminuiria significativamente a superfície de ataque da Rússia voltada para o exterior, permitindo assim que ela se envolva em medidas de escalada com menos risco de enfrentar uma retaliação efetiva (Adamsky, 2018).

Segundo o CERT-UA (2022), o setor mais frequentemente atacado por *hackers* é o público, responsável por cerca de um quarto de todos os casos estudados. Os ataques cibernéticos a empresas relacionadas com a energia diferem na complexidade de preparação e implementação, pelo que são mais difíceis de detectar. As empresas que fornecem serviços, *hardware* e *software* aos fornecedores de energia também estão sob constante olhar. Assim, os ataques através das cadeias de abastecimento continuam sendo uma fonte de ameaça crescente.

A Ucrânia tem lidado com ataques persistentes às suas Infraestruturas Críticas promovido pelo Estado russo desde 2014 que se intensificaram com a escalada do conflito em fevereiro de 2022. Foram documentados 178 incidentes cibernéticos contra organizações na Ucrânia entre janeiro e setembro de 2022, nos meses de maio e junho houve um declínio no número de ataques que gerou um aumento discrepante em julho como pode ser observado no gráfico 1 abaixo (CyberPeace Institute, 2022a):

Gráfico 1 - Número de incidentes da Ucrânia em 2022

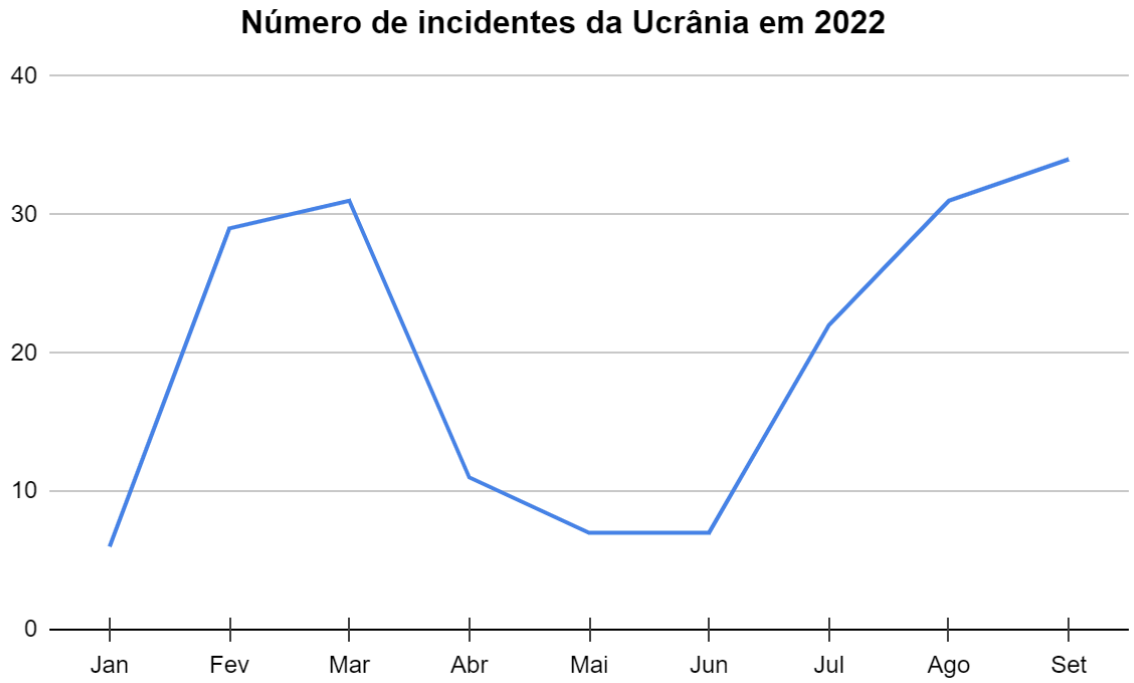


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2022a.

O aumento em julho de 2022 é representado pelas intenções russas de gerar ataques cibernéticos focados em gerar dano aos cidadãos, por exemplo o ataque a maior companhia de energia da Ucrânia, DTEK sendo esta a maior no setor privado do país (Strzelecki, 2023). Com 87 incidentes afetando 17 setores no terceiro trimestre (julho a setembro de 2022), houve um aumento de 248% nos incidentes em comparação com o trimestre anterior (abril a junho de 2022) sendo impulsionado por um aumento significativo nos ataques DDoS direcionados aos setores ucranianos. A administração pública continua sendo o setor mais visado no terceiro trimestre de 2022. Em comparação com os trimestres anteriores, houve um aumento notável nos ataques contra organizações nos setores de Mídia, Tecnologia da Informação e Comunicação, Energia e Transporte como pode ser observado no Gráfico 2 abaixo em que aponta-se os setores das Infraestruturas Críticas mais afetados (CyberPeace Institute, 2022a):

Gráfico 2 - Incidentes por setor na Ucrânia de Julho a Setembro de 2022

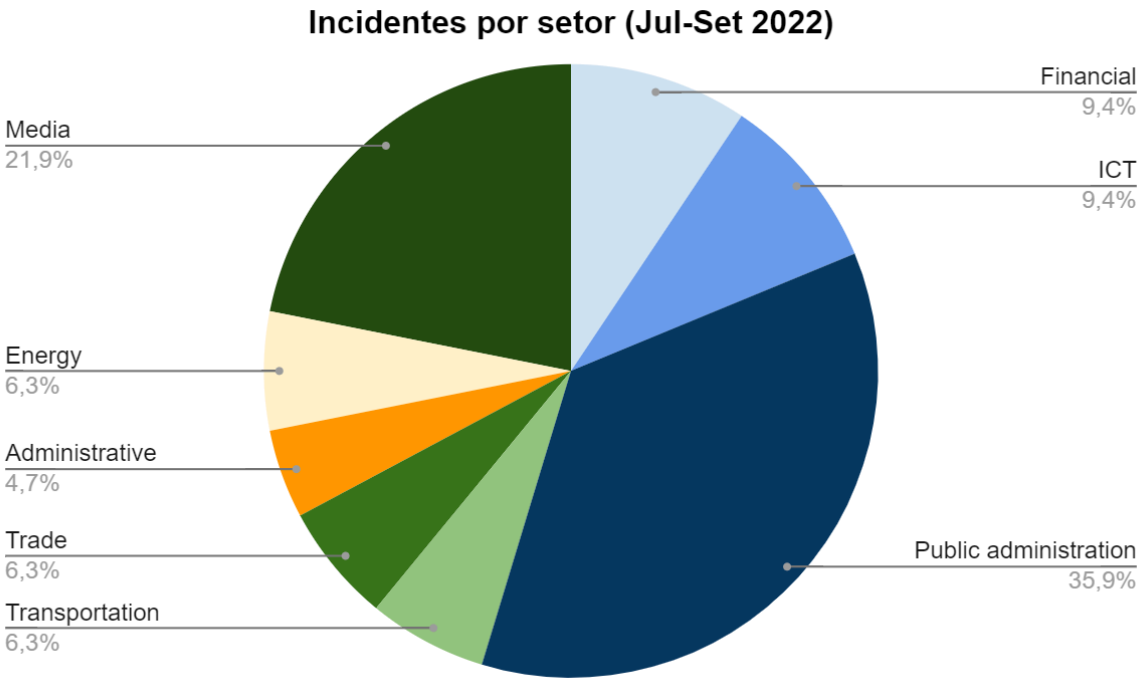


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2022a.

Ademais, os ataques DDoS são responsáveis por 71,3% de todos os incidentes, seguidos por *malware* (8%) e os grupos de hacktivistas são responsáveis por 80% de todos os incidentes. Os ataques distribuídos de negação de serviço (DDoS) envolvem um esforço coordenado para atingir a disponibilidade de serviços e recursos da Internet. Esses ataques usam técnicas semelhantes às dos ataques DoS comuns, mas em uma escala maior. Na prática, ataques DDoS fazem com que um recurso *on-line*, como um site com informações cruciais ou um portal de serviços, fique inacessível ou indisponível para os visitantes por um período de tempo durante ou após um ataque (CyberPeace Institute, 2022a).

De acordo com o relatório desenvolvido pelo Cyberspace Institute entre janeiro de 2022 e junho de 2023 foram observados 474 incidentes contra autoridades ucranianas. Com 71 incidentes que afetaram 16 setores no quarto trimestre (Outubro a Dezembro de 2022), houve uma redução de 18,4% nos incidentes em comparação com o trimestre anterior (Julho a Setembro de 2022). Essa redução é impulsionada por um declínio nos incidentes comprovados direcionados a entidades ucranianas por grupos de *hacktivistas* pró-Rússia (CyberPeace Institute, 2022b).

Os grupos *hacktivistas* são responsáveis por 91,4% de todos os incidentes direcionados a entidades governamentais na Ucrânia. O setor mais visado na Ucrânia foi o setor financeiro, que registrou um aumento de 116,7% em comparação com o terceiro trimestre que pode ser notado no gráfico 3 abaixo (CyberPeace Institute, 2022b):

Gráfico 3 - Incidentes por setor na Ucrânia entre Outubro e Dezembro de 2022

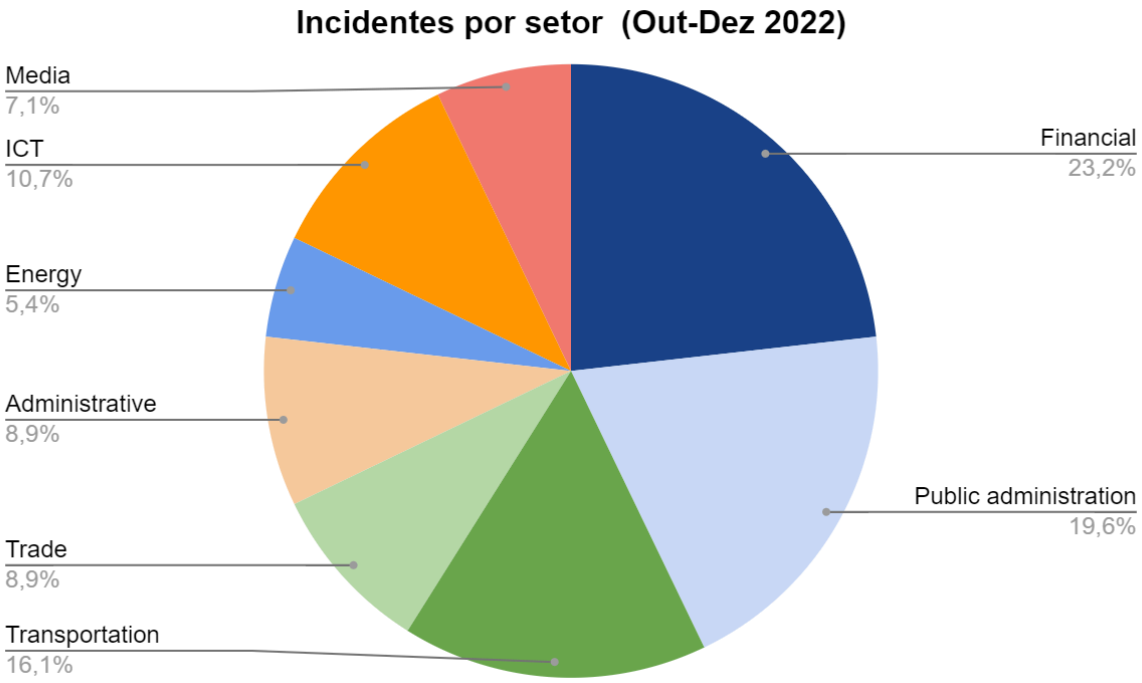


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2022b.

No primeiro trimestre de 2023 (Janeiro a Março) foram documentados 104 incidentes, gerando um aumento de 36,8% em comparação com o quarto trimestre de 2022. Os ataques tipo DDoS representaram 87,5% dos incidentes e os setores alvo foram o financeiro, o público administrativo e o Tecnologia da Informação e Comunicação (ICT) como pode ser observado no Gráfico 4 abaixo (CyberPeace Institute, 2023a):

Gráfico 4 - Incidentes por setor na Ucrânia de Janeiro a Março de 2023

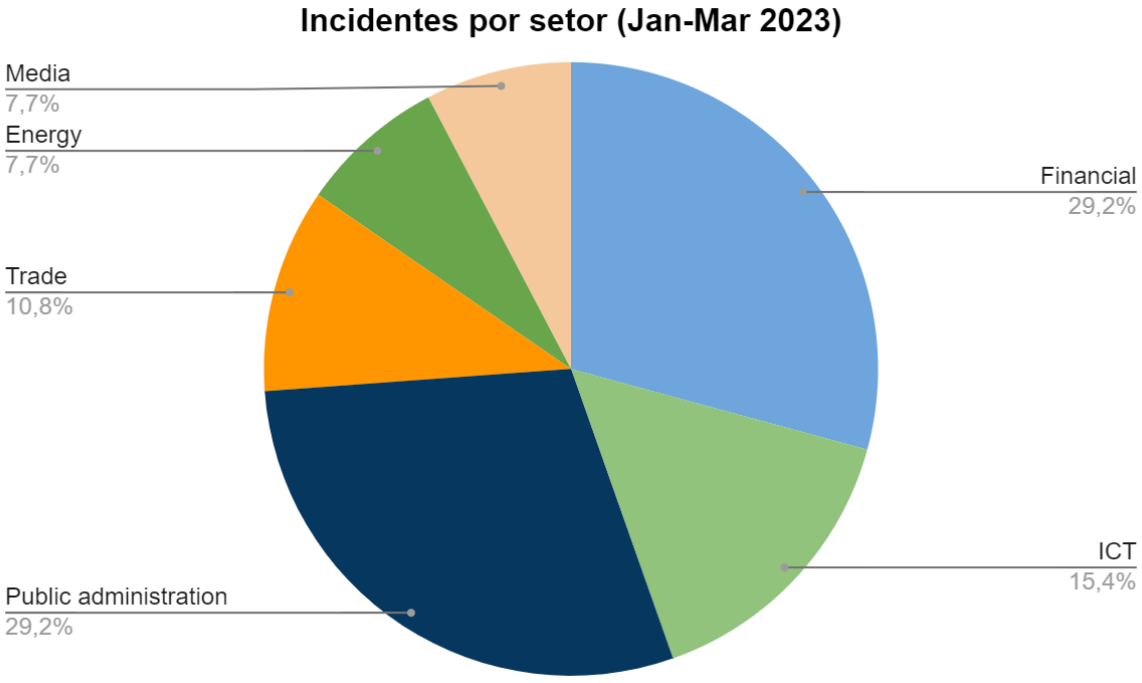


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2023a.

Entre abril e junho de 2023 observou-se que o tipo de ataque cibernético tipo DDoS representa 88,8% dos incidentes, além disso, os setores que foram mais atingidos foram o público administrativo, mídia, sistema financeiro e transportes como pode ser observado no gráfico 2 abaixo (CyberPeace Institute, 2023a):

Gráfico 5 - Incidentes por setor na Ucrânia entre Abril e Junho de 2023

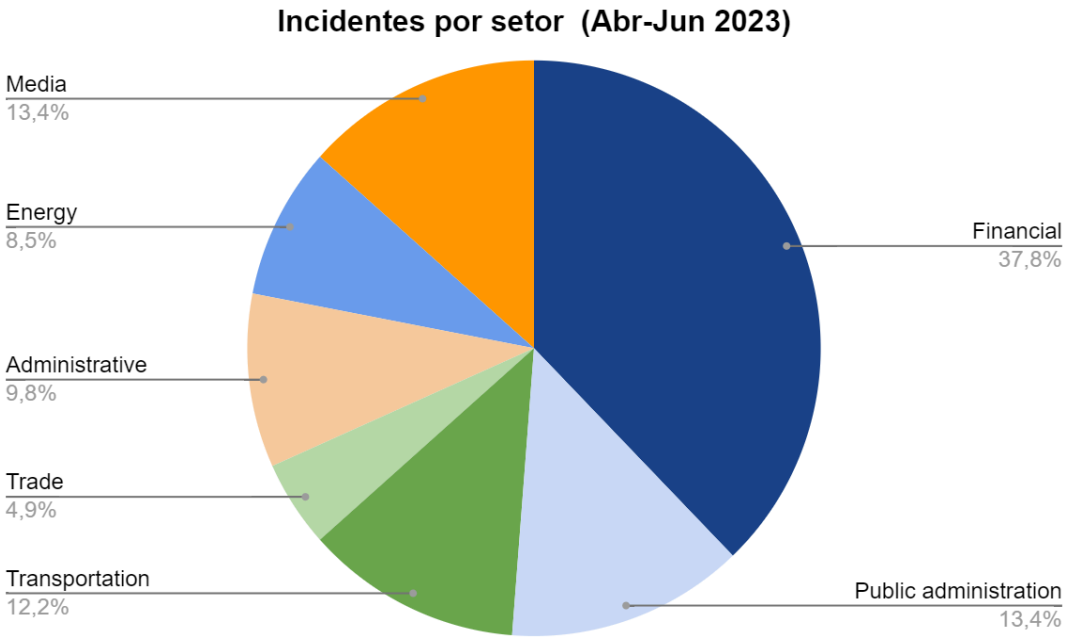


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2023b.

Comparando em análise o terceiro e quarto trimestre de 2022 (Jul-Dez) e o primeiro e segundo trimestre de 2023 (Jan-Jun) pode-se observar que o número de incidentes em 2023 teve um aumento significativo principalmente de fevereiro (CyberPeace Institute, 2023b) como pode ser observado no gráfico 6 abaixo:

Gráfico 6 - Análise do número de incidentes entre 2022 e 2023

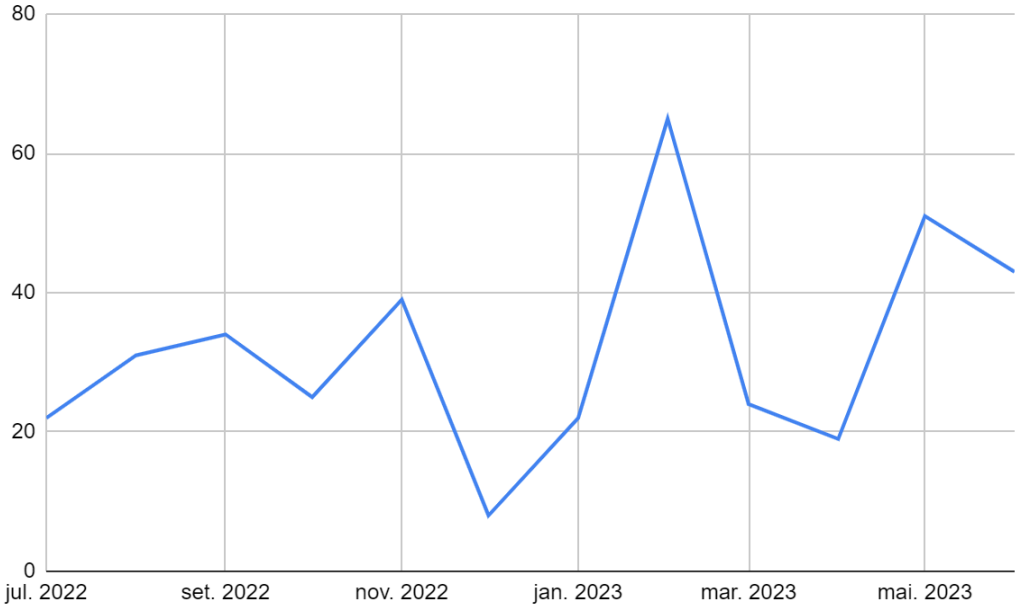


Gráfico desenvolvido pela autora de acordo com o CyberPeace Institute, 2023b.

As atividades cibernéticas russas têm se concentrado principalmente na coleta de informações, destruição de dados e ataques de negação de serviço em Infraestruturas Críticas. Surpreendentemente, graças à Defesa Cibernética proativa e à resiliência social da Ucrânia, esse tipo de guerra cibernética não produziu benefícios estratégicos, operacionais ou táticos significativos para a Rússia, pelo menos até onde sabemos publicamente (Schulze e Kerttunen, 2023).

Ainda assim, o fato de a Rússia não ter conseguido alinhar suas manobras digitais e analógicas dessa vez não significa que outros não possam aprender com essa falha e fazer o mesmo em outro conflito. No entanto, algoritmos melhores por si só não equilibrarão os pontos fracos inerentes às operações cibernéticas ofensivas: elas exigem tempo excessivo, dependem do alvo e podem simplesmente falhar contra um defensor ágil e proativo. Para a Defesa Cibernética ser bem-sucedida, ela exige flexibilidade, velocidade, visão de futuro, inteligência útil sobre ameaças e processos interministeriais simplificados para reduzir os silos de informações, além de exercícios e treinamento (Schulze e Kerttunen, 2023).

6 CONSIDERAÇÕES FINAIS

A Guerra Cibernética é responsável por gerar danos, destruição e prejuízo de sistemas que podem ultrapassar o quinto domínio gerando danos físicos e reais principalmente ataques direcionados às Infraestruturas Críticas de um Estado. Com isso, aponta-se que o avanço tecnológico e o aumento de vulnerabilidades têm exposto a Defesa Cibernética como um dos pontos de maior ameaça no cenário atual mundial, principalmente quando combinado com ataques cinéticos como no caso russo-ucraniano.

Este artigo buscou entender as diferentes visões teóricas que abordam os conceitos de espaço cibernético, Guerra Cibernética e Infraestruturas Críticas, bem como analisar a Guerra Cibernética Russo-ucraniana. Deste modo, apontou-se que o espaço cibernético se tornou um espaço para combate em que ataques podem gerar sérios danos e instabilidade para um Estado gerando um conflito do ambiente digital que pode gerar prejuízos físicos. Os ataques

cibernéticos já são aparentes desde 2014 na Guerra da Crimeia e tem apresentado um aumento com o estopim do conflito em 24 de fevereiro de 2022.

Assim, a Ucrânia buscou apoio através da cooperação com outros Estados que também sofreram com operações cibernéticas russas, tal como Geórgia, Estados Unidos, Geórgia e até mesmo a OTAN tem disponibilizado auxílio para a Ucrânia. Com o setor privado o apoio têm sido por meio de empresas como Microsoft, SpaceX e Amazon e gerando melhorias na Defesa Cibernética do país, por exemplo, a criação do Centro Nacional de Coordenação de Segurança Cibernética em junho de 2016 buscando aumentar a velocidade das respostas contra os incidentes e diminuir as vulnerabilidades.

Através da análise dos ataques cibernéticos promovidos pela Rússia o tipo DDoS tem sido o mais frequente e os setores mais prejudicados foram o financeiro, o público administrativo e o setor de Tecnologia da Informação e Comunicação. Apesar da alta frequência, a Rússia não conseguiu trazer impactos significativos na Guerra Cibernética, tendo demonstrado um desempenho abaixo do esperado e uma estratégia que demonstra a utilização da cibernética como um apoio que busca gerar a desestabilização gerando o aumento da capacidade destrutiva dos outros domínios no teatro de operações.

A hipótese do trabalho era que a Rússia utilizava a Guerra Cibernética como um instrumento precursor em relação a Guerra Cinética o que pode ser comprovado analisando a proximidade das datas entre ataques cibernéticos e cinéticos no período entre fevereiro e abril de 2022 através de uma linha do tempo que demonstra que as operações cibernéticas em torno de poucos dias antes, buscando assim, gerar instabilidade para a Ucrânia através danos às suas Infraestruturas Críticas.

A Guerra Cibernética russo-ucraniana apresenta oportunidades de pesquisa e exemplos relevantes acerca do funcionamento de uma Guerra moderna, ou seja, um conflito que utiliza ataques cinéticos e cibernéticos para a promoção de capacidades do Estado. Ademais, estes estudos podem ser utilizados para a construção de novos parâmetros e novas definições acerca das políticas de Defesa no cenário atual. A análise do conflito gera oportunidades para melhorias nos setores de Defesa e do processo de integração das forças, desenvolvendo assim, ferramentas capazes de aumentar a capacidade militar e estratégica dos Estados no setor cibernético. Levando-se em consideração que este trabalho possui um caráter exploratório e um recorte de um conflito que ainda permanece ativo, recomenda-se complementações e trabalhos com recortes temporais atualizados acerca do tema.

REFERÊNCIAS

ADAMSKY, D. From Moscow with coercion: Russian deterrence theory and strategic culture. **Journal of Strategic Studies**, v. 41, n. 1-2, p. 33-60, 2018.

ARQUILLA, John; RONFELDT, David. Cyberwar Is Coming! In: _____ (Org.). In Athena's Camp: Preparing for Conflict in the Information Age. Santa Monica: RAND, 1993.

AUCHARD, Eric; STUBBS, Jack; PRENTICE, Alessandra. New computer virus spreads from Ukraine to disrupt world business. Reuters, 27 june 2017. Disponível em: https://www.reuters.com/article/us-cyber-attack/new-computer-virus-spreads-from-ukraine-to-disrupt-world-business-idUSKBN19I1TD. Acesso em: 10 set. 2023.

BEECROFT, Nick. Evaluating the International Support to Ukrainian Cyber Defense. **Carnegie Endowment for International Peace**, 3 november 2022. Disponível em: https://carnegieendowment.org/2022/11/03/evaluating-international-support-to-ukrainian-cyber-defense-pub-88322. Acesso em: 23 out. 2023.

BETZ, David; STEVENS, Tim. Cyberspace and the State: Toward a Strategy for Cyber-Power. Londres: **IISS**, 2011.

BLINKEN, Antony. Attribution of Russia´s Malicious Cyber Activity Against Ukraine, US, **Department of State**, 10 May 2022. Disponível em: https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/. Acesso em: 12 set. 2023.

BURGUESS, Matt. A Mysterious Satellite Hack Has Victims Far Beyond Ukraine. **Wired**, 23 march 2022. Disponível em: <https://www.wired.com/story/viasat-internet-hack-ukraine-russia/>. Acesso em: 15 set. 2023.

BRASIL. Ministério da Defesa. Estratégia Nacional de Defesa - END. Brasília. 2012. Disponível em: https://www.defesa.gov.br/arquivos/2012/mes07/end.pdf. Acesso em: 20 mai. 2023.

CANADA. Cyber threat activity associated russian invasion of Ukraine. Government of Canada, 2022. Disponível em: https://www.cyber.gc.ca/sites/default/files/cyber-threat-activity-associated-russian-invasion-ukraine-e.pdf. Acesso em: 26 out. 2023.

CERT-UA, Russia's Cyber Tactics: Lessons Learned, State Service of Special Communications and Information Protection of Ukraine, 2022. Disponível em: file:///C:/Users/Marli/Downloads/Russia%E2%80%99s%20Cyber%20Tactics%20Lessons%20Learned%202022.pdf. Acesso em: 30 out. 2023.

CLARKE, Richard e KNAKE, Robert. Cyber War: The Next Threat to National Security and What To Do About It. Nova York: Ecco, 2012.

CLARKE, Richard e OLCOTT, Jacob. Confronting Cyber Risk in Critical Infrastructure: The National and Economic Benefits of Security Development Processes. **Good Harbor Consulting**, 2012.

CLAUSEWITZ, C. von; HOWARD, M.; PARET, P. (Eds.). On War. Princeton: Princeton University Press, 1984.

CLAYTON, Mark. Ukraine election narrowly avoided "wanton destruction" from hackers, CS Monitor, 2014. Disponível em: https://www.csmonitor.com/World/Passcode/2014/0617/Ukraine-election-narrowly-avoided-wanton-destruction-from-hackers. Acesso em: 16 de set. 2023.

CORERA, Gordon. Russia hacked Ukrainian satellite communications, officials believe. **BBC**, 25 march 2022. Disponível em: <https://www.bbc.com/news/technology-60796079>. Acesso em: 20 set. 2023.

CYBERPEACE INSTITUTE. Cyber Attacks in Times of Conflict Platform #Ukraine, 2022a. Disponível em: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q3%20Report.pdf. Acesso em: 22 out 2023.

CYBERPEACE INSTITUTE. Cyber Attacks in Times of Conflict Platform #Ukraine, 2022b. Disponível em: https://cyberpeaceinstitute.org/wp-content/uploads/Cyber%20Dimensions_Ukraine%20Q4%20Report.pdf. Acesso em: 24 out. 2023.

CYBERPEACE INSTITUTE. Cyber Attacks in Times of Conflict Platform #Ukraine, 2023a. Disponível em: file:///C:/Users/Marli/Downloads/Ukraine-Report-Q1_FINAL.pdf. Acesso em: 24 out. 2023.

CYBERPEACE INSTITUTE. Cyber Attacks in Times of Conflict Platform #Ukraine, 2023b. Disponível em: https://cyberpeaceinstitute.org/wp-content/uploads/2023/09/Ukraine-Report-Q2_4.09.pdf. Acesso em: 26 out. 2023.

EUA, CI Scoop: history of critical infrastructures designation. United States Election Assistance Commission, 2017.

EUA, Department of Defense Strategy for Operating in Cyberspace (DoD), 2011. Disponível em:https://csrc.nist.gov/CSRC/media/Projects/ISPAB/documents/DOD-Strategy-for-Operating-in-Cyberspace.pdf. Acesso em: 30 ago. 2023.

EUA, President 's Commission on Critical Infrastructures Protection. Critical Foundations: protecting America's infrastructures: the report of the Presidential´s Commission on Critical Infrastructures. U.S. Government Printing Office, Washington, D.C., 1997.

FONSECA, Leila. A Guerra Cibernética e o conflito Rússia versus Ucrânia. **Revista de Relações Exteriores**, 2023. Disponível em: <https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/>. Acesso em: 1 ago. 2023.

GILES, Keir. Handbook of Russian information warfare. Defense College Collège de Défense de l'OTAN, 2016. Disponível em: https://bdex.eb.mil.br/jspui/bitstream/123456789/4262/1/2016_Handbook%2c%20Russian%20Information%20Warfare.pdf. Acesso em: 27 out. 2023.

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

GREIG, Jonathan. Viasat confirms report of wiper malware used in Ukraine cyberattack. **The Record**, 31 march 2022. Disponível em: <https://therecord.media/viasat-confirms-report-of-wiper-malware-used-in-ukraine-cyberattack>. Acesso em: 22 set. 2023.

HANDLER, Stephenie Gosnell. New cyber face of battle: developing a legal approach to accommodate emerging trends in warfare. **Stan. J. Int'l L.**, v. 48, p. 209, 2012.

ICS-CERT. Cyber-Attack Against Ukrainian Critical Infrastructure. **United States Department of Homeland Security**, 20 July 2021. Disponível em: https://www.cisa.gov/news-events/ics-alerts/ir-alert-h-16-056-01. Acesso em: 1 set. 2023.

KALDOR, Mary. **New and old wars: Organised violence in a global era**. John Wiley & Sons, 2013.

KJENNERUD Erik, CULLEN Patrick. What is Hybrid Warfare? Norwegian Institute of International Affaris, n. 1, p. 1-4, 2016.

KUKKOLA, Juha *et al*. Digital Soviet Union: The Russian national segment of the Internet as a closed national network shaped by strategic cultural ideas. **Series 1: Research Publications No. 40**, 2020.

KUKKOLA, Juha, RISTOLAINEN, Mari, NIKKARILA, Juha-Pekka. Game Changer: structural transformation of cyberspace. Finnish Defence Research Agency Publications, 2017.

LIBICKI, Martin C. Cyberdeterrence and Cyber War. Santa Monica: RAND, 2010.

LOBATO, Luisa; KENKEL, Kai Michael. A Ciberguerra é moderna! Uma investigação sobre a relação entre tecnologia e modernização na guerra. **Contexto Internacional**, v. 37, p. 629-660, 2015.

MANDARINO JR, Raphael. **Segurança e defesa do espaço cibernético brasileiro**. Cubzac, 2010.

MARCONI, Marina; LAKATOS, Eva Maria. Técnicas de pesquisa. **São Paulo: Atlas**, v. 205, p. 88, 1996.

MICROSOFT, An overview of Russia's cyberattack activity in Ukraine, 2022. Disponível em: https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd. Acesso em: 2 set. 2023.

MOTEFF, John *et al*. Critical infrastructures: What makes an infrastructure critical?. Washington, DC: **Congressional Research Service**, Library of Congress, 2003.

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

NAKASHIMA, Ellen. Russian military was behind 'NotPetya' cyberattack in Ukraine, CIA concludes. **The Washington Post,** 12 January 2018. Disponível em: https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html?noredirect=on. Acesso em: 20 set. 2023.

NYE, Joseph S. Cyber war and peace. **Project Syndicate**, v. 10, 2012.

OUYANG, Min. Review on modeling and simulation of interdependent critical infrastructure systems. **Reliability engineering & System safety**, v. 121, p. 43-60, 2014.

PERNIK, Piret. Hacking for influence: Foreign Influence Activities and Cyber-attacks. **International Centre for Defence and Security**, 2018.

POLITYUK, Pavel. Ukraine points finger at Russian security services in recent cyber attack. **Reuters**, 1 July 2017. Disponível em: https://www.reuters.com/article/us-cyber-attack-ukraine/ukraine-points-finger-at-russian-security-services-in-recent-cyber-attack-idUSKBN19M39P. Acesso em: 14 set. 2023.

REUTERS, Satellite outage knocks out thousands of Enercon's wind turbines, 28 February 2022. Disponível em: https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/. Acesso em: 1 set. 2023.

RID, Thomas. Cyber war will not take place. In: **Strategic Studies**. Routledge, p. 408-428, 2014.

RINALDI, Steven; PEERENBOOM, James; KELLY, Terrence. Identifying, understanding, and analyzing critical infrastructure interdependencies. **IEEE control systems magazine**, v. 21, n. 6, p. 11-25, 2001. Disponível em: https://www.researchgate.net/publication/3206740_Identifying_understanding_and_analyzing_critical_infrastructure_interdependencies. Acesso em: 1 de set. 2023.

RUSSIA, Russian Federation. Conceptual Views on the Activities of the Russian Federation Armed Forces in the Information Space, Russian Ministry of Defence, 2011.

SAADE, Juan; AMERONGEN, Max. AcidRain | A Modem Wiper Rains Down on Europe, **Sentinel Labs**, 31 march 2022. Disponível em: https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/. Acesso em: 20 out. 2023.

SCHULZE, Matthias; KERTTUNEN, Mika. Cyber Operations in Russia's War against Ukraine: Uses, limitations, and lessons learned so far. **Stiftung Wissenschaft und Politik**, 17 april 2023. Disponível em: https://www.swp-berlin.org/10.18449/2023C23/. Acesso em: 25 out. 2023.

SPÎNU, Nathalia. Ukraine Cybersecurity Governance Assessment. **DCAF**, 2020. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf. Acesso em: 21 out. 2023.

STRZELECKI, Marek. Ukraine's power plants need missile defence ahead of winter, DTEK CEO says. **Reuters**. November 20, 2023. Disponível em: https://www.reuters.com/world/europe/ukraines-power-plants-need-missile-defense-ahead-winter-dtek-ceo-says-2023-11-17/. Acesso em: 6 jan 2024.

STONE, John. Cyber war will take place!. **Journal of strategic studies**, v. 36, n. 1, p. 101-108, 2013.

SYMANTEC, Destructive Disakil malware linked to Ukraine power outages also used against media organizations. Symantec team response, 5 Jan 2016. Disponível em: https://www.symantec.com/connect/blogs/destructive-disakil-malware-linked-ukraine-power-outages-also-used-against-media-organizations?om_ext_cid=hho_ext_social__Sym_UPowerGrid_TWITTER_Connect%20Blog&linkId=20140284. Acesso em: 15 out. 2023.

TAQUARY SEGUNDO, Célio. **A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos**. 2019. TCC (Especialista em Altos Estudos em Defesa), Escola Superior de Guerra, Brasília, 2019.

TEIXEIRA JÚNIOR, A.; LOPES, G. V.; FREITAS, M. As três tendências da guerra cibernética: novo domínio, arma combinada e arma estratégica. Carta Internacional, v. 12, n. 3, p. 30–53, 2017. Disponível em: https://cartainternacional.abri.org.br/Carta/article/view/620. Acesso em: 4 ago. 2023.

TKACHENKO, Oleksii. Cybersecurity in Ukraine: National Strategy and international cooperation. **GFCE**, 7 June 2017. Disponível em: https://thegfce.org/cybersecurity-in-ukraine-national-strategy-and-international-cooperation/. Acesso em: 22 out. 2023.

TZU, Sun; PIN, Sun. **A arte da guerra**. WWF Martins Fontes, 2015.

UCRÂNIA. The President of Ukraine approved a new Cybersecurity Strategy of Ukraine. **National Security and Defense Council of Ukraine**, 2021. Disponível em: https://www.rnbo.gov.ua/en/Diialnist/4976.html#:~:text=The%20Cybersecurity%20Strategy%20of%20Ukraine%20defines%20the%20priorities%20of%20national,account%20current%20threats%20and%20challenges. Acesso em: 20 out. 2023.

UK. Foreign Affairs. Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion. **UK Government**, 10 May 2022. Disponível em: https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion. Acesso em: 1 out. 2023.

UE. Council of the EU. Russian cyber operations against Ukraine. Declaration by the High Representative on behalf of the European Union, **Council of the UE**, 10 May 2022. Disponível em: https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/. Acesso em: 1 out. 2023.

USAID. Review of the regulatory framework for Critical Infrastructures cybersecurity in Ukraine: legislative assessment report. **USAID Gov**, 16 november 2020. Disponível em: https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf. Acesso em 3 set. 2023.

VENTRE, Daniel (Ed.). **Cyberwar and information warfare**. John Wiley & Sons, 2012.

VIASAT, KA-SAT Network cyber attack overview. **Viasat News**, 30 march 2022. Disponível em: https://news.viasat.com/blog/corporate/ka-sat-network-cyber-attack-overview. Acesso em: 10 set. 2023.

WILLETT, Marcus. The Cyber Dimension of the Russia–Ukraine War. In: Survival: October-November 2022. Routledge, 2023. p. 7-26.

WORLD ECONOMIC FORUM, in partnership with Marsh & McLennan Companies, SK Group and Zurich Insurance Group. 2022. The Global Risks Report 2022. Insight Report. Chapter 3. Geneva: World Economic Forum, 2022. Disponível em: https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

YIN, Robert. Estudo de Caso: Planejamento e métodos. Bookman editora, 2015.

ZETTER, Kim. Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid. **Wired**, 3 March 2023. Disponível em: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/. Acesso em: 20 out. 2023.

AGRADECIMENTOS

Agradeço a Jesus por sempre permanecer comigo mesmo sem eu merecer. Durante toda a minha graduação fui sustentada pela tua palavra e guardei no coração o que diz em Isaías 40:31 - “mas aqueles que esperam no Senhor renovam as suas forças. Voam alto como águias; correm e não ficam exaustos, andam e não se cansam.” Essas palavras me deram força para continuar quando achei que não conseguiria chegar ao fim dessa jornada

Agradeço à minha bisavó Ivanilde Soares, aos meus avós maternos Jodelmir Souza e Eunice Soares (*in memoriam*), à minha avó paterna, Marilene Santos, aos meus padrinhos, Helvécio Soares e Rafaella Souza, às minhas tias Helenilde Fortes e Suzana Bittencourt por todo apoio, carinho e motivação durante a minha formação. Vocês são grandes exemplos para mim sobre coisas que a universidade não é capaz de ensinar.

Aos meus pais, Myrella Souza e Rodrigo Souza, sem o apoio de vocês, eu jamais conseguiria conquistar tudo o que conquistei. Sem o amor de vocês, eu não saberia qual o significado de amor incondicional. Sem os cuidados de vocês, eu não teria a capacidade de cuidar sem esperar nada em troca. Sem vocês, eu seria tão pouco.

Ao meu professor e orientador Dr. Fábio Nobre, meus sinceros agradecimentos pela oportunidade de discussão, pelo ensino, pela grande dedicação e paciência durante a elaboração deste trabalho. Agradeço pela orientação firme e objetiva, bem como pelas revisões e sugestões que facilitaram a conclusão deste trabalho.

À professora Dra. Thays Oliveira, por todos os conselhos, pela ajuda e pela paciência com a qual guiou o meu aprendizado. Saliento o apoio incondicional prestado, a forma interessada, extraordinária e pertinente como acompanhou a realização deste trabalho. As suas críticas construtivas, as discussões e reflexões foram fundamentais ao longo de todo o percurso. Não posso esquecer a sua grande contribuição para o meu crescimento como investigadora. Eternamente grata por todo o apoio.

À banca examinadora na pessoa do professor Dr. Bernardo Salgado, e ao professor Dr. Gills Vilar Lopes por disponibilizarem o seu tempo para me ouvir e por realizarem os apontamentos necessários visando a melhoria do meu trabalho.

Às minhas amigas, Ma. Ana Raphaela Florêncio e Ma. Rebeca Rabêlo, por toda a ajuda na minha trajetória e pelos conselhos que fizeram com que eu me apaixonasse pela academia.

Ao meu namorado e companheiro de vida, Cadete Thiago Gomes, por sempre me incentivar, apoiar e permitir com que as minhas asas pudessem levantar voo novamente. Você me apoiou incansavelmente em todas as fases deste trabalho. Sua paciência, compreensão e carinho foram fundamentais para que eu pudesse manter o equilíbrio emocional e alcançar a conclusão deste TCC. Eu te amo.

Aos meus sogros, Marluce Olimpia e Wellington Gomes por todo carinho comigo e pelo apoio. Foi uma bênção ter começado a fazer parte desta querida família e partilhar todos os momentos que temos vivido.

Aos meus amigos e companheiros de formação, Luan Miranda, Josinadja Freitas, Isadora Braga, Débora Régis e Ana Virgínia. Quero expressar minha gratidão a vocês, que sempre me encorajaram a perseguir meus objetivos e me ajudaram a manter a motivação em momentos difíceis.

Aos meus amigos, Ester Hadassa, Letícia Gomes e Israel Bertrand por estarem comigo, mesmo longe, vocês estão sempre guardados no meu coração.