ESCOLA DE COMANDO E ESTADO-MAIOR DO EXÉRCITO
ESCOLA MARECHAL CASTELLO BRANCO

Maj Com RODRIGO **TARGINO** SOUZA

Impactos da segurança da informação no nível tático no desenvolvimento do conflito russo-ucraniano.

Rio de Janeiro
2023

Maj Com RODRIGO **TARGINO** SOUZA

Impactos da segurança da informação no nível tático no desenvolvimento do conflito russo-ucraniano.

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Orientador: Ten Cel Inf BRUNO RODRIGO DE **SOUZA ROSA**

Rio de Janeiro
2023

S729i Souza, Rodrigo Targino.
Impactos da Segurança da Informação no nível tático no desenvolvimento do conflito Russo-ucraniano. / Rodrigo Targino Souza. - 2023.
61 f. : il. : 30 cm.

Orientação: Bruno Rodrigo de Souza Rosa.

Trabalho de Conclusão de Curso (Especialização em Ciências Militares) — Escola de Comando e Estado-Maior do Exército, Rio de Janeiro, 2023.
Bibliografia: f. 51-61

1. Segurança da Informação. 2. Guerra. 3. Rússia. 4. Ucrânia. I. Título.

CDD 355.4

Maj Com RODRIGO **TARGINO** SOUZA

Impactos da segurança da informação no nível tático no desenvolvimento do conflito russo-ucraniano.

Trabalho de Conclusão de Curso apresentado à Escola de Comando e Estado-Maior do Exército, como requisito parcial para a obtenção do título de Especialista em Ciências Militares, com ênfase em Defesa Nacional.

Aprovado em _____.

COMISSÃO AVALIADORA

_____
Bruno Rodrigo de Souza Rosa - Ten Cel Inf - Presidente
Escola de Comando e Estado-Maior do Exército

_____
Romulo Torres Ramiro - Ten Cel Inf - Membro
Escola de Comando e Estado-Maior do Exército

_____
Joel Henrique Fonseca de Ávila - Ten Cel Art - Membro
Escola de Comando e Estado-Maior do Exército

À minha esposa Anny por tornar meus dias mais felizes. Uma sincera homenagem pelo carinho e compreensão demonstrados durante a realização deste trabalho.

AGRADECIMENTOS

Agradeço primeiramente a Deus por todas as oportunidades e conquistas alcançadas, pelos ensinamentos que a escola da vida nos proporciona na lida diária.

À minha esposa, fiel companheira de todos os dias. Seu coração acolhedor e seu otimismo contagiante sem foram a inspiração dos meus dias.

Ao meu orientador, Ten Cel Souza Rosa, pela paciência, confiança, camaradagem e precisão nos apontamentos dados em cada etapa deste trabalho.

Ao comando da ECEME, pela atenção e cuidado na formação dos oficiais de Estado-Maior.

Aos meus pais Sócrates e Maurineide, por toda dedicação e educação voltados à minha formação pessoal.

RESUMO

Este trabalho teve como objetivo analisar os principais incidentes relacionados à segurança da informação ao longo do primeiro ano do conflito e russo-ucraniano. Para tanto foram explorados aspectos referentes a caracterização do conflito russo-ucraniano; à segurança da informação no âmbito dos conflitos armados, às ações desenvolvidas e pela Rússia no campo cibernético e informacional; às reações ucranianas nesses dois campos e à estrutura militar brasileira relacionada à segurança da informação. A pesquisa foi realizada por meio da consulta a artigos publicados, manuais, documentos externos, relatórios, sítios oficiais do Governo Federal e do Exército Brasileiro, além de outros trabalhos acadêmicos relacionados ao assunto. A análise dos fatos estudados evidenciou a adequação da estratégia nacional de defesa brasileira na área de segurança da informação. Esse estudo ganha relevância com a atual conjuntura de desenvolvimento tecnológico atrelado ao emprego da expressão do poder militar. Por fim, o Estado brasileiro tem buscado se manter atualizado e competitivo no contexto internacional quanto à segurança da informação, particularmente empenhado em salvaguardar os interesses nacionais.

Palavras-chave: Segurança da informação, guerra, Rússia, Ucrânia.

ABSTRACT

This paper analyzed the main incidents related to information security throughout the first year of the Russian-Ukrainian conflict. It was explored the aspects relating to the characterization of the Russian-Ukrainian conflict were explored; information security in the context of armed conflicts, the actions developed by Russia in the cyber and informational field; the Ukrainian reactions in these two fields and the Brazilian military structure related to information security. The research was carried out by consulting published articles, manuals, external documents, reports, official websites of the Federal Government and the Brazilian Army, as well as other academic works related to the subject. The analysis of the facts studied highlighted the adequacy of the Brazilian national defense strategy in the area of information security. This study gains relevance with the current situation of technological development linked to the use of the expression of military power. Finally, the Brazilian State has sought to remain updated and competitive in the international context regarding information security, particularly committed to safeguarding national interests.

Keywords: Information security, war, Russia, Ukraine.

SUMÁRIO

1. INTRODUÇÃO

A presente pesquisa analisou os impactos da segurança da informação no conflito entre Rússia e Ucrânia, no nível tático, durante o período de 22 de fevereiro de 2022 a 22 de fevereiro de 2023. Segundo o Manual de Operações de Informação, a informação tem tomado vulto proeminente nas operações militares e afetado as formas de emprego das Forças Armadas (BRASIL, 2019).

Segundo Fontes (2006), a informação é um ativo importante, pois constitui um conjunto de dados que tem valor para uma organização. Ainda segundo o autor:

> A segurança da informação é o conjunto de orientações, normas, procedimentos, políticas e demais ações que tem por objetivo proteger o recurso informação, possibilitando que o negócio da organização seja realizado e a sua missão seja alcançada (FONTES, 2006, p. 20).

Dessa forma, a segurança da informação é importante para garantir a confidencialidade, integridade e disponibilidade dos dados e sistemas, bem como proteger ativos contra ameaças como ataques cibernéticos, roubo de informações, espionagem, entre outros (MACHADO, 2014).

As medidas de segurança da informação podem incluir políticas, procedimentos, tecnologias e práticas de gestão de risco para proteger a informação e minimizar os impactos de incidentes de segurança (PONTES, 2012).

Os conflitos atuais, marcados pela influência da Era da Informação, revestem-se de especial atenção dada à dimensão informacional (VISACRO, 2018). Esse contexto aponta a segurança da informação como fator multiplicador do poder nacional. Em eventos com uso do componente militar, os Estados podem se encontrar em condição de superioridade ou vulnerabilidade de acordo com suas capacidades relacionadas à segurança da informação (CEPIK, 2002).

Essa demanda por superioridade informacional interfere diretamente na organização das Forças Armadas de um Estado e interage com as dimensões humana e física (BRASIL, 2017). Assim, a segurança informacional pode influenciar a conduta militar em todas as dimensões do conflito (MARTINS, 2020).

Nesse sentido, faz-se necessário superar possíveis deficiências encontradas na segurança informacional, visando estabelecer, no nível tático da aplicação do poder militar de um Estado, a vantagem necessária para atingir-se os objetivos políticos e estratégicos que norteiam suas ações (BETHLEM, 1981). A proteção de

ativos de informação e a mitigação de eventos provenientes de exploração de vulnerabilidades pode, eventualmente, resultar em decisiva vantagem no desempenho militar de um Estado em conflito bélico (NOGUEIRA, 2018).

Em relação ao conflito Russo-Ucraniano, a Guerra Cibernética e Eletrônica já são empregadas por russos desde 2014 (SILVA, 2023), quando esses realizaram ataques na região do Donbass. Entretanto, existem relatos atuais que apontam para usuários que denunciam posições de homizio pela simples utilização de redes sociais, o que torna a segurança da informação e a contrainteligência ainda mais sensíveis no amplo espectro dos conflitos (ALVES, 2022). Esse acesso ininterrupto e irrefreado a ativos de informação reacende a discussão em torno da correta utilização de meios informacionais num contexto do combate convencional.

No âmbito do Brasil, a análise do tratamento dado à segurança da informação no conflito entre Rússia e Ucrânia pode ocasionar a revisão de estruturas e processos organizacionais e implicar racionalização e maior eficiência. O próprio Exército Brasileiro (EB) sinaliza esse intento em seu Plano Estratégico, incentivando a pesquisa e inovação na área informacional (BRASIL, 2019b).

Paralelamente, o EB demonstra latente preocupação com a utilização de ativos de informação, o que é observado nas diretrizes emitidas pelo Comandante da Força, Estado-Maior do Exército (EME) e pelos demais órgãos da Força Terrestre vinculado à C&T. Entretanto, tais diretrizes encontram-se contextualizadas num ambiente de paz, ressaltando a necessidade de investigar os impactos da segurança da informação no planejamento e condução de atividades militares em contexto de guerra.

Tudo isso, leva ao questionamento: quais são os impactos da segurança da informação nas condutas militares ucranianas, no conflito entre Rússia e Ucrânia, no nível tático, ao longo do primeiro ano desse conflito?

Portanto, a presente pesquisa teve como objetivo analisar os impactos da segurança da informação nas Forças Armadas Ucranianas no primeiro ano de conflito entre Rússia e Ucrânia. Nesse escopo, voltou-se o foco para incidentes e seus tratamentos passíveis de aferir valor à realidade brasileira, de modo a servir como alicerce para possíveis ajustes doutrinários.

Diante disso, os objetivos específicos da pesquisa foram: identificar eventos ocorridos no conflito russo-ucraniano relacionados à segurança da informacão;

identificar os impactos desses eventos no primeiro ano conflito, particularmente em condutas militares ucranianas relacionadas à segurança da informação; e relacionar condutas militares ucranianas supracitadas com práticas relacionadas à segurança da informação adotadas no Brasil.

A razão social pela qual a pesquisa se justifica encontra-se em seu tema central, qual seja a defesa. É de interesse de toda sociedade brasileira que o Estado brasileiro se encontre a par das inovações doutrinárias provenientes de avanços tecnológicos a fim de ofertar segurança e bem-estar social à sua população (HOBBES, 1988).

Academicamente, por se tratar de evento recente, procura-se avançar na pesquisa científica que explora o conflito entre Rússia e Ucrânia, particularmente no setor informacional. Essa pesquisa propicia maior discussão e possíveis aplicações para a Defesa do Brasil, partindo de eventos experimentados por outros Estados. Além disso, a análise do tema pode apontar prognósticos e tendências acerca de novos conflitos e situações de emprego das Forças Armadas (VISACRO, 2023).

Adicionalmente, o presente estudo alinha-se estrategicamente com os objetivos do Exército Brasileiro. Observa-se no Plano Estratégico do Exército 2020-2023, o Objetivo Estratégico do Exército Nr 7: Aprimorar a gestão estratégica da informação. Esse objetivo se ramifica em outro dois, quais sejam: 7.2 - reorganização do sistema de informação do Exército; 7.2.1 - aperfeiçoar a gestão da informação organizacional do Exército e 7.2.1.2 - otimizar e racionalizar a produção de sistemas de informação. Todos esses objetivos serão abordados direta ou indiretamente no escopo desse trabalho (BRASIL, 2019c).

2. METODOLOGIA

2.1 TIPO DE PESQUISA

Essa é uma pesquisa qualitativa, uma vez que procurou aprofundar a compreensão dos fatos em torno de processos sociais (RICHARDSON, 1999). Seu caráter metodológico visou basear-se em eventos reais para relacioná-los a condutas e estruturas observadas durante o conflito russo-ucraniano, associando formas, maneiras e procedimentos para se atingir determinado fim. Para se atingir o objetivo da pesquisa, usou-se a Análise de Conteúdo (BARDIN, 2004) como forma de analisar os dados oriundos da coleta.

A pesquisa privilegiou relatos e análises de documentos para entender os impactos da segurança da informação no conflito russo-ucraniano. Seguindo a taxionomia de Vergara (2006), quanto aos meios de investigação, essa é uma pesquisa bibliográfica, amparando-se em livros, jornais, artigos, revistas e sites da internet, disponibilizados ao público em geral.

2.2 COLETA DE DADOS

Todos os dados coletados referiram-se ao período de 22 de fevereiro de 2022 a 22 de fevereiro de 2023, relacionados à Guerra Russo-ucraniana.

Esta pesquisa realizou o levantamento de dados por meio de pesquisa bibliográfica (LIMA; MIOTO, 2007) de literatura (livros, trabalhos acadêmicos, jornais, revistas e redes eletrônicas), além de documentos internos produzidos pelo Exército Brasileiro. As consultas foram baseadas nas principais fontes de pesquisa de trabalhos acadêmicos, como as plataformas digitais do Google Acadêmico, Scielo, Biblioteca Digital do Exército e EB Revistas.

Os instrumentos utilizados para coleta de dados e informações visaram a explicação e análise dos aspectos teóricos estudados. Os dados priorizados foram aqueles classificados como secundários e terciários, quais sejam, documentos escritos, relatórios, artigos, sejam citados ou fornecidos por terceiros.

2.3 TRATAMENTO DOS DADOS

O tratamento dos dados foi feito por meio da análise dos eventos reportados nas operações realizadas em solo Ucraniano, entre os dias 22 feveireiro de 2022 a 22 fevereiro de 2023, por meio da análise de conteúdo.

A análise de conteúdo (AC) agrega um conjunto de técnicas de análise de comunicação e tem por objetivo indicar as condições de produção dessa mensagem. Isso se dá por meio de procedimentos sistemáticos de descrição do conteúdo da mensagem (BARDIN, 2004).

O registro de eventos militares estudados levou em consideração não uma palavra-chave, mas um tema em questão associado a seu impacto na segurança da informação, tomando por base os ramos da segurança física, de redes, de sistemas, de banco de dados e de continuidade dos serviços.

A seguir, esse impacto foi relacionado a uma possível reação de qualquer dos envolvidos diretos no conflito e comparado às estruturas e doutrinas existentes no EB. Finalmente, fruto dessa comparação, procurou-se inferir acerca de possivel adequação doutrinária brasileira.

2.4 LIMITAÇÕES DO MÉTODO

A principal limitação do método se deu pela grande dificuldade de selecionar fontes seguras para a obtenção de dados, fruto da natureza da Guerra Informacional. Isso implicou a necessidade de intensa confrontação de informações, a fim de agregar credibilidade ao dado em estudo.

Outra limitação se deveu ao fato de que a análise desses dados revestiu-se de caráter parcial, particularmente pelo fato do conflito estar em desenvolvimento e seu desfecho ser imprevisível, o que insufla a necessidade da continuidade de estudo em torno desse tema.

3. A GUERRA NA UCRÂNIA E A SEGURANÇA DA INFORMAÇÃO

3.1. A GUERRA DA UCRÂNIA

Desde seu início, em 24 de fevereiro de 2022, a Guerra Russo-Ucraniana tem sido objeto de estudo em todo o mundo. As análises em torno do conflito apontam desde antecedentes históricos até veiculação de vídeos em tempo real.

A situação entre Ucrânia e Rússia é complexa e foi analisada por Garnett (1997) a partir da dissolução da URSS em 1991. Segundo o autor, o estado das minorias russas em território ucraniano é motivo de preocupação da política interna de Kiev desde a década de 1990, já que, ao longo dos anos, a presença de falantes de russo nesse território cresceu a ponto de atingir a marca de 50% da população (GARNETT, 1997).

Esse contexto foi bem utilizado pelo presidente russo, Vladimir Putin, que utilizou o discurso da diáspora Rússia como uma estratégia para incentivar o início de uma guerra civil entre russos e ucranianos. Dessa forma, a Rússia poderia obter maior liberdade de ação nas regiões de maior concentração russa, justamente as regiões leste e sul da Ucrânia (MIELNICZUK, 2006).

A influência da política externa de Moscou na Ucrânia foi investigada por Costa (2022), que revela como os governos ucranianos mantiveram alinhamento com o pensamento estratégico russo. Essa postura fez com que a Ucrânia viesse a ceder à Rússia, em 1994, 3 anos após sua independência, seu arsenal nuclear em troca de proteção e reconhecimento da soberania de seu país (COSTA, 2022).

Mielniczuk (2014) avaliou a situação ucraniana no início da década de 2010. Segundo o autor, fruto de crises econômicas, má gestão de recursos e consequente desvalorização monetária, a Ucrânia imergiu na chamada “Revolução Laranja”. Esse movimento popular buscou romper o controle russo na política ucraniana e propiciou a aproximação desse país com a esfera ocidental, como forma de recuperar a identidade nacional e o desenvolvimento econômico.

Essas ações reduziram a dissuasão ucraniana e facilitaram as manobras militares russas na região do leste europeu. Não obstante, Rodrigues da Silva (2018) exemplifica a rápida anexação da Crimeia em 2014 como consequência dos fatos

supracitados. A conquista da Crimeia pela Rússia só foi possível pela intensa liberdade de ação conquistada por esse país na região.

Aparecido e Aguilar (2022) indicaram os anseios da Ucrânia em aderir à OTAN como fator deflagrador para a ação militar russa em 2022. Esses autores também levaram em consideração os movimentos separatistas no leste ucraniano, na região de Donbass, e a anexação da Crimeia por Moscou como importantes antecedentes da Guerra.

Nesse contexto, o anseio russo pelo acesso e controle de mais áreas de “águas quentes” é apontado por Mazat (2013) como reconhecidamente antigo, assim como a intenção de conter a expansão da Organização do Tratado do Atlântico Norte (OTAN) no seu entorno estratégico. Segundo a autora, o conflito histórico entre Rússia e Ucrânia pode reconfigurar o panorama político na região e influenciar o controle de rotas comerciais estratégicas.

Em relação à Guerra Russo-Ucraniana, Costa e Dejour (2022) citam que desde a ofensiva militar de fevereiro de 2022, as ações russas são amplamente legitimadas pelo discurso de seu presidente. Esse discurso visa legitimar o controle sobre as regiões de Donbass, Luhansk e Donetsk, além de áreas litorâneas como as cidades de Odessa e Mariupol, sob o pretexto de defender a integridade da população russa residente nesses locais (COSTA E DEJOUR, 2022).

Diante disso, diversos impactos têm se observado. No âmbito mundial, pôs-se à prova toda a legitimidade do sistema internacional como eficiente garantidor de estabilidade e paz (SOUZA, 2023). Na esfera de cada Estado, os líderes mundiais vêm encontrando profundos óbices, seja no quesito segurança energética, particularmente dos países europeus, quanto na segurança alimentar, haja vista a importância da região na produção e exportação de grãos, a exemplo do trigo (JOSEPHS, 2022).

Fruto desse contexto, o líder ucraniano, Volodymyr Zelensky, tem recebido apoio de potências ocidentais, principalmente nas expressões política, econômica e militar. O suporte ofertado por Estados Unidos da América (EUA) e demais países membros da OTAN aumentaram a dimensão do conflito que já é percebido como de longa duração (UNITED STATES, 2022). A fim de rivalizar com essa aliança militar, a Rússia busca apoio em outros rivais do ocidente, o que coloca mais uma vez a China como grande *player* no tabuleiro mundial (CAMPATO, 2022).

Simultaneamente a essas expressões, a ciência e tecnologia (C&T) tomou grande vulto na Guerra Russo-Ucraniana por meio da dimensão informacional (NUNES, 2022). Seja na utilização de ataques cibernéticos, seja pela aquisição de informações e escolha de alvos pelas Forças Russas em diferentes contextos. O combate convencional agora é observado dentro da Era da Informação por diversos atores que interagem diversamente com o conflito, como se observa:

> A invasão ocorreu no dia 24 fevereiro de 2022 e as ações que se desenrolaram ao longo dos dias seguintes demonstraram diversas oportunidades de pesquisa para estudiosos de assuntos militares e políticos, mas de forma objetiva, evidenciam a preparação prévia e a utilização de conceitos modernos, principalmente no tocante à guerra cibernética, mobilização de meios, suporte logístico, participação de elementos não estatais, emprego de materiais de emprego militares de última geração, evidenciando o preparo das nações envolvidas (COSTA E DEJOUR, 2022, p. 14).

A exemplo disso, a guerra de narrativas e o papel das redes sociais tem incentivado a participação de civis no conflito, que, por vezes, noticiam e veiculam imagens de modo autônomo (GRAÇA, 2022). Essa prática influencia, inclusive, a aquisição de alvos e falhas de segurança na dimensão física.

Dessa forma, observa-se que o conflito russo-ucraniano é antigo e complexo, envolvendo múltiplos atores e dimensões. Essa característica aliada a novas tecnologias e práticas associadas ao ambiente informacional multiplicam os impactos gerados pela guerra.

3.2. A SEGURANÇA DA INFORMAÇÃO NOS CONFLITOS

A segurança da informação pode impactar significativamente nos conflitos armados modernos (BRASIL, 2014). Com o aumento da tecnologia e da conectividade, a informação se tornou uma ferramenta cada vez mais importante na condução da guerra. Essa informação ganha ainda mais impacto quando associada ao meio pelo qual trafega e ao público ao qual é direcionado (MORGADO, 2021).

A proteção das comunicações tem sido apontada como uma das principais formas de preservar os ativos de informação (BRASIL, 2014). Júnior e Macedo (2019) indicam que uma das medidas mais comuns entre as Forças Armadas nesse quesito, é a utilização de criptografias para transmissão de informações sensíveis, como

planos, ordens e posições. Afinal, o comprometimento de informações pode implicar significativa vantagem a ser explorada pelo inimigo.

A segurança da informação durante os conflitos também é indicada por Nonato e Pinho (2021) como relevante na proteção de infraestruturas críticas. O ataque a sistemas de energia, comunicações e financeiros podem causar severos danos estruturais às tropas regulares e à população, escalando o conflito e afetando os envolvidos também no nível psicológico.

Nesse âmbito, Furlanetto (2020) revela que a segurança informacional confere proteção a informações críticas desde os tempos de paz. Isso se deve ao sigilo atribuído a informações críticas como Hipóteses de Emprego da Forças Armadas, tecnologias de uso militar, infraestruturas militares ou críticas e cadeias de suprimento.

Na dimensão informacional dos conflitos, a desinformação também têm sido objeto de estudo como ferramenta para a condução das operações. Como observam Teixeira e Costa:

> "Nesse aparato tecnológico que alimenta a guerra, a desinformação representa, portanto, valiosa arma de capital para a defesa de suas incalculáveis pretensões – seja para o convencimento da audiência sobre a legitimidade da batalha ou para a destruição total do inimigo.
> Diariamente, algoritmos treinados se encarregam de espalhar, milimétricamente, mentiras sobre a batalha no leste europeu. A guerrilha digital oscila entro o duro confronto e a tênue conciliação da desinformação com textos originados nas plataformas digitais e nas mídias corporativa e estatal." (TEIXEIRA e COSTA, 2023, p. 31)

Lopes (2021) estudou o termo "controle reflexivo", adotado pela Rússia, no qual o fornecimento de informações falsas e amplo uso da comunicação estratégica adquirem papéis fundamentais na manipulação do adversário e controle de seu processo decisório. Essa atitude é relacionada à doutrina normatizada pelo Gen. Gerasimov que descreveu o quadro atual do conceito operacional russo como a utilização de todos os "métodos não militares na resolução de conflitos interestaduais" (DUARTE, 2022).

Essa doutrina representa um desafio ao modo de combate ocidental. A falta de familiaridade, aliado a suposta ilegalidade de seu uso pode atuar como fator limitador dos Estados ocidentais. Diante disso, outros atores não-estatais, particularmente empresas de grande porte da tecnologia da informação, assumiram protagonismo na dimensão informacional da guerra Russo-Ucraniana. Além das empresas, aplicativos

mensageiros são amplamente empregados para coordenação de atividades civis na dimensão informacional, como aponta Duarte:

> Gigantes tecnológicas como a Google, Meta, Amazon, Microsoft e Apple têm uma linha direta para os corações e mentes de milhões de pessoas diariamente
> No entanto, estes países utilizam uma plataforma em comum: o Telegram! Esta plataforma criptografada, que não transmite as informações na internet como o Twitter ou Facebook, tornou-se no campo de batalha mais importante nesta Guerra da Informação. Isto possibilita a ocultação de informação sensível. Ambos os presidentes têm vários canais nesta rede, mas Zelensky usa-os para chegar ao povo russo falando em russo, enquanto Putin aproveita para reforçar a sua propaganda aos seus habitantes.
> Para além disso, as plataformas deixaram de ser neutras e tomaram o lado ucraniano ao bloquearam as mensagens russas. Por exemplo, o Youtube removeu mais de 1000 canais e 15000 vídeos e o Facebook restringiu o acesso às contas oficiais da Rússia Today e Sputnik e proibiu-os de publicar anúncios. Em resposta, a Rússia considerou o Facebook uma organização extremista (DUARTE, 2022, p. 25).

Ainda no campo da informação, SILVA (2023) observa a ampla utilização da Guerra Cibernética como fator multiplicador dos efeitos do combate ou como preparação para ataque cinéticos:

> Na invasão da Rússia à Ucrânia, ocorrida em 2022, um dos campos de batalha foi o front cibernético, que foi iniciado antes mesmo da invasão física. Foram realizadas ações cibernéticas contra a Ucrânia atingindo provedores de Internet, instituições financeiras, instalação governamentais e áreas importantes do governo tais como o Ministperio da Defesa nacional e as Forças Armadas, emissoras de televisão e órgãos nacionais. A maior parte desses ataques passuía como objetivo a criação de instabilidade na comunicação da Ucrânia (SILVA, 2023, p. 50).

Nesse diapasão, as atividades de ataque, exploração e proteção cibernéticas foram observadas em momentos diversos do conflito. Como elenca o mesmo autor:

> Os ataques cibernéticos russos à Ucrânia já haviam ocorrido em junho de 2017, com o malware *NotPetya*. O ataque tinha como alvo majoritariamente organizações ucranianas, especificamente do setor de infraestrutura. Este *Malware* se espalhou rapidamente pela Europa e afetou diversas indústrias como bancos, governos, lojas de varejo, empresas energéticas, entre outros, causando um prejuízo de US$ 10 bilhões, de acordo com a empresa de serviços de tecnologia Apex.
> O *malware NotPetya* reescrevia uma parte do disco rígido denominado registro Mestre de Inicialização ou *Master Boot Record* (MBR), que impossibilita a máquina infectada de inicializar o sistema operacional Windows corretamente.
> Um dos riscos dos ataques cibernéticos é que estes podem se espalhar para outras partes do mundo, principalmente devido às estruturas de computação em nuvem ou *cloud computing* que estão interligadas por todo o globo.
> Adicionalmente, existe um efeito psicológico devido à proliferação de fake News, a população pode ficar desorientada e perde a confiança. Por exemplo, no início da guerra Rússia x Ucrânia, foi difundido que o presidente ucraniano

> havia fugido do país. Posteriormente, o próprio presidente postou vídeos mostrando que isso não era verdade. Existe um efeito psicológico devastador nas pessoas, principalmente em situações de guerra (SILVA, 2023, p. 54).

Em resposta às ações russas, relatos apontam o ineditismo ucraniano em recrutar voluntários a fim de compor um “exército digital” no país. As ações desse componente são coordenadas via aplicativo *Telegram*, que reúne cerca de 200 mil usuários (LYNGAAS, 2022).

O Brasil, preocupado com esse novo vetor de combate e com a segurança das informações trafegadas nos órgãos federais, publicou o Decreto nº 5.772, em 2006. Esse decreto cria o Departamento de Segurança da Informação e Comunicações (DSIC) do Gabinete de Segurança Institucional da Presidência da República (GSI/PR), que tem, dentre suas atribuições, a responsabilidade de orientar a implementação de ações de segurança da informação e comunicações, inclusive as de segurança cibernética, no âmbito da administração pública federal (CONCEIÇÃO, 2017).

Outro documento que normatiza ese assunto é a Política Nacional de Segurança de Infraestruturas Críticas (PNSIC) que define como infraestruturas críticas as instalações, os serviços, os bens e os sistemas, cuja interrupção ou destruição, total ou parcial, provoque impacto social, ambiental, econômico, político, internacional ou à segurança do Estado e da sociedade. Assim, o Estado brasileiro procura aliar esforços de seu poder nacional a fim de adotar medidas preventivas e de caráter reativo, para preservar ou restabelecer a prestação dos serviços essenciais prestados por essas infraestruturas (BRASIL, 2018).

Diante desse panorama, infere-se que o conflito bélico russo-ucraniano se configura como ambiente inovador no emprego de artefatos cibernéticos e na exploração de vulnerabilidades de segurança da informação. Esse cenário indica a possibilidade de analisar possíveis lições aprendidas pelos atores envolvidos a fim de predizer boas práticas relacionadas a esse assunto num contexto de combate convencional.

4. INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DURANTE O CONFLITO RUSSO-UCRANIANO

O ano de 2022 foi marcado pelo avanço russo em solo ucraniano, porém essa atitude ofensiva não se deu apenas na dimensão física. Na dimensão informacional, o governo russo parece ter utilizado amplo portifólio e capacidade dos meios a fim de potencializar suas ações e conquistar seus objetivos estratégicos.

4.1 INCIDENTES DE REDE, SISTEMAS E BANCOS DE DADOS

4.1.1 INCIDENTES DE ESPIONAGEM

Os incidentes cibernéticos ocorridos na Ucrânia revelam ter correlação com as atividades de inteligência nos momentos anteriores às invasões físicas do território. Isso se deve à forma como esses ataques ocorreram. Ao invés de visar a destruição ou corrupção de ativos de informação, as ações cibernética em solo ucraniano visaram a aquisição de informação por meio das técnicas de *phishing* (THREAT ANALISIS GROUP, 2023).

O ataques conhecidos como *phishing* procuraram ludibriar o usuário fazendo-o clicar em um *link* e comprometer a segurança de seus dados. Isso pôde ser observado pela intensidade de *e-mails* veiculados na redes ucranianas e que podem ter relação com as informações usadas para planejar o ataque coordenado a partir do dia 24 de fevereiro de 2022 (SERPANOS, 2022).

Segundo o grupo de análise ameaças do Threat Analisis Group (TAG) do Google (2023), *hackers* supostamente homiziados em Moscou e conhecidos como o grupo “*Frozenvista*” lançaram cerca de 14 mil *e-mails* de *phishing* contra a Ucrânia e outros países apoiadores ainda em 2021. Essas iniciativas foram, paulatinamente, substituídas pelo grupo conhecido como *Pushcha* que intensificou seus esforços a partir de fevereiro, mesmo mês de invasão da região do Donbass. Esses ataques cibernéticos foram mais frequentes durante os primeiros quatro meses de ofensiva russa (KANTOLA, 2023).

A partir do gráfico abaixo, é possível observar que houve significativo número de ataques ao longo do ano de 2022, particularmente envolvendo os grupos FROZENVISTA e PUSHCHA, provavelmente sediados em Moscou e na Bielorrúsia,

respectivamente (MANDIANT, 2021). Também se constata que os ataques ocorreram em ondas, dentre as quais, a ocorrida no período entre fevereiro e agosto de 2022, acompanhando a ofensiva russa na dimensão física.

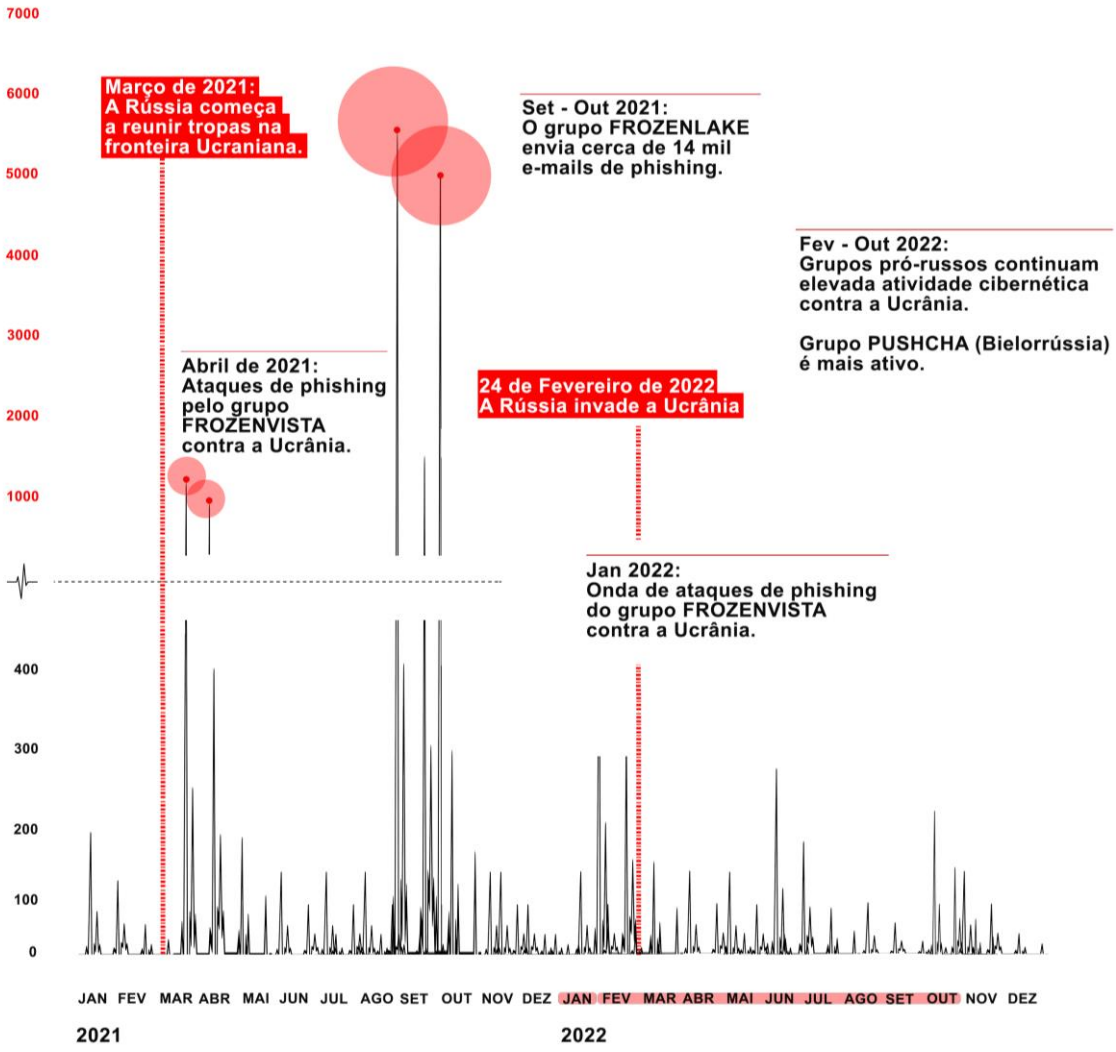


Gráfico 1 – Campanhas de *Phishing* na Ucrânia.
Fonte: TAG, 2023.

Paralelamente ao observado na Ucrânia, os ataques também foram direcionados a países da OTAN que relataram, entre fevereiro e junho de 2022, um aumento de 300% na incidência desses eventos. Essa iniciativa também é atribuída ao grupo PUSHCHA (ou Ghostwrite ou UNC1151), que foi apontado como principal autor, apoiado pelo governo bielorrusso. Além desse, outros grupos foram

relacionados como autores ou colaboradores dos ataques de *phishing* no contexto do conflito russo-ucraniano (INSIKT, 2023), são eles:

- FROZENBARENTS (também conhecido como Sandworm ou Voodoo Bear);
- FROZENLAKE (também conhecido como APT28 ou Fancy Bear);
- COLDRIVER (também conhecido como Callisto Group);
- FROZENVISTA (também conhecido como DEV-0586 ou UNC2589); e
- SUMMIT (também conhecido como Turla ou Urso Venenoso).

Segundo a Equipe de Resposta a Emergências de Computadores da Ucrânia (CERT-UA, 2022), o principal *modus operandi* dos *phishing* foram e-mails que fingiam ser atualizações críticas de segurança às organizações e instituições ucranianas, mas que na verdade eram arquivos executáveis que levavam à implantação de software de controle de área de trabalho remota nos sistemas infectados (LAKSHMANAN, 2023).

Além disso, algumas páginas foram elencadas como fraudulentas e apontadas como risco financeiro aos cidadãos ucranianos, pois solicitavam informações de cartões de créditos e outros dados pessoais que poderiam ficar comprometidos (CERT-UA, 2022). Eis alguns delas:

hXXp://kohhd[.]com/
hXXps://rivierafamily[.]com/
hXXps://compensationukr[.]com/
hXXps://compensations-ukrain[.]bar/
hXXps://compensation-ukr[.]com/
hXXps://europadonnaireland[.]org/
hXXps://foundpomoshi[.]com/
hXXps://peer-gos[.]top/
hXXps://helpzzfound[.]site/
hXXps://uacompensation[.]xyz/
hXXps://pay.uacompensation[.]xyz/

Com a alta incidência de ataques de phishing, é possível supor que houve largo acesso a dados ucranianos antes mesma da invasão ao território. Ao ludibriar usuários, o atacante pode ter se valido dos links e páginas maliciosas para acessar e conitnuar monitorando de forma remota qualquer servidor ou dipositivo infectado, sem que o usuário pudesse tomar ciência do ocorrido.

4.1.2 INCIDENTES DE SABOTAGEM

Ao longo de 2022, a sabotagem contra a Ucrânia assumiu, com frequência, a forma de ataques *DDoS*, e *Malwares* para negação de acesso a serviços ou corrupção de dados. O uso de *Malwares* foi diversificado, sendo possível o apagamento de

discos rígidos pelos conhecidos *Wipers* ou sequestro de dados por meio de *Rasonware.* Dessa forma, existe a possibilidade de que os dados desses sistemas tenham sido corrompidos ou explorados sem que se tenha pleno controle sobre essas ações (CANZANESE, 2023).

Diante disso, as vulnerabilidades dos bancos de dados ucranianos não são completamente conhecidas, entretanto é sabido que muitos desses *wipers* russos surgiram para atacar a Ucrânia, incluindo *WhisperGate, HermeticWiper, IsaacWiper* e outros. Um recente ataque usou uma nova família de *ransomware* conhecida como *Prestige* para atingir os setores de logística e transporte na Ucrânia e na Polônia (INSIKT, 2023).

Algumas das operações de hackers apoiados pelo governo russo contra a Ucrânia chamam a atenção. Em 14 de março de 2022, um *malware* destrutivo infectou uma organização ucraniana não identificada com um vírus que limpou todos os discos rígidos do órgão. Esse ativo, conhecido como *CaddyWiper*, também se infiltrou em sistemas financeiros e governamentais e pode ter apagado dados desses setores (PRZETACZNIK e TARPOVA, 2022). A linha do tempo abaixo, revela os tipos e ocorrências de *malwares* detectados em solo ucraniano:

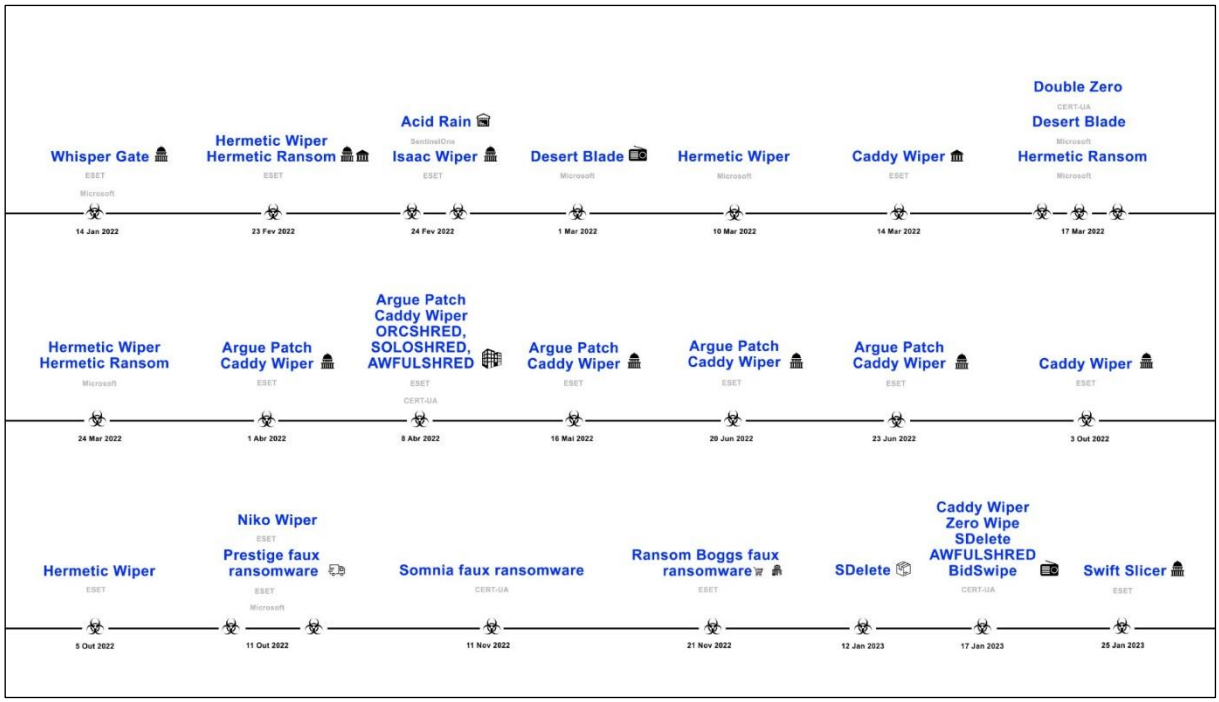


Figura 1 – Linha do tempo de ataques com *malwares* contra a Ucrânia.

Fonte: TAG, 2023 e o autor.

Nesse contexto, 15% dos ataques têm como alvo outras nações aliadas da Ucrânia, enquanto aproximadamente 85% dos ataques foram direcionados a indivíduos ou organizações dentro da Rússia ou da Ucrânia. Os ataques a alvos em outras nações também miraram infraestruturas críticas e agências governamentais (CANZANESE, 2023).

Esse aumento de ataques a usuários na Ucrânia foi de 250% em comparação com 2020. Os ataques a usuários nos países da OTAN aumentaram mais de 300% no mesmo período. Dias antes da invasão, relata-se a ocorrência de ataques a dois dos principais bancos estatais da Ucrânia. O Ministério da Defesa e as Forças Armadas ucranianas também foram alvos de ataques de negação de serviço ou *Distributed denial of service (DDoS)*. Os Estados Unidos e o Reino Unido indicaram os ataques ao Estado Maior das Forças Armadas da Rússia, embora o Kremlin tenha negado todas as acusações (FONSECA, 2023).

Segundo o a empresa Karspersky:

> Os ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído (DDoS). Esse tipo de ataque aproveita os limites de capacidade específicos que se aplicam a todos os recursos de rede, como a infraestrutura que viabiliza o site de uma empresa. O ataque DDoS envia múltiplas solicitações para o recurso Web invadido com o objetivo de exceder a capacidade que o site tem de lidar com diversas solicitações, impedindo seu funcionamento correto (KARSPERSKY, 2023).

Dentro desse escopo, dois setores foram apontados como alvos prioritários das ações cibernéticas russas: o financeiro e o governamental (JOTA, 2022). Aparentemente, esses setores foram privilegiados pelo caráter abrangente de seu impacto em todos os demais setores do Estado. Isso pode ser observado pelo caos instaurado na população ao ter o serviço de Energia Elétrica interrompido por ação de hackers que desligaram disjuntores remotamente após acessarem os sistemas de gerenciamento das redes elétricas ucranianas (PAGLIUSI, 2022).

Quanto ao setor financeiro, a estratégia se voltou para a implantação de *malwares* com a finalidade de corromper os bancos de dados e interromper os serviços bancários, de pagamento e instituições financeiras. Como resultado, os prejuízos foram alarmantes, além de provocar comoção nacional e impactos no setor de consumo (CORRÊA, 2023).

A ofensiva informacional, que coincidiu e persistiu desde a invasão militar do país na Ucrânia em fevereiro de 2022, concentrou-se fortemente no governo

ucraniano e nas entidades militares, juntamente com infraestrutura crítica, serviços públicos e setores de mídia. O famoso grupo de *ransomware* Conti e grupos de crimes cibernéticos *CoomingProject* manifestaram proteção ao governo russo e parecem cooperar com Moscou no sequestro e corrupção de dados ucranianos (LAKSHMANAN, 2023).

Outro aspecto interessante é que o número de ocorrências de *malwares* aumentou ao longo da ofensiva russa. Isso revela um potencial de mudança de objetivo nos ataques cibernéticos, que migraram de um perfil de exploração para destruição e corrupção da informação. Esse dado pode ser observado no gráfico abaixo:

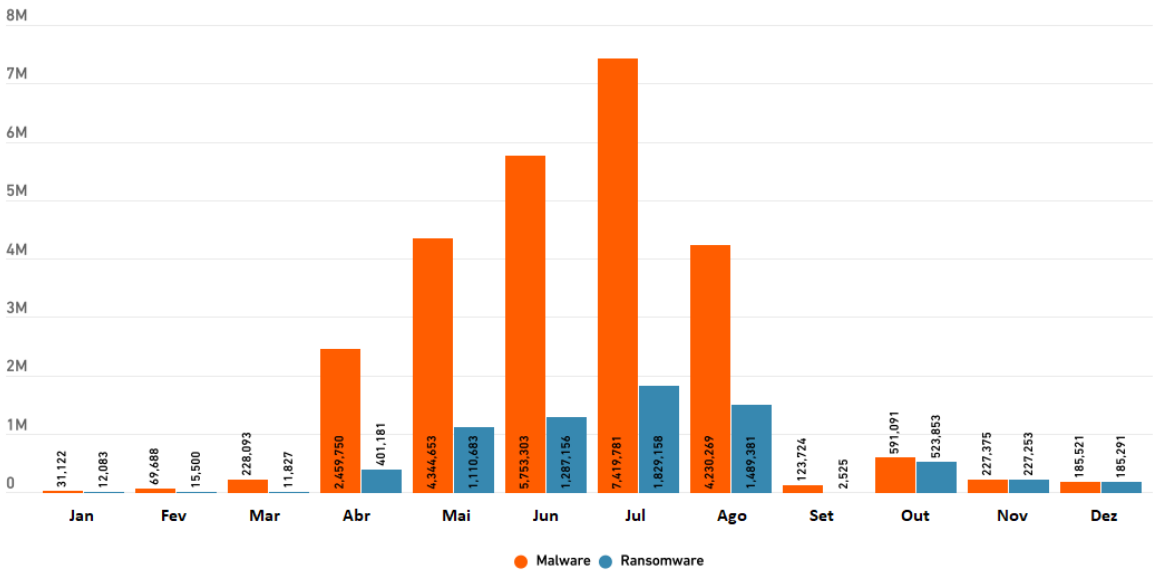


Gráfico 2 – Volume de ataques cibernéticos de sabotagem na Ucrânia 2022.
Fonte: SonicWall Cyber Threat Report, 2023.

Quanto à interrupção de serviços ucranianos, diversas organizações e bancos ucranianos passaram a ser alvos também de ataques distribuídos de negação de serviço (*DDoS*, sigla em inglês). *DDoS* é um tipo de ataque de rede de hosts infectados, mais conhecidos como bots, que tem por finalidade interromper e indisponibilizar o funcionamento de servidores e redes.

Os principais alvos desses ataques foram elencados abaixo:

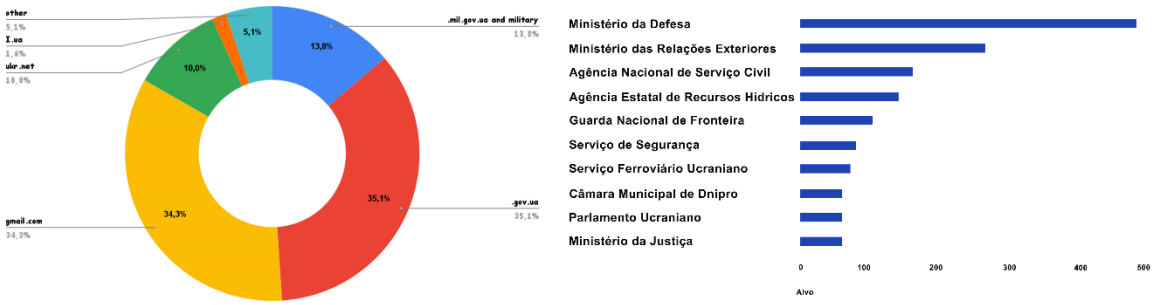
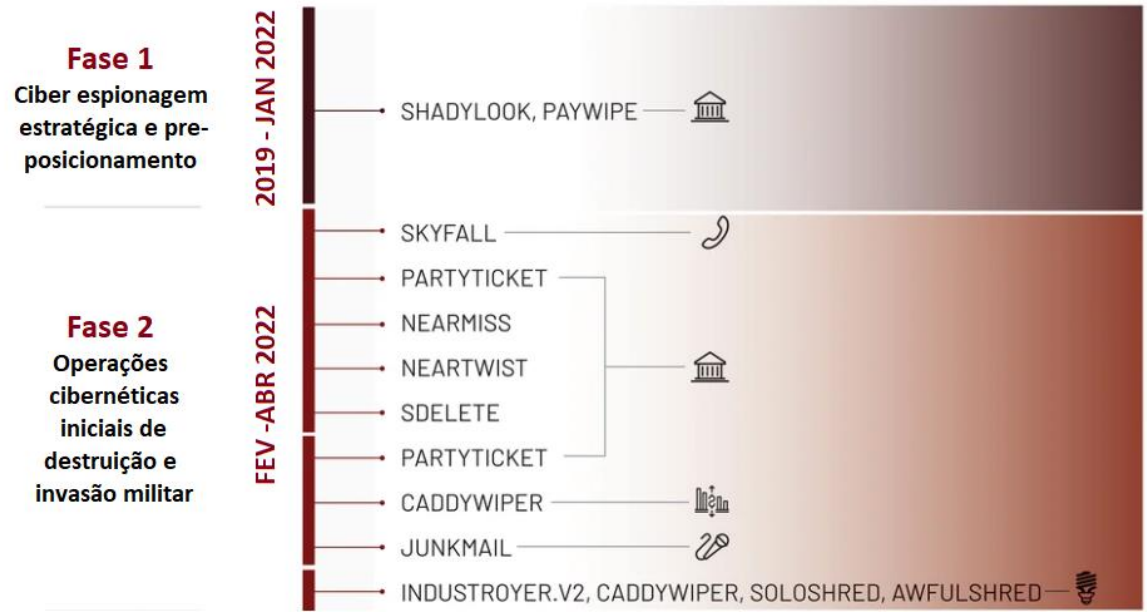


Gráfico 3: Número de alvos ucranianos que sofrerem ataques *DDoS*.
Fonte: TAG, 2023.

Nesse contexto, a gangue hacktivista *Killnet*, pró-Rússia, tem promovido sofisticados ataques *DDoS* a infraestruturas críticas dos membros da OTAN e apoiadores da Ucrânia. A dimensão desses ataques é percebida pela amostragem exposta pelo Centro de Tratamento de Respostas a Incidentes ucraniano (CERT-UA) em meados de março de 2022. Segundo o CERT-UA (2022) foram registrados, em apenas uma semana, 65 ataques a infraestruturas críticas do país. (CERT-UA, 2022).

Os ataques cibernéticos em solo ucraniano apontam um faseamento ilustrado no infográfico a seguir:



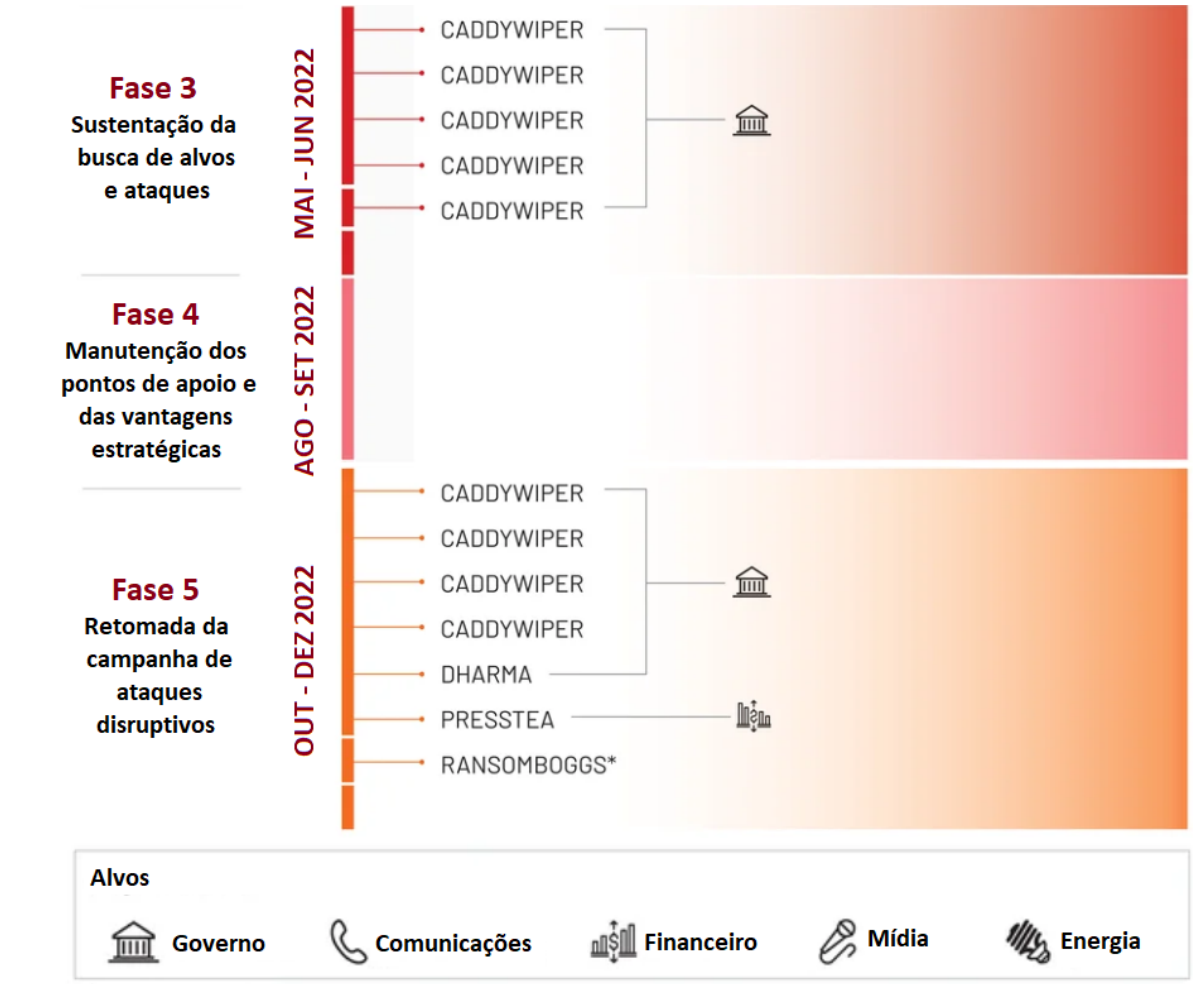


Figura 2 – Possíveis fases da campanha cibernética na Ucrânia.
Fonte: BLACK e RONCONE, 2023.

4.2 CAMPANHAS DE DESINFORMAÇÃO

Além dos ataques diretos à infraestrutura, a Rússia também lançou uma série de campanhas de desinformação e propaganda contra a Ucrânia. Essas operações buscaram manipular a opinião pública e criar divisões internas, espalhando notícias falsas, informações distorcidas e propaganda enganosa. Além disso, essas táticas de desinformação tiveram como objetivo gerar confusão, aumentar a polarização e dificultar a resposta coordenada do governo ucraniano, a fim de minar a estabilidade política e social do país (TEIXEIRA e COSTA, 2023).

Para tal, a Rússia procurou controlar a narrativa em domínios cibernéticos. As redes sociais se tornaram plataformas viáveis à disseminação de conteúdo relacionado a decisões militares, reações da comunidade internacional ante o conflito,

imagens degradantes de personalidades internacionais e resultados exitosos ou não de operações militares. Essas temáticas foram prioritariamente abordadas por meio de fotos e vídeos (GARCÍA-MARÍN, 2023).

Dentre as principais técnicas utilizadas, observou-se a invasão de mídias locais para o espalhamento de noticias falsas. Dois dias após a detecção do *Caddywipper*, em 16 de março de 2022, supostos invasores russos teriam se infiltrado em uma empresa de mídia para espalhar a informação de que Kiev se renderia a Moscou em breve. O “vazamento” era falso, como se mostrou posteriormente. Em seguida, um vídeo *deepfake* viralizou. As imagens mostravam o presidente ucraniano, Volodymyr Zelensky, afirmar que o país logo “desistiria de sua luta”. Desde então, os ataques foram mais direcionados aos ministérios da Defesa e Relações Exteriores da Ucrânia, assim como à Agência Nacional de Serviços do país. (PRZETACZNIK e TARPOVA, 2022)

Além dessas iniciativas, os ataques de desfiguração (*defacement*) eliminaram ou modificaram as informações em sites. Essa é uma ferramenta básica de desinformação que tem a capacidade de levar os internautas a acreditarem que dados incorretos são verdadeiros. A grande vantagem dessa técnica é a possibilidade viral de espalhamento do dado pelos próprios usuários. Trata-se de uma técnica antiga usada nos conflitos armados, sendo chamada de “ofuscação”, quando os lados de um conflito bélico abarrotam uma determinada população civil com informações enganosas. O efeito é basicamente psicológico e muito eficaz (ABBANY, 2022).

Diante desses eventos, as multinacionais vinculadas ao setor de TI, *BigTechs*, começaram a obtiver um papel mais relevante no cenário do conflito. O Facebook, por exemplo, restringiu o conteúdo proveniente da mídia estatal russa em todo o mundo. Todavia, não foi o único: Google, Microsoft, Netflix, TikTok, Twitter, Youtube, entre outras, também adotaram medidas semelhantes. Moscou, por sua vez, proibiu o acesso a partir de seu território ao Facebook e ao Twitter (HAYS, 2022).

Dentre as estratégias de comunicação para controle de narrativa, os seguintes temas se sobressaem: possibilidade de encenação de danos colaterais relacionados a ataques russos, ataques à credibilidade da imprensa, ligação entre o governo ucraniano e ideais nazistas, ligação de refugiados ucranianos com grupos neonazistas, retirada de apoio ocidental à Ucrânia e repercussões negativas em torno

da crise energética na Europa (FAN, 2023). Cada um desse temas é veiculado de forma independente, e conta com os recursos supracitados para ganhar capilaridade.

García-Marin (2023) aponta que, no período compreendido pelos quatro primeiros meses de conflito, 83,74% das 326 imagens analisadas no Twitter e Facebook tinha contexto falso ou eram inventadas. Os dados obtidos podem ser analisados a partir da tabela abaixo:

	n	%
Forma de desinformar		
Falso contexto	206	63,19%
Conteúdo manipulado	30	9,20%
Suplantação de imagem	21	6,44%
Imitação	1	0,30%
Conteúdo inventado	67	20,55%
Narrativa		
Decisão/Ataque militar	92	28,22%
Reação da Comunidade internacional	41	12,57%
Resultados Militares	39	11,96%
Reação da população	62	19,01%
Decisões não militares	22	6,75%
Imagem de personalidade distorcida ou degrada	52	15,95%
Outras	18	5,52%
Intenção		
Pró-Rússia	160	49,07%
Pró-Ucrânia	146	44,78%
Neutro	20	6,13%
Plataforma		
Twitter	97	29,75%
Facebook	179	54,90%
Instagram	4	1,22%
Web/Blog	11	3,37%
TikTok	12	3,68%
TV	5	1,53%
Youtube	9	2,76%
Outras	8	2,45%
Formato		
Fotografia	168	51,53%
Vídeo	158	48,46%

Tabela 1: Uso de desinformação na Ucrânia
Fonte García-Marin, 2023.

Uma outra plataforma apontada como protagonista na disseminação de notícias falsas é o *Telegram*. Essa mídia social, extremamente popular, possui seus servidores sediados em território russo. Nesse contexto, o canal “*War On Fakes*”, possui de milhares de membros, se intitula “objetivo” e “imparcial” e afirma combater

a “guerra de informação lançada contra a Rússia”, porém tem veiculado material contraditório (FAN, 2023).

Adicionalmente, a plataforma *Sputnik* também serviu de palco para as operações de informação voltadas ao conflito russo-ucraniano. Segundo Jevtic (2022) que analisou cerca de 86 artigos dessa plataforma nos primeiros 100 dias de conflito, a Guerra de Informação Russa enfatiza a hostilidade das atividades da Rússia contra adversários. Nesse sentido, a informação serve como uma ferramenta para obtenção de vantagem em diversas expressões do poder.

Essa hostilidade relatada se constitui de padrões narrativos que procuram formar percepções. As narrativas procuram ser positivas acerca de aliados, demonizar os Estados Unidos da América (EUA), a União Europeia (UE) a OTAN e glorificar os feitos da Rússia como protetora da população moradora das regiões invadidas (JEVTIC, 2022).

Dessa forma, percebe-se a intensa relação entre a campanha de desinformação e a conquista de objetivos estratégicos russos em solo ucraniano. As técnicas utilizadas são diversificadas, exigindo um arcabouço de meios e tecnologias que possam tornar as ações ucranianas resilientes aos ataques sofridos em seu território.

5. IMPACTOS DOS INCIDENTES DE SEGURANÇA DA INFORMAÇÃO NA EXPRESSÃO MILITAR DO CONFLITO.

As atividades russas contra a Ucrânia no primeiro ano conflito levaram a uma série de reações no âmbito nacional e internacional do conflito. Aproveitando-se da escala que esses eventos tomaram, o governo ucraniano implementou uma série de medidas que serão elencadas a seguir. Nesse contexto, é importante lembrar que qualquer resposta a um incidente na segurança da informação pode variar dependendo da complexidade e da natureza dos ataques, bem como das considerações políticas e diplomáticas envolvidas.

Por motivos didáticos, essas ações serão classificadas dentro dos princípios da segurança da informação: prevenção, recuperabilidade e detecção. Paralelamente, será analisada a resposta à campanha informacional russa.

5.1 PREVENÇÃO E RECUPERABILIDADE

Como observado no capítulo anterior, as ações cibernéticas russas contra alvos em solo ucraniano não se iniciaram em 2022. Elas apenas se intensificaram nesse período, o que permitiu que a Ucrânia buscasse prevenir possíveis danos decorrentes de novos ataques (CÔRREA, 2023).

A principal medida observada, em resposta aos ataques russos, foi a manutenção de uma equipe de resposta a incidentes cibernéticos, materializada pelo *Computer Emergency Response Team of Ukraine* (CERT-UA). Como supracitado, o ciberataques russos contra a Ucrânia remetem ao período de invasão da Crimeia e anteriores. Isso propiciou uma preparação por parte do governo de Kiev que já sofria grande pressão nesse ambiente (GODINHO, 2023).

As defesas ucranianas passaram a contar com a intensa participação voluntária de grupos ou indivíduos nacionais. Essas ações, coordenadas via *telegram*, formaram o que o presidente Zelensky chamou de “exército de TI”. O apelo presidencial no sentido de recrutar esse exército foi fundamental para adesão de mais de 4.000 voluntários em 13 centrais espalhadas pela Europa Oriental. Dentre os grupos, destacam-se o NertWork Battalion 65, The Elves, The Cyber Partisans e o Anonymous (WILLETT, 2022).

Outra medida de vulto foi a utilização do apoio de grandes empresas privadas do ramo de tecnologia da informação, as *Big Techs*, a fim de reforçar defesas cibernéticas. Essas empresas investiram em tecnologias e equipes especializadas para mitigar futuros ataques e proteger infraestruturas críticas. A Ucrânia obteve significativa assistência vinda da Cisco, Google, Facebook e Microsoft (MUELLER, 2023). Essa última alega ter gastado cerca 239 milhões de dólares em financiamento e assistência técnica para monitorar atividades cibernéticas russas em 2022 (WILLETT, 2022).

Nesse contexto, cabe ressaltar o papel exercido pela empresa *Starlink*, associada à *SpaceX*, de Elon Musk, que ofertou acesso à internet satelital no território ucraniano. Isso veio a ocorrer logo após os ataques russos à *Viasat*, que paralisou inúmeros serviços de localização e comunicações via satélite no país. Por meio da *Starlink*, as forças atacadas puderam retomar a consciência situacional do conflito (MILLER e SCOTT, 2022).

Outro aspecto que auxiliou a Ucrânia a manter a disponibilidade de suas informações, foi o serviço em nuvem. Embora a Rússia tenha sido capaz de destruir *data centers* inteiros com ataques de mísseis de cruzeiro, a recuperabilidade dos dados foi alcançada com apoio da Amazon Web Services (AWS) e da empresa de segurança cibernética Cloudflare (PRINCE, 2022).

Segundo o vice-primeiro-ministro ucraniano e ministro da transformação digital, Mykhalio Fedorov, a Ucrânia foi capaz de “desembolsar sua infraestrutura digital na nuvem pública” e sobreviver aos ataques russos. A empresa de segurança cibernética Cloudflare, por sua vez, estendeu seus serviços do Projeto Galileo - um conjunto completo de proteção para organizações nas artes, direitos humanos, sociedade civil, jornalismo e promoção da democracia - para organizações importantes em toda a Ucrânia (TANGALAKIS-LIPPERT, 2022).

Ademais, as *Big Techs* buscaram reforçar as condutas já adotadas por meio da proteção comportamental. A proteção comportamental é um protocolo que identifica ameaças emergentes com base no comportamento dos arquivos. Ela detecta os códigos maliciosos antes que as definições de vírus estejam disponíveis para atualização e protege o usuário contra ameaças (NORTON, 2023).

A partir dessa prática, é possível categorizar as ameaças como de nível alto ou baixo de certeza com base em seus comportamentos. Inicialmente, a proteção

comportamental bloqueia ameaças com nível de certeza alto. Dessa forma, ainda que um usuário tenha um comportamento indesejado, é possível impedir que o ativo de informação manuseado seja comprometido.

Entretanto, a questão comportamental precisou extrapolar a defesa lógica de ativos. O comportamento dos combatentes precisou ser alterado dentro da dimensão informacional. Um exemplo claro disso decorreu de um ataque russo por meio de ações cinéticas contra as posições de homizio ucranianas após um soldado realizar a postagem de uma foto em sua rede social (O TEMPO, 2022).

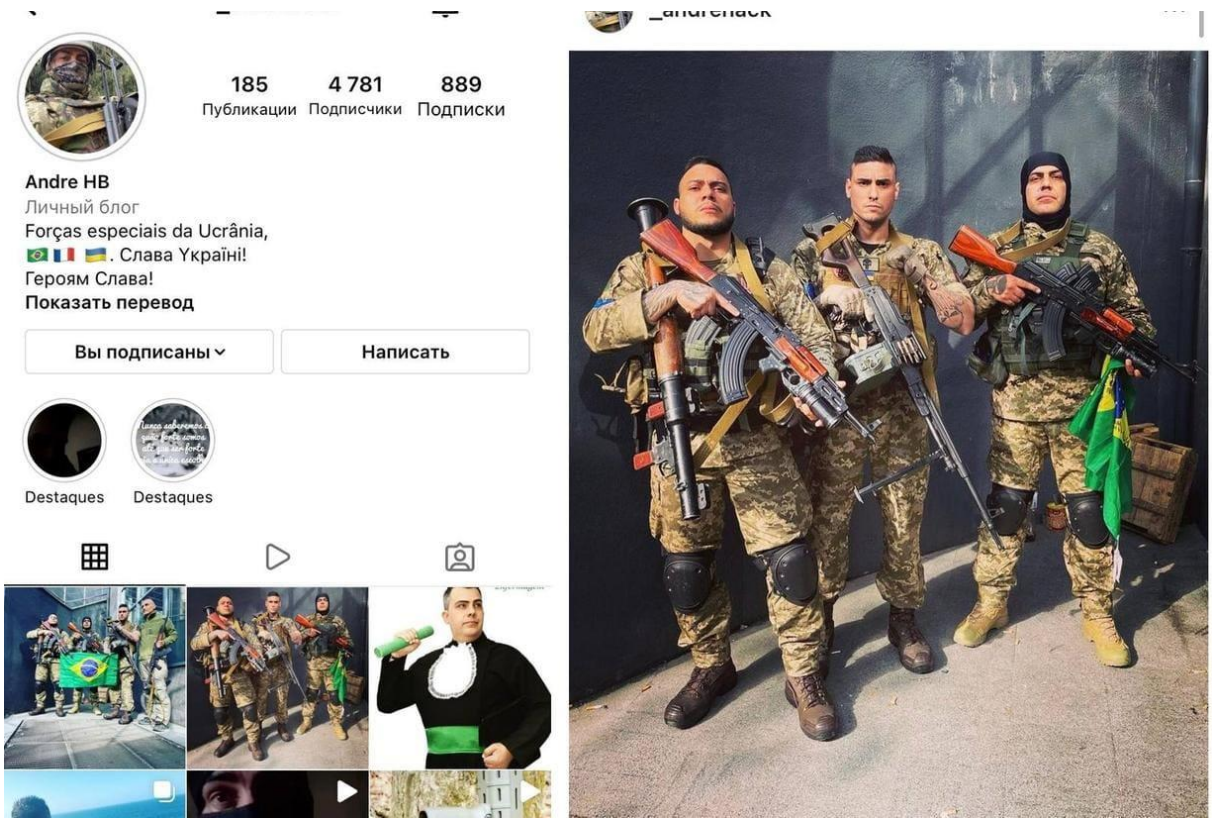


Figura 3 - Homem posta foto no Instagram como voluntário na guerra russo-ucraniana.
Fonte: O tempo, 2022.

A partir dos incidentes reportados, também foi necessária a implementação de medidas de segurança adicionais. Isso se deu pelo aumento da conscientização sobre segurança cibernética entre cidadãos e empresas envolvidas no conflito, incentivando práticas seguras na internet (DE SOUZA, 2019).

Outra forma inusitada de resposta cibernética foi a passagem à ofensiva: Dependendo da gravidade dos ataques, a Ucrânia optou por conduzir uma resposta

cibernética ofensiva contra alvos russos para dissuadir futuras agressões. Houve ocorrência de ataques DDoS generalizados e desfiguração de sites em alvos, incluindo o Kremlin, a estação de notícias estatal Russia *Today*, a agência de notícias estatal TASS e o site de hospedagem de vídeo RUTUBE (WILLET, 2022).

5.2 DETECÇÃO

A detecção dos ataques foi realizada por meio da investigação e atribuição de responsabilidade. Os órgãos ucranianos conduziram investigações para identificar a origem e os responsáveis pelos ataques cibernéticos e tornaram essas informações públicas para chamar a atenção internacional para o comportamento hostil da Rússia e seus grupos apoiadores. Essa medida ajudou o governo de Kiev a fomentar sua campanha informacional e angariar ou consolidar o apoio internacional necessário.

Uma das tecnologias empregadas da Ucrânia foi a conhecida *honeypot*, uma rede segregada e utilizada para atrair atacante. Essa rede facilita o monitoramento de suas atividades suspeitas e a identificação dos usuários. Uma *honeypot* de alta interação pode promover dados de até 3 meses quanto a possíveis invasores que se utilizam de acesso remoto para obter controle de sistemas. Além disso, os dados coletados, podem servir para análise estatística comportamental (FRAUNHOLZ et al, 2018).

Essa análise de parâmetros dos ataques pode revelar os agressores, tendências e novos vetores de ataque e tentativas de invasão. A partir de um monitoramento constante e metódico, é possível detectar o nível de habilidade do adversário, serviços utilizados, país de origem e IP do invasor. Os dados coletados foram analisados quanto a características que permitiram a classificação de tipos de atacantes e sessões. Tudo isso serve de base para novas medidas preventivas além de ajudar a imputar responsabilidade a criminosos cibernéticos. (MOROSOV, 2023).

Uma vez que a guerra começou, os EUA e o Reino Unido reforçaram o governo ucraniano com efetivas operações de inteligência, amparadas em ativos coletados antes do conflito. As estruturas *do Federal Bureau of Investigation* (FBI) dos EUA e *Cybersecurity and Technical Advice* possibilitaram o emprego de mais especialistas e provera, mais de 6750 dispositivos de emergência, como telefone satelitais e terminais

de dados (MARTIN, 2022). Essa infraestrutura se mostrou crítica para detecção de ameaças em setores como energia e telecomunicações (NUNES, 2023).

A detecção de ataques cibernéticos se tornou um problema legal na Ucrânia. O volume de ataques sem precedentes requereu um arcabouço legal mais robusto a fim de atender às demandas do país no tocante à segurança da informação. Nesse sentido, houve a abertura de canais diplomáticos e meios de comunicação para denunciar os ataques cibernéticos russos e chamar a atenção para o impacto negativo dessas ações (KHLAPONIN e DOLHOPOLOV, 2023).

Ademais, o governo de Kiev endureceu sua legislação a fim de responder aos ataques e imputar responsabilidades. Para tal, precisou especificar uma lista de setores de infraestrutura crítica, como energia, transporte, informação e comunicação, entre outros. Além disso, as novas leis exigem a formação de um sistema nacional para proteger infraestrutura crítica, incluindo o estabelecimento de uma entidade coordenadora e a adoção de planos de proteção setoriais (KHLAPONIN e DOLHOPOLOV, 2023).

Esta lei forma o Centro Nacional de Coordenação de Cibersegurança como a autoridade central responsável por coordenar os esforços de segurança cibernética em todo o governo e setores de infraestrutura. Também impõe várias responsabilidades na infraestrutura crítica operadoras, incluindo o desenvolvimento de políticas de segurança cibernética, implementação de segurança medidas e relatórios de incidentes cibernéticos (KHLAPONIN e DOLHOPOLOV, 2023).

As parcerias encontradas pela Ucrânia parecem ter funcionado como alternativa eficaz contra eventuais falhas na segurança de informação. A sinergia encontrada entre os ramos público e privado são sem precedentes nessa área e inferem o surgimento de uma nova forma de conduzir o combate convencional.

5.3 CAMPANHA INFORMACIONAL

Um dos possíveis fatores que contribuiu para que a ofensiva russa não tomasse Kiev nas primeiras semanas do conflito foi a inesperada figura de liderança atribuída ao presidente Volodymir Zelensky. Sua imagem passou e seu vinculada ao arquétipo do líder-herói, gerando um impacto nacionalista e motivacional em suas tropas e no mundo ocidental (ZACHARA-SZYMAŃSKA, 2023).

A construção dessa campanha foi feita desde a vestimenta utilizada por Zelensky, até o ângulo e cenário escolhido pelas mídias simpáticas à causa ucraniana. O terno deu lugar a camisas e calças leves, mais adequadas ao ambiente de combate, passando a impressão de que Zelensky acabara de sair do front. Paralelamente, o presidente foi fotografado diversas vezes cercado por carros de combate ou soldados, sempre centralizado, à frente e numa postura firme. Essa composição ajudou a solidificar o discurso ucraniano de nacionalismo em torno da campanha militar (SÁNCHEZ-CASTILLO, 2023).

Essa visibilidade no ocidente foi largamente utilizada para promover o discurso de financiamento, parcerias e associações a empresas privadas e intensa participação de civis, de forma voluntária, nas mais diversas áreas do conflito. Rapidamente, a guerra russo-ucraniana se tornou uma nova guerra por procuração, onde Estados aliados são as potências ocidentais (MORRIS, 2023).

Uma outra resposta já esperada da Ucrânia no campo informacional se desenvolveu em torno das associações, feitas pela Rússia, entre as condutas ucranianas e as nazistas. Além disso, Moscou buscou imputar a iniciativa da ofensiva à OTAN por meio de sua expansão para o leste. Isso tudo, buscou justificar a campanha liderada por Putin por meio da construção do heroísmo russo e o resgate de territórios e de sua população (JEVTIC, 2022).

A campanha ucraniana buscou a substituição de imagem construída por Putin. A proposta foi de suplantar a imagem de heroísmo pela salvação de pessoas e da nação russa, por uma campanha justificada pela aventura militar de um chefe norteado pelo próprio ego. O custo das operações e as condutas severas do próprio Putin em território russo também contribuíram para essa vertente informacional. A partir de seu engajamento, o presidente ucraniano pode expandir seu discurso no âmbito internacional e chegar até o território inimigo, enviando mensagens às mães russas e denunciando abusos ao público russo em geral.

Figura 5 – Técnicas de fotografia auxiliam a construir o mito do líder-herói em torno de Volodymir Zelensky
Fonte: www.president.gov.ua

Associados a isso, centenas de vídeos têm circulado em mídias sociais como TikTok e Facebook inspirados pela onda nacionalista e convocando indivíduos de maneira informal a participar das forças ucranianas. O próprio presidente Zelensky utilizou-se das mídias para a formação do “exército de TI” a fim de responder aos ataques cibernéticos russos. Esse cenário remete à conhecida “primavera árabe”, que também se utilizou dessas redes para coordenar e mobilizar pessoal (WILLETT, 2022).

A participação das redes sociais no conflito, entretanto, não se limitam à propaganda. Por meio delas, a população e as tropas têm acesso a vídeos em tempo real, veiculando campanhas que podem desequilibrar o combate. Como exemplo,

> as contas oficiais do Twitter da Ucrânia e de Kiev alavancaram suas plataformas online para vencer a guerra da opinião pública, transmitindo as atrocidades da guerra em tempo real, interagindo com outros países como uma forma de diplomacia pública digital e reunindo o público interno por meio de estratégias de mensagens de construção nacional (BOATWRIGHT, 2023).

As ações mais efetivas no combate à desinformação foram aquelas com apoio internacional, particularmente estado-unidense e inglês, para repetidamente expor as atividades híbridas do Kremlin. Essas ações não apenas ajudaram a ruir a narrativa russa como ajudaram a justificar as ações da OTAN, assegurando a tão almejada liberdade de ação esperada com a campanha informacional (BRANDT, 2022).

No meio dessa guerra informacional, os algoritmos de busca em mídias parecem ter adquirido maior proeminência. O Twitter, por exemplo, rebaixou ou não promoveu o conteúdo Sputnik e RT por meio de seu algoritmo. A Microsoft disse que seu mecanismo de busca Bing não enviará usuários ao conteúdo da mídia estatal russa, a menos que esteja claro que é para onde o usuário pretendia ir. O Google News disse que não apresentará mais o conteúdo de propaganda do Kremlin nas pesquisas de notícias. E o Facebook bloqueou totalmente o conteúdo da mídia estatal russa supostamente a pedido dos governos. Mais uma comprovação a importância das *Big Techs* no conflito.

Todas essas ações apontam para a possibilidade de que uma combinação inovadora do setor privado, coordenação estatal e doutrina emergente tenha tornado a defesa do domínio cibernético dominante. O emprego das tecnologias de empresas do ramo da informação com os serviços de inteligência nacionais e internacionais foram condicionantes para que a Ucrânia pudesse manter a capacidade de acessar o ciberespaço, a resistir a uma alta porcentagem de ciberataques russos destrutivos (MUELLER, 2023) e a resistir de modo equivalente à campanha informacional russa.

6. A ESTRUTURA MILITAR DE DEFESA BRASILEIRA VINCULADA Á SEGURANÇA DA INFORMAÇÃO.

A Estrutura Militar de Defesa do Brasil está completamente inserida e integrada à Estratégia Nacional de Defesa (END). Como tal, as atividades militares voltadas à segurança da informação buscam constante integração com outros órgãos nacionais a fim de minimizar riscos e maximizar os efeitos desejados.

Apesar de não estar diretamente envolvido no conflito russo-ucraniano, o Brasil é o segundo país no mundo a sofrer o maior número de ataques cibernéticos, o que infere a relevância desse assunto atualmente no âmbito nacional (ALVES, 2022). Diante disso, o esforço nacional em manter e desenvolver a segurança informacional tem sido constante e, ao mesmo tempo, desafiador. A seguir, observa-se o desenvolvimento e consolidação da Estrutura Militar de Defesa voltada à Segurança da Informação.

6.1 HISTÓRICO

A adequação da estrutura nacional voltada à segurança da informação no Brasil teve início no ano de 2000, quando o Decreto nº 3.505 deu instituiu a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal (APF) (BRASIL, 2000). No ano seguinte, ocorreu a atribuição ao Gabinete de Segurança Institucional da Presidência da República (GSI/PR) quanto à Segurança da Informação, por meio da Medida Provisória (MP) nº 2.216-37, de 31 de agosto de 2001 (BRASIL, 2001). A partir desse momento, procurou-se aperfeiçoar essa estrutura com a criação de novos setores e ampliação da interação entre eles.

Em 2006, o GSI/PR cria o Departamento de Segurança da Informação e Comunicações (DSIC) (BRASIL, 2006). Esse setor se mostra extremamente relevante quando, em 2008, a Estratégia Nacional de Defesa (END) estabeleceu a Defesa Cibernética como uma das três prioridades estratégicas do Brasil. A END também elencou que o caberia ao Exército Brasileiro (EB) a responsabilidade pela coordenação e integração do Setor Cibernético (BRASIL, 2008).

Com base nessa evolução, o EB ativou, em 2 de agosto de 2010, o Núcleo do Centro de Defesa Cibernética (BRASIL, 2010). Ainda nesse mesmo ano, o Decreto nº

7.411, de 29 de dezembro de 2010, normatizou que o DSIC – GSI/PR deveria coordenar e planejar as atividades de Segurança Cibernética e de Segurança da Informação no âmbito da Administração Pública Federal (APF). Nesse contexto, foi lançado, o Livro Verde - Segurança Cibernética no Brasil, explorando diretrizes para estabelecer a Política Nacional de Segurança Cibernética (BRASIL, 2010).

Consequentemente, em 2012, o Decreto Presidencial nº 7.809 institui o Centro de Defesa Cibernética na Estrutura Regimental do Comando do Exército. Apesar de subordinada ao Comando do Exército, essa nova estrutura recebeu, no mesmo ano, a responsabilidade de coordenar e integrar as atividades de Defesa Cibernética no âmbito do Ministério da Defesa (MD) (BRASIL, 2012).

Em 2013, a atualização da END e aprovação do Livro Branco de Defesa Nacional estabeleceram premissas para o setor cibernético que incluíram a necessidade de “pesquisa, capacitação, inteligência, doutrina, preparo, emprego operacional e gestão de pessoal”. Isso fomentou a ampliação do setor cibernético no contexto nacional, permitindo maior capilaridade e parcerias das estruturas governamentais com órgãos privados (BRASIL, 2013).

A partir de 2014, os eventos em torno da Comissão Parlamentar de Inquérito (CPI) da Espionagem alavancaram as ações governamentais em torno da segurança informacional. Com a urgência gerada nesse tema, o Tribunal de Contas da União foi consultado e apontou no Acórdão nº 3.051 a ausência de planejamento estratégico do Estado brasileiro em relação à Segurança da Informação (MORETTI, 2022). Nesse ano, o MD publicou o manual MD31-M-07, Doutrina Militar de Defesa Cibernética (BRASIL, 2014).

O ano de 2016, por sua vez deu espaço à CPI de Crimes Cibernéticos que demandou ao GSI/PR a Política Nacional de Segurança da Informação, entregue em maio do ano seguinte. Nessa impulsão, em 2018, duas normativas assinalaram uma grande evolução na estratégia nacional vinculada à segurança informacional: a aprovação da Política Nacional de Segurança de Infraestruturas Críticas (PNSIC), pelo Decreto nº 9.573 e a instituição da Política Nacional de Segurança da Informação (PNSI), no âmbito da Administração Pública Federal (BRASIL, 2018). Esses acontecimentos políticos no Brasil desencadearam, em 2020, os decretos nº 10.222 e nº 10.569 que aprovaram, respectivamente, a Estratégia Nacional de Segurança

Cibernética e a Estratégia Nacional de Segurança de Infraestruturas Críticas (BRASIL, 2020).

No início do ano de 2021, o Decreto nº 10.641 alterou o Decreto nº 9.637/2018, que instituiu o PNSI (BRASIL, 2021), apontando a finalidade da política em “assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação em âmbito nacional”. Em julho do mesmo ano, o Decreto nº 10.748 instituiu a Rede Federal de Gestão de Incidentes Cibernéticos, que tem por finalidade “aprimorar e manter a coordenação entre órgãos e entidades da administração pública federal direta, autárquica e fundacional para prevenção, tratamento e resposta a incidentes cibernéticos, de modo a elevar o nível de resiliência em segurança cibernética de seus ativos de informação” (BRASIL, 2021).

Todas essas evoluções asseguraram a regulamentação da Estrutura Nacional voltada à segurança da informação. Os órgãos federais são os responsáveis pela segurança informacional da APF e extrapolam essa esfera ao assegurar a confidencialidade, disponibilidade e integridade da informação em infraestruturas críticas.

Como consequência relevante nesse escopo, o Brasil subiu 53 posições e passou do 71º para o 18º lugar no Índice Global de Segurança Cibernética 2020, divulgado pela União Internacional de Telecomunicações (UIT) – agência especializada em tecnologias de informação e comunicação da Organização das Nações Unidas (ONU). Entre os países da América, o Brasil está na 3ª colocação, atrás somente dos Estados Unidos e do Canadá. Nesta edição do levantamento, 193 países foram pesquisados ao todo (BRASIL, 2022).

6.2 A ESTRUTURA NACIONAL DE SEGURANÇA DE INFORMAÇÃO

Como visto no tópico anterior, a Política Nacional de Segurança da Informação (PNSI) passou a normatizar as diretrizes do Estado Brasileiro nesse tema. No texto desse decreto, é possível identificar que essa política dar-se-á por meio dos seguintes instrumentos: a Estratégia Nacional de Segurança da Informação (ENSI) e o demais Planos Nacionais relacionados a cada órgão elencado na própria ENSI. A ENSI, por sua vez, é concebida pelos seguintes módulos: segurança cibernética (Seg Ciber), defesa cibernética (Def Ciber), segurança da informação sigilosa, segurança de

infraestruturas críticas e proteção contra vazamento de dados. A fim de facilitar esse entendimento, segue o quadro abaixo (BRASIL, 2018).

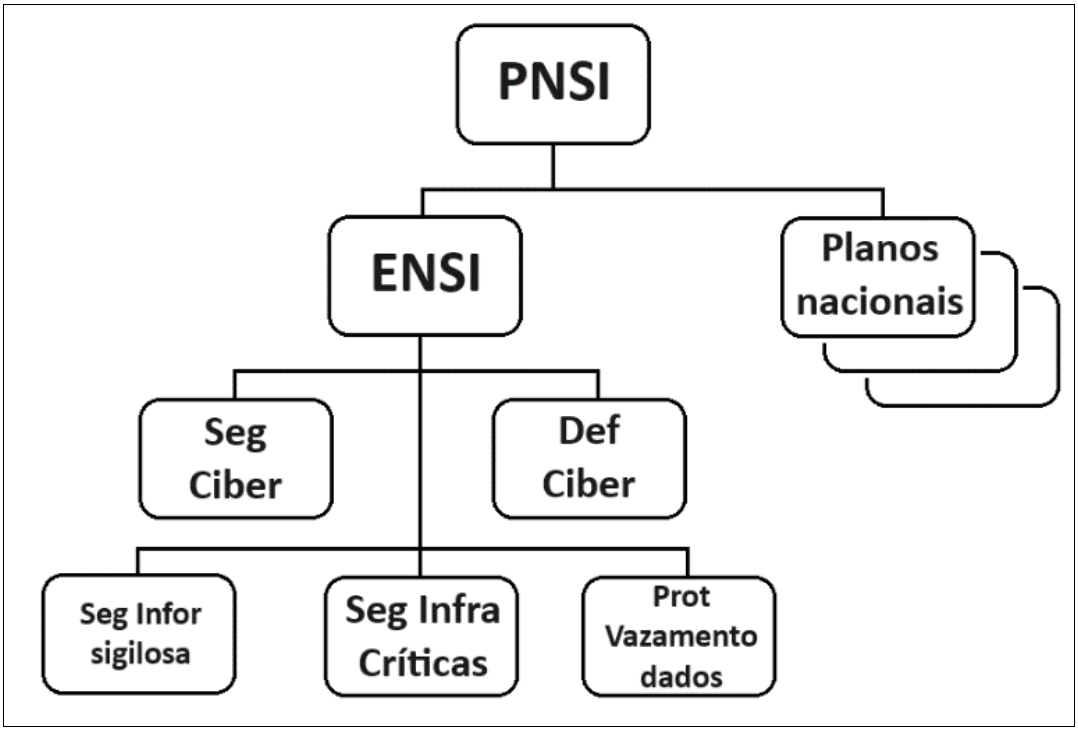


Figura 7 – Instrumentos e módulos da Política Nacional de Segurança da Informação
Fonte: o autor

A PNSI também estabelece o Comitê Gestor de Segurança da Informação que é composto por pelo menos um representante dos seguintes órgãos: GSI/PR, Casa Civil, Controladoria Geral da União (CGU), Secretaria Geral e de Governo da Presidência, Banco Central, Autoridade Nacional de Proteção de Dados e 17 ministérios. Essa norma ainda delega a competência ao GSI/PR

> para estabelecer norma sobre a definição dos requisitos metodológicos para a implementação da gestão de risco dos ativos da informação pelos órgãos e pelas entidades da administração pública federal (BRASIL, 2018, Art 12).

Além do GSI/PR, o outro órgão que protagoniza a Seg Infor no âmbito federal é o Ministério da Defesa por meio das Forças Armadas. Os objetivos e metas esperados foram descritos pelo GSI/PR na Estratégia de Segurança da Informação e Comunicações e de Segurança Cibernética da Administração Pública Federal e na Estratégia Nacional de Segurança Cibernética (E-Ciber). Esses documentos esclarecem que a estratégia do GSI é concebida em módulos, quais sejam: Subgrupo 1: Governança Cibernética; Pesquisa, Desenvolvimento e Inovação; Conscientização, Educação e Capacitação; Dimensão Internacional e

Parcerias Estratégicas; Subgrupo 2: Prevenção e Mitigação de Ameaças Cibernéticas e Confiança Digital; e Subgrupo 3: Proteção Estratégica - proteção do governo e proteção às infraestruturas críticas (BRASIL, 2019).

Nesse texto da E-Ciber, ressalta-se como objetivo:

> permitir a convergência dos esforços e de iniciativas, e atuar de forma complementar para receber denúncias, apurar incidentes e promover a conscientização e a educação da sociedade quanto ao tema. Para viabilizar a sua implementação, ficará a cargo do Gabinete de Segurança Institucional da Presidência da República a coordenação da segurança cibernética em âmbito nacional, que possibilite a atuação de modo amplo, cooperativo, participativo, e alinhado com as ações de defesa cibernética, a cargo do Ministério da Defesa. (BRASIL, 2020, p. 9)

Assim, é possível denotar que diversos órgãos da federação participam de forma direta ou indireta da Segurança da Informação do Estado brasileiro, seja como planejador, coordenador e até mesmo como auditor. Porém, está claro que o GSI/PR e o Ministério da Defesa desempenham papel protagonista nas ações de segurança e defesa dos ativos de informação do Brasil.

6.3 DOUTRINA MILITAR DE SEGURANÇA DA INFORMAÇÃO

Diante do supracitado, percebe-se que o Ministério da Defesa do Brasil constitui o principal órgão voltado para ações de defesa na área da Segurança da Informação, particularmente a Defesa Cibernética. Como apontado anteriormente, o Ministério da Defesa normatizou a Doutrina Militar de Defesa Cibernética por meio do Manual (MD31-M-08). Segundo esse manual:

> A Defesa Cibernética, por ser um dos componentes da Defesa Nacional, é missão das Forças Armadas (FA), conforme a legislação referenciada no capítulo I. Entretanto, as peculiaridades do Espaço Cibernético tornam impraticável o cumprimento dessa missão se não houver o comprometimento da sociedade como um todo, imbuída do sentimento de responsabilidade individual e coletiva pela proteção das infraestruturas críticas nacionais no Espaço Cibernético. (BRASIL, 2014, p. 25)

E ainda:

> O Setor Cibernético nacional envolve a atuação integrada de vários órgãos, sejam civis ou militares, cada um com atribuições específicas. Desta forma, o modelo de atuação cibernética mais provável para emprego em operações normalmente será o de operações em ambiente interagências. (BRASIL, 2014, p. 29)

A estruturação voltada para a Defesa Cibernética começa nos níveis de decisão desde o Tático ao Político, conforme figura abaixo:

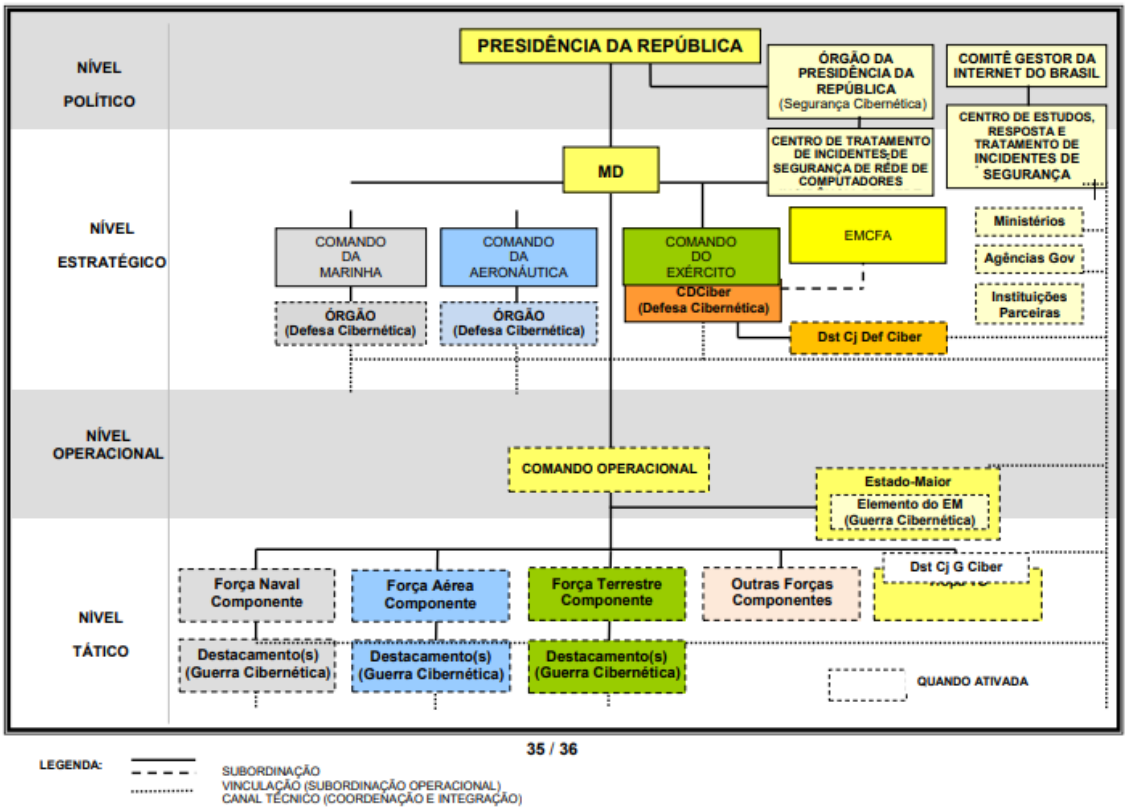


Figura 6 – Níveis decisórios na Estrutura Militar de Defesa Cibernética
Fonte: BRASIL, 2014

O Sistema Militar de Defesa Cibernética (SMDC), elencado pelo MD, confere ao Estado-Maior Conjunto das Forças Armadas (EMCFA) a competência para implantá-lo e geri-lo; e ao Centro de Defesa Cibernética (CDCiber) a competência para planejamento e controle centralizado das ações, operando de forma conjunta a fim de obter sinergia entre as forças e os órgãos civis. É interessante notar que:

> 3.3.5 O CDCiber mantém canal técnico para coordenação e integração com os órgãos de interesse envolvidos nas atividades de Defesa Cibernética (CERT.br, CTIR Gov, órgãos de Defesa/Guerra Cibernética das FA, Ministérios, Agências Governamentais, APF e outros). 3.3.6 O CDCiber mantém canal sistêmico/técnico com os órgãos centrais de inteligência das FA, no âmbito do Sistema de Inteligência de Defesa (SINDE), no tocante ao Setor Cibernético, para a difusão e obtenção dos dados obtidos por intermédio da Fonte Cibernética (BRASIL, 2014, p. 26).

Essa premissa indica a preocupação latente do Estado Brasileiro em manter constante integração de diversos setores militares e civis na defesa cibernética e consequente segurança da informação.

Esse mesmo manual aponta uma série de características voltadas à segurança cibernética. Dentre elas, destacam-se a Insegurança latente – “nenhum sistema computacional é totalmente seguro, tendo em vista que as vulnerabilidades nos ativos

de informação serão sempre objeto de exploração por ameaças cibernéticas” e o Alcance Global – “a Defesa Cibernética possibilita a condução de ações em escala global, simultaneamente, em diferentes frentes. Limitações físicas de distância e espaço não se aplicam ao Espaço Cibernético.” Esses dois aspectos ilustram a importância na manutenção de uma estrutura resiliente mesmo em tempos de paz (BRASIL, 2014).

Dessa forma, O SMDC fica assim escalonado dentro do Sistema Nacional de Segurança da Informação:

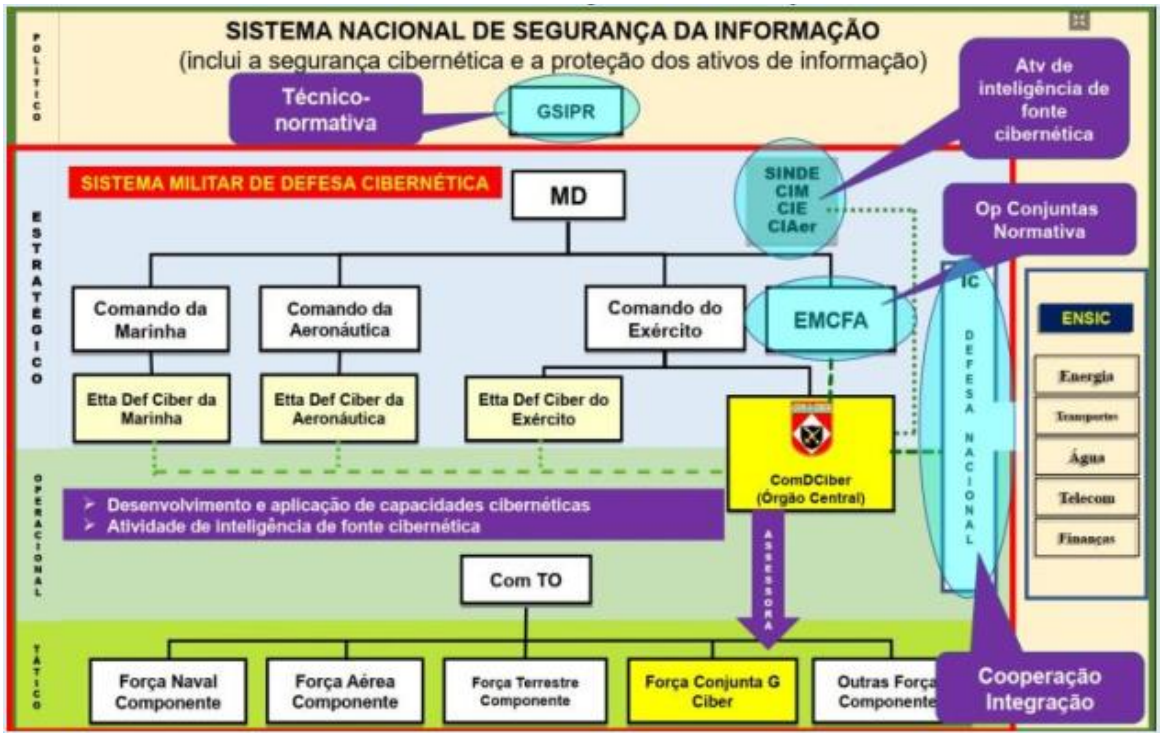


Figura 7 – Sistema Nacional de Segurança da Informação
Fonte: BRASIL, 2014

6.4 O SMDC NA PRÁTICA

Uma relevante iniciativa do SMDC é a implantação e operação de simuladores para capacitação e pesquisa na área. O Simulador Nacional de Operações Cibernéticas (SIMOC) surgiu para auxiliar na capacitação dos militares brasileiros para uma possível guerra cibernética. Ele faz parte da Estratégia de Defesa Nacional do Centro de Comunicações e Guerra Eletrônica do Exército (CComGEx), o que permite planejar e criar treinamentos em um ambiente de rede (DA SILVA e NOGUEIRA, 2019).

Todo esse esforço se apoia nos princípios da confidencialidade, integridade e disponibilidade. Esses princípios de extrema importância quando se considera que eventuais ataques cibernéticos podem interromper o acesso de informações indispensáveis e relevantes para os usuários autorizados. Diante disso, algumas ferramentas são indicadas para conferir disponibilidade e integridade aos sistemas informacionais, como, por exemplo, o *Nobreak*, o *Firewall* e os *backups* (MORETTI, 2022).

Os *Nobreaks* são dispositivos eletrônicos que fornecem uma fonte de alimentação de eletricidade de modo alternativo à fonte principal e visam proteger todos os ativos de TI em casos de queda ou surtos de energia (FERREIRA e BARRETO, 2018). Eles são essenciais para manter a atividade regular das infraestruturas críticas brasileiras. O Governo Federal já faz uso da tecnologia em alguns de seus setores críticos, como na Agência Nacional de Transportes Terrestres (ANTT) (MORETTI, 2022). Os sistemas militares utilizam-se de fontes alternativas baseadas em *nobreaks* e geradores a fim de conferir redundância para a alimentação desses sistemas.

Já o *Firewall* serve como uma barreira para impedir ataques que podem atrapalhar o normal funcionamento dos sistemas, ou seja, é um sistema concebido para impedir acessos não autorizados a ou de uma rede privada. (RASH, 2007). Frequentemente utilizado para impedir o acesso de utilizadores da Internet a redes privadas, os *firewalls* já são largamente utilizados no âmbito das Forças Armadas, em particular no EB, por meio dos Centros de Telemática de Área (CTA) em tempos de paz (BRASIL, 2023).

Em situações de emprego operacional, esse recurso é utilizado pelas unidades e subunidades de Comunicações, por meio do Módulo de Proteção Cibernética (MPC).

> O MPC é constituído de hardware e software capazes de incrementar a proteção cibernética por meio do (a): robustecimento da capacidade operativa cibernética da Força Terrestre; diminuição da possibilidade de interceptação de tráfego de dados; monitoramento e controle de vulnerabilidades em redes de Comunicações; e mitigação de ataques cibernéticos (BRASIL, 2022).

Os Backups, por sua vez, são cópias de segurança de dados de um dispositivo de armazenamento a outro para que possam ser restaurados em caso da perda dos originais, o que pode envolver apagamentos acidentais ou corrupção de dados (FONTES, 2017). Essa é uma prática recomendada pelos CTA e implementadas por meio da doutrina e adestramento de todas as tropas envolvidas no ambiente cibernético.

Diante dos princípios da confidencialidade e integridade, as práticas vão desde uso regular de senhas até os certificados digitais conferidos pelas Autoridades Certificadoras (AC). Por meio da E-Ciber, o Governo Federal reconhece a importância da utilização correta de ferramentas que buscam garantir a segurança das informações, dando destaque para os certificados digitais.

> Esses certificados garantem o compartilhamento seguro: conjunto de dados de computador, gerados por uma autoridade certificadora, em observância à recomendação internacional ITU-T X.509 que se destina a registrar, de forma única, exclusiva e intransferível, a relação existente entre uma chave criptográfica e uma pessoa física, jurídica, máquina ou aplicação (MORETTI, 2022).

O certificado é uma forma de verificar a autenticidade de documentos eletrônicos, uma vez que “com ele, é possível garantir de forma inequívoca a identidade de um indivíduo ou de uma instituição, sem uma apresentação presencial” (BRASIL, 2020), o que é realizado por uma criptografia complexa. No âmbito da Defesa, o Brasil conta com AC exclusiva para tal, a AC Defesa que tem por missão “emitir e fornecer certificados digitais para o Ministério da Defesa (MD), bem como para as três Forças: Marinha do Brasil (MB), Exército Brasileiro (EB) e Força Aérea Brasileira (FAB)” (BRASIL, 2023).

Outras iniciativas também foram tomadas no contexto da Defesa, como as parcerias com entidades nacionais e internacionais. Em 2017, foi assinado acordo com a Fundação Parque Tecnológico Itaipu (FPTI) e o EB em 2017, esse acordo trata sobre cooperação mútua no Laboratório de Segurança Eletrônica, de Comunicações e Cibernética que funciona desde 2015 no Complexo Hidrelétrico de Itaipu (BRASIL, 2017).

No quesito capacitação, o EB conta com a Escola Nacional de Defesa Cibernética (ENaDCiber), do Comando de Defesa Cibernética (CD Ciber), o Centro de Instrução de Guerra Eletrônica (CIGE) e a Escola de Comunicações (EsCom),

ambas do Comando de Comunicações e Guerra Eletrônica do Exército (CComGEx) para a formação de quadros na área cibernética (BRASIL, 2023). Vale ressaltar que a ENaDciber tem o viés de formação de quadros dentro e fora das Forças Armadas.

Ademais, buscou integrar o esforço de defesa por meio de parcerias com empresas privadas, como aquelas sediadas no Porto Digital em Recife-PE, para o desenvolvimento de soluções voltadas à Segurança da Informação (PERNAMBUCO, 2019). Nesse sentido, o EB conduz Estágio Internacional de Defesa Cibernética com o objetivo de trocar conhecimentos com países que mantêm relações com o Brasil (BRASIL, 2018c) e mantém parcerias internacionais junto à Polícia Federal do Brasil, integrando o sistema global de comunicações policiais I-24/7 desenvolvido pela Interpol para conectar policiais, incluindo crimes cibernéticos (ITU, 2017).

Infere-se que todas as iniciativas do Estado Brasileiro estão atualizadas com o atual panorama de incerteza e desafios ligados à Segurança da Informação. As políticas públicas são robustas e integradas a fim de prover ao país a segurança proporcional a suas dimensões e relevância no Contexto internacional.

7. CONCLUSÃO

O presente trabalho teve como objetivo principal analisar os impactos dos principais incidentes relacionados à segurança da informação ocorridos ao longo do primeiro ano do conflito russo-ucraniano. Para isso forma elencados alguns objetivos intermediários como: identificar eventos ocorridos no conflito russo-ucraniano relacionados à segurança da informação; identificar os impactos desses eventos no primeiro ano conflito, particularmente em condutas militares ucranianas relacionadas à segurança da informação; e relacionar condutas militares ucranianas supracitadas com práticas relacionadas à segurança da informação adotadas no Brasil.

Foi possível observar que as ações russas indicam um faseamento que sicroniza as ações de quebra de segurança da informação, uso de propaganda no campo informacional e a manobra física no campo de batalha. Essas ações sincronizadas inferem a intenção russa em obter superioridade na manobra física pela legitimidade e liberdade de ação relacionadas às Operações de Informação e à capacidade de inteligência relacionada às Operações Cibernéticas.

Nesse contexto, a Ucrânia precisou reagir. As ações ucranianas também priorizaram os campos de atuação do ofensor, quais sejam o cibernético e o informacional. Nesse sentido, a campanha informacional em torno da imagem do presidente Zelensky foi primordial para agregar poder ao campo cibernético. Isso se deveu às parcerias alcançadas com países ocidentais, empresas de grande porte na área de TI, as *Big Techs*, e a alta capacidade de mobilização da população em torno desse tema.

Diante desse panorama, buscou-se investigar as iniciativas e estruturas brasileiras voltadas para a segurança da informação a fim de verificar possíveis vulnerabilidades e seu alinhamento ao atual contexto de conflito envolvendo a dimensão informacional. Como resultado, verificou-se que o Estado Brasileiro apresenta uma estrutura bem organizada e integrada aos diversos órgãos públicos e privados. Essa estratégia, normatizada na END, se desdobra em todo o território nacional e confere resiliência cibernética, além de promover a continuada pesquisa voltada à segurança da informação em prol da Defesa.

O trabalho serve de subsídio para pesquisas futuras que tenham como tema a segurança da informação, uma vez que essa capacidade foi incluída no Plano Estratégico do Exército 2020-2023, o Objetivo Estratégico do Exército Nr 7: Aprimorar

a gestão estratégica da informação. Esse objetivo se ramifica em outro dois, quais sejam: 7.2 - reorganização do sistema de informação do Exército; 7.2.1 - aperfeiçoar a gestão da informação organizacional do Exército e 7.2.1.2 - otimizar e racionalizar a produção de sistemas de informação. Todos esses objetivos alinham-se com o esforço nacional de aprimorar a segurança da informação.

A principal limitação do método se deu pela grande dificuldade de selecionar fontes seguras para a obtenção de dados, fruto da natureza da Guerra Informacional. Isso implicou a necessidade de intensa confrontação de informações, a fim de agregar credibilidade ao dado em estudo. Outra limitação se deveu ao fato de que a análise desses dados revestiu-se de caráter parcial, particularmente pelo fato do conflito estar em desenvolvimento e seu desfecho ser imprevisível, o que insufla a necessidade da continuidade de estudo em torno desse tema.

Por fim, a segurança informacional é condição *sine qua non* para a Defesa, desde os níveis mais altos de política até o nivel tático. A Estrutura Militar voltada para a segurança informacional está alinhada com a conjuntura atual de conflitos imersos nos campos cibernéticos e informacional. Essa estrutura propricia ao Estado Brasileiro o desenvolvimento de doutrina e capacidade autóctones, fundamentais para a manutenção da soberania nacional.

REFERÊNCIAS

ABBANY, Zulfikar. **Ukraine: Cyberwar creates chaos, 'it won't win the war'.** Deutsche Welle, 03 mar. 2022. Disponível em: <https://p.dw.com/p/47wg1>. Acesso em: 04 mar. 2022.

ALVES, Dafne. **Ataques cibernéticos ao Brasil: levantamento sistemático dos últimos dez anos (2010–2020**). 2022.

ALVES, Renato. **Fotos de voluntários brasileiros na Ucrânia facilitariam ataques russos.** O Tempo, 15 de março de 2022. Disponível em: <https://www.otempo.com.br/politica/fotos-de-voluntarios-brasileiros-na-ucrania-facilitariam-ataques-russos-1.2633419>. Acesso em 10 Mar. 2023.

APARECIDO, Julia Mori; AGUILAR, Sergio Luiz Cruz. **A Guerra entre a Rússia e a Ucrânia.** Série Conflitos Internacionais, v. 9, n. 1, 2022.

BARDIN, Laurence. **Análise do conteúdo**, 3ª. Lisboa: Edições, v. 70, 2004.

BETHLEM, Agrícola. **Os conceitos de política estratégica**. Revista de administração de empresas, v. 21, p. 7-15, 1981.

BLACK, Dan; RONCONE, Gabby. JUL 12, 2023. **The GRU's Disruptive Playbook**. Disponível em: <https://www.mandiant.com/resources/blog/gru-disruptive-playbook>. Acesso em 15 de jul. 2023.

BRANDT, Jessica; PITA, Adrianna. How is Russia conducting cyber and information warfare in Ukraine? 2022.

BRASIL. Exército. Estado-Maior. **Caderno de Instrução Medidas de Proteção Eletrônica.** EB70- CI-11.403. 1ª Ed. Brasília, DF: Estado-Maior do Exército, 2014.

_____. **Decreto nº 10.222, de 05 de fevereiro de 2020**. Aprova a Estratégia Nacional de Segurança Cibernética. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10222.htm>. Acesso em: 17 ago. 2023.

_____. **Decreto nº 10.569, de 09 de dezembro de 2020**. Aprova a Estratégia Nacional de Segurança de Infraestruturas Críticas. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2020. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/decreto/D10569.htm>. Acesso em: 17 ago. 2023.

_____. **Estratégia Nacional de Segurança da Informação**. Gabinete de Segurança Institucional, 2019. Disponível em: <https://www.gov.br/gsi/pt-br/centrais-de-conteudo/noticias/2019/estrategia-nacional-de-seguranca-da-informacao-ensi>. Acesso em: 03 ago. 2023.

_____. **Portaria Nº 3.781/GM-MD, de 17 de novembro de 2020**. Cria o Sistema Militar de Defesa Cibernética (SMDC) e dá outras providências. Minist[erio da Defesa, Gabinete do ministro, 2020. Disponível em: <https://sintse.tse.jus.br/documentos/2020/Nov/19/diario-oficial-da-uniao-secao-1/portaria-no-3-781-de-17-de-novembro-de-2020-cria-o-sistema-militar-de-defesa-cibernetica-smdc-e-da-o>. Acesso em: 20 ago. 2023.

_____. **Decreto nº 10.641, de 02 de março de 2021**. Altera o Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o , que regulamenta o disposto no art. 24, caput , inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2021. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10641.htm>. Acesso em: 17 ago. 2023.

_____. **Decreto nº 10.748, de 16 de julho de 2021**. Institui a Rede Federal de Gestão de Incidentes Cibernéticos. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2021. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/decreto/D10748.htm. Acesso em: 17 ago. 2023.

_____. **Medida Provisória nº 2.216-37, de 31 de agosto de 2001**. Altera dispositivos da Lei nº 9.649, de 27 de maio de 1998, que dispõe sobre a organização da Presidência da República e dos Ministérios, e dá outras providências. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/2216-37.htm>. Acesso em: 10 ago. 2023.

_____. **Decreto Nº 5.772, de 8 de maio de 2006.** Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República, e dá outras providências. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/2216-37.htm>. Acesso em: 10 ago. 2023.

_____. **Decreto Nº 6.703, de 18 de dezembro de 2008**. Aprova a Estratégia Nacional de Defesa, e dá outras providências. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2008. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2007-2010/2008/decreto/d6703.htm>. Acesso em: 10 ago. 2023.

_____. **Portaria Nº 666, de 4 de agosto de 2010.** Cria o Centro de Defesa Cibernética do Exército e dá outras providências. Comandante do Exército, 2010. Disponível em: <http://www.sgex.eb.mil.br/sistemas/boletim_do_exercito/copiar.php?codarquivo=824&act=bre>. Acesso em: 10 ago. 2023.

_____. Exército Brasileiro. **Cooperação internacional e defesa cibernética atuam juntos para o enfrentamento das ameaças dessa natureza.** Noticiário do Exército. Brasília: 14 mai. 2018c. Disponível em: <http://www.eb.mil.br/web/noticias/noticiario-do-exercito/-/asset_publisher/MjaG93KcunQI/content/cooperacao-internacional-e-defesa-cibernetica-atuam-juntos-para-enfrentamento-das-ameacas-dessa-natureza->. Acesso em: 14 ago. 2023.

_____. Exército Brasileiro. **Centro integrado de Telemática do Exército.** 2023. Disponível em: <https://citex.eb.mil.br/>. Acesso em: 14 ago. 2023.

_____. **Decreto nº 7.411, de 29 de dezembro de 2010**. Dispõe sobre remanejamento de cargos em comissão do Grupo-Direção e Assessoramento Superiores - DAS, aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Gratificações de Exercício em Cargo de Confiança do Gabinete de Segurança Institucional da Presidência da República; altera o Anexo II do Decreto nº 7.063, de 13 de janeiro de 2010, e dá outras providências. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2010. Disponível em: <planalto.gov.br/ccivil_03/_ato2007-2010/2010/decreto/D7411.htm>. Acesso em: 17 ago. 2023.

_____. **Decreto nº 3.505, de 13 de junho de 2000**. Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2000. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto/D3505impressao.htm>. Acesso em: 14 ago. 2023.

_____. **Decreto nº 9.573, de 22 de novembro de 2018.** Aprova a Política Nacional de Segurança de Infraestruturas Críticas. Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm. Acesso em: 17 mar. 2022. BRASIL. Decreto nº 9.637, de 26 de dezembro de 2018. Institui a Política Nacional de Segurança da Informação, dispõe sobre a governança da segurança da informação, e altera o Decreto nº 2.295, de 4 de agosto de 1997, que regulamenta o disposto no art. 24, caput, inciso IX, da Lei nº 8.666, de 21 de junho de 1993, e dispõe sobre a dispensa de licitação nos casos que possam comprometer a segurança nacional. Brasília, Presidência da República, Secretaria-Geral, Subchefia para Assuntos Jurídicos, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9637.htm>. Acesso em: 14 ago. 2023.

_____. Gabinete de Segurança Institucional da Presidência da República. **Portaria nº 45, de 8 de setembro de 2009**. Institui, no âmbito da Câmara de Relações Exteriores e Defesa Nacional (CREDEN), o Grupo Técnico de Segurança Cibernética e dá outras providências. Brasília, 2009. Disponível em: <https://www.legisweb.com.br/legislacao/?id=213726>. Acesso em: 14 ago. 2023.

BRASIL. **Medida Provisória nº 2.200-2, de 24 de agosto de 2001**. Institui a InfraEstrutura de Chaves Públicas Brasileira – ICP-Brasil, transforma o Instituto Nacional de Tecnologia da Informação em autarquia, e dá outras providências.

Disponível em: <http://www.planalto.gov.br/ccivil_03/mpv/antigas_2001/2200-2.htm>. Acesso em: 03 set. 2023.

_____. Presidência da República. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. **Livro Verde: segurança cibernética no Brasil**. Gabinete de Segurança Institucional, Departamento de Segurança da Informação e Comunicações; organização Claudia Canongia, Admilson Gonçalves Júnior e Raphael Mandarino Junior. – Brasília: GSIPR/SE/DSIC, 2010. Disponível em: <https://www.bibliotecadeseguranca.com.br/wpcontent/uploads/2015/10/Livro_Verde_SEG_CIBER.pdf>. Acesso em: 03 ago. 2023.

_____. Tribunal de Contas da União (Plenário). **Acórdão nº 3.051/2014. Processo nº TC 023.050/2013-6**. Relator Ministro-Substituto Weder de Oliveira, 5 de novembro de 2014. Disponível em: <https://www.cjf.jus.br/publico/biblioteca/Acord%C3%A3o%2030512014.pdf>. Acesso em: 30 ago. 2023.

_____. **Decreto Nº 7.809, de 20 de setembro de 2012.** Altera os Decretos nº 5.417, de 13 de abril de 2005, nº 5.751, de 12 de abril de 2006, e nº 6.834, de 30 de abril de 2009, que aprovam as estruturas regimentais e os quadros demonstrativos dos cargos em comissão e das funções gratificadas dos Comandos da Marinha, do Exército e da Aeronáutica, do Ministério da Defesa. Presidência da República, Casa Civil, Subchefia para Assuntos Jurídicos, 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/decreto/d7809.htm#:~:text=Altera%20os%20Decretos%20n%C2%BA%205.417,Aeron%C3%A1utica%2C%20do%20Minist%C3%A9rio%20da%20Defesa>. Acesso em: 17 ago. 2023.

_____. Ministério da Defesa. MD31-M-07 - **Doutrina militar de defesa cibernética.** 1. ed. Brasília, DF: Estado-Maior Conjunto das Forças Armadas, 2014.

_____. **Brasil sobe 53 posições no Índice Global de Segurança Cibernética**. Atualizado em 31/10/2022. Disponível em: <https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/07/brasil-sobe-53-posicoes-no-indice-global-de-seguranca-cibernetica#:~:text=O%20Brasil%20subiu%2053%20posi%C3%A7%C3%B5es,das%20Na%C3%A7%C3%B5es%20Unidas%20(ONU)>. Acesso em: 11 ago. 2023.

_____. Ministério da Defesa. Comando Militar do Sul, 3º Batalhão de Comunicações. **Capacitação do Módulo De Proteção Cibernética**. Dez, 2022. Disponível em: <https://3bcom.eb.mil.br/index.php/entrega-do-mpc-a-todas-as-om-de-comunicacoes-do-cms-e-conferencia-do-material#portal-siteactions>. Acesso em: 15 ago. 2023.

_____. Ministério da Defesa Exército Brasileiro Departamento de Educação e Cultura do Exército. **Catálogo de Curso e Estágios. 2023** Disponível em: <https://www.decex.eb.mil.br/images/2022/catalogo_de_cursos_2022.pdf>. Acesso em: 15 set. 2023.

_____. Exército. Estado-Maior. **Operações de Informação**. EB70- MC-10.213. 2ª Ed. Brasília, DF: Estado-Maior do Exército, 2015.

_____. Exército. Comando de Operações Terrestres. **Operações**. EB70-MC-10.223. 5ª Ed. Brasília, DF: COTER, 2017.

_____. Decreto nº 9.573, de 22 de novembro de 2018. **Aprova a Política Nacional de Segurança das Infraestruturas Críticas.** Diário Oficial da União, Brasília, DF, 23 nov. 2018a. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/decreto/D9573.htm>. Acesso em: 14 ago. 2023.

_____. Ministério da Defesa Nacional. **Estratégia Nacional de Defesa**, 2021.

BOATWRIGHT, Brandon C.; PYLE, Andrew S. "Don't Mess with Ukrainian Farmers": An examination of Ukraine and Kyiv's official Twitter accounts as crisis communication, public diplomacy, and nation building during Russian invasion. **Public Relations Review**, v. 49, n. 3, p. 102-338, 2023.

CAMPATO JR, João Adalberto. **A Guerra Russo-ucraniana e os discursos sobre o imperialismo da nova desordem mundial.** Revista Eletrônica de Estudos Integrados em Discurso e Argumentação, v. 22, n. 1, p. 82-102, 2022.

CANZANESE, Ray. **Lições prendidas após um ano do ciberguerra russo-ucraniana, 2023**. Disponível em: <https://www.securityreport.com.br/licoes-aprendidas-apos-um-ano-de-ciberguerra-russo-ucraniana> Acesso em: 20 de jul. 2023.

CEPIK, Marco. **Inteligência e Políticas Públicas: dinâmicas operacionais e condições de legitimação.** Security and Defense Studies Review, v. 2, n. 2, p. 246-267, 2002.

CERT-UA. **Fraude online usando o assunto "compensação monetária", 2022**. Disponível em: <https://cert.gov.ua/article/761668>. Acesso em : 17 de jul. de 2023.

CONCEIÇÃO, Marcelo Eduardo de Souza. **Ataques cibernéticos perpetrados na atualidade e os possíveis impactos para as OMs do Exército Brasileiro.** 2017.

CORRÊA, Fernanda das Graças. **Guerra russo-ucraniana: grande laboratório para ensaios destrutivos e não destrutivos de tecnologias emergentes e disruptivas.** Centro de Estudos Estratégicos do Exército: Análise Estratégica, v. 28, n. 1, p. 47-58, 2023.

COSTA, Maria Gabriela. **As raízes da guerra: Rússia e Ucrânia. Observatório da Democracia no Mundo (ODEC-USP).** Disponível em: <http://odec. iri. usp. br/analises/as-raizes-da-guerra-russia-e-ucrania% EF% BF% BC/>. Acesso em: 14 ago. 2023.

COSTA, Rodrigo Barbosa Bastos; DEJOUR, Matthieu. **Ensinamentos do Conflito Ucrânia-Rússia** para a revisão da Política Nacional de Defesa do Brasil. 2022.

DA SILVA, Washington Rodrigues; NOGUEIRA, Jorge Madeira. Ataques cibernéticos e medidas governamentais para combatê-los. **O Comunicante**, v. 9, n. 1, p. 42-57, 2019.

DE SOUZA, Deywisson Ronaldo Oliveira et al. Guerra híbrida e ciberconflitos: uma análise das ferramentas cibernéticas nos casos da síria e conflito rússia-ucrânia. **Revista Eletrônica da Estácio Recife**, v. 5, n. 3, 2019.

DUARTE, Mariana. **Ucrânia vs Rússia: Guerra de Informação**. The Trends Hub, n. 2, 2022.

FAN, Ricardo. **Um ano de desinformação sobre a guerra na Ucrânia**, 17 de fev de 2023. Disponível em: <https://www.defesanet.com.br/geopolitica/noticia/1047916/um-ano-de-desinformacao-sobre-a-guerra-na-ucrania/>. Acesso em: 20 de jul. 2023.

FONTES, Edison Luiz Gonçalves. **Segurança da informação**. Saraiva Educação SA, 2017.

FONTES, Eduardo. **Segurança da Informação: o usuário faz a diferença**. São Paulo, Saraiva, 2006.

FONSECA, Leila Oliveira da. **A guerra cibernética e o conflito Rússia versus Ucrânia, 2023.** Disponível em: <https://relacoesexteriores.com.br/a-guerra-cibernetica-e-o-conflito-russia-versus-ucrania/>. Acesso em 15 de jul. 2023.

FRAUNHOLZ, Daniel et al. Introducing FALCOM: A multifunctional high-interaction honeypot framework for industrial and embedded applications. In: **2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)**. IEEE, 2018. p. 1-8.

FURLANETTO, Tiago Murer et al. **Segurança da informação nas cadeias de suprimentos de saúde: uma análise das práticas críticas de proteção de informações.** Gestão & Produção, v. 27, 2020.

GARCÍA-MARÍN, David et al. Desinformación y guerra. Verificación de las imágenes falsas sobre el conflicto ruso-ucraniano. **Revista ICONO 14. Revista científica de Comunicación y Tecnologías emergentes**, v. 21, n. 1, 2023.

GARNETT, Sherman. **Keystone in the Arch: Ukraine in the Emerging Security Environment of Central and Eastern Europe**. Washington, Brookings Institution Press. 1997.

GODINHO, Lilian Dill Donati et al. **Ciberterrorismo: a nova guerra fria?** 2023. Dissertação de Mestrado.

GRAÇA, Joana Rita Pedralva. **O espaço dos media digitais como ambiente de promoção da consciencialização social: o caso da invasão da Ucrânia**. 2022. Tese de Doutorado.

GREENBERG, Karl. **With political 'hacktivism' rising, Google offers Project Shield to fight DDOS attacks**. Tech Republic, 28 de Mar. 2023. Disponível em: <https://www.techrepublic.com/article/googlelaunches-project-shield/>. Acesso em: 7 jul. 2023.

HAYS, Kali. **Facebook demotes Russian state media across its platforms worldwide.** Business Insider, 01 de mar. 2022. Disponível em: <https://www.businessinsider.com/facebook-ukraine-russia-news-state-media-2022-3>. Acesso em: 14 ago. 2023.

HOBBES, Thomas. **Leviatã**. São Paulo. Abril Cultural, 1988.

INSIKT GROUP, 2023. **Threat analysis, Recorded Future, 2023.** Disponível em: <https://go.recordedfuture.com/hubfs/reports/ta-2023-0209.pdf>. Acesso em 15 de jul. de 2023.

INTERNATIONAL TELECOMMUNICATION UNION (ITU). **Global Cybersecurity Index 2017.** Genebra: 2017. ISBN: 978-92-61-25071-3. Disponível em: <https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf>. Acesso em: 14 ago. 2023.

JEVTIC, Jelena. **Russian information operations via Sputnik Srbija: The case study of Russia-Ukraine war**. 2022.

JOSEPHS, J. **Por que Banco Mundial prevê pior choque de preços em 50 anos?** BBC, 27 de abril de 2022. Disponível em: <https://www.bbc.com/portuguese/internacional-61238851>. Acesso em: 14 jul. 2023.

JOTA, Lucas Machado Guimarães et al. **A Informação como Elemento de Difusão de Poder no Espaço Cibernético: o uso da inteligência de fontes abertas (OSINT) no conflito entre Rússia e Ucrânia**. 2022.

JÚNIOR, Ferreira; MACEDO, Eurésio. **Utilização de tecnologias de segurança das comunicações nos rádios HARRIS MPR 9600 pelas organizações militares de comunicações: proposta de implementação de medidas para planejamento e emprego em operações.** 2019.

KANTOLA, Harry. **Categorizing Cyber Activity Through an Information-psychological and Information-technological Perspective, Case Ukraine**. In: International Conference on Cyber Warfare and Security. 2023. p. 480-488.

KARSPERSKY, 2023. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/ddos-attacks>. Acesso em 15 de jul. 2023.

KHLAPONIN, Yurii; DOLHOPOLOV, Serhii. Legislative support for the protection of critical infrastructure from cyberattacks of Ukraine. **ELPA–NDT**, p. 14, 2023.

LAKSHMANAN, Ravie. **Google Reveals Alarming Surge in Russian Cyber Attacks Against Ukraine.** The hackersNews, 2023. Disponível em: <https://thehackernews.com/2023/02/google-reveals-alarming-surge-in.html>. Acesso em 17 de jul.de 2023.

LIMA, Telma CS; MIOTO, Regina Célia Tamaso. **Procedimentos metodológicos na construção do conhecimento científico: a pesquisa bibliográfica.** Revista Katálysis, v. 10, n. 1, p. 37-45, 2007.

LOPES, J. R. DA C. C**. Controle reflexivo russo: teoria militar e aplicações.** Coleção Meira Mattos: revista das ciências militares, v. 15, n. especial, p. 15-41, 28 dez. 2021.

LYNGAAS, Sean. **Ministro ucraniano pede que 'Exército de TI' se junte à 'luta na frente cibernética'.** CNN, 26 fev. 2022. disponível em: <https://www.cnnbrasil.com.br/internacional/ministro-ucraniano-pede-que-exercito-de-ti-se-junte-a-luta-na-frente-cibernetica/>. Acesso em: 30 jun. 2023.

MACHADO, Felipe Nery Rodrigues. **Segurança da informação: princípios e controles de ameaças.** São Paulo, Érica, 2014.

MANDIANT, 2021. **UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests.** Dispon[ivel em: <https://www.mandiant.com/resources/blog/unc1151-linked-to-belarus-government>. Acesso em: 23 de jun. de 2023.

MARTIN, Alexander. **US military hackers conducting offensive operations in support of Ukraine, says head of Cyber Command**. 1 de jun. 2022, UK. Disponível em: <https://news.sky.com/story/us-military-hackers-conducting-offensive-operations-in-support-of-ukraine-says-head-of-cyber-command-12625139>. Acesso em: 25 de jul. 2023.

MARTINS, Luis Fernando Ribeiro. **Os desafios da logística militar terrestre, no nível tático, na guerra da era da informação**. Doutrina Militar Terrestre em Revista, v. 1, n. 21, p. 54-61, 2020.

MASCHMEYER, Lennart; CAVELTY, Myriam Dunn. **Goodbye Cyberwar: Ukraine as Reality Check. Policy Perspectives.Center for Security Studies** (CSS). Vol. 10/3, 2022, pp. 1-4. Disponível m: <https://css.ethz.ch/en/center/CSS-news/2022/06/goodbye-cyberwar-ukraine-as-reality-check.html>. Acesso em: 01 jun. 2023.

MAZAT, Numa. **Uma análise estrutural da vulnerabilidade externa econômica e geopolítica da Rússia. 2013.** Tese de Doutorado. Tese de Doutorado em Economia Política Internacional, Instituto de Economia, Universidade Federal do Rio de Janeiro, Rio de Janeiro.

MITCHELL, Russ. **How Amazon put Ukraine's 'government in a box' – and saved its economy from Russia**. Los Angeles Times, 15 de dez. 2022. Disponível em: <https://www.latimes.com/business/story/2022-12-15/amazon-ukraine-war-cloud-data>. Acesso em: 1 jul. 2023.

MIELNICZUK, Fabiano. **Identidade como fonte de conflito: Ucrânia e Rússia no pós-URSS**. Contexto internacional, v. 28, p. 223-258, 2006.

MILLER. Christopher; SCOTT, Mark; BENDER, Bryan. **UkraineX: How Elon Musk's space satellites changed the war on the ground**. Politico, June 8, 2022. Disponível em: <https://www.politico.eu/article/elonmusk-ukraine-starlink/>. Acesso em 18 jun. 2023.

MORETTI, Rafaela. **Ataques cibernéticos e segurança da informação nos órgãos federais**. TCC, 2022.

MORGADO, Flávio Roberto Bezerra. **A Era da Comunicação e suas repercussões para a Doutrina Militar.** Observatório Militar da Praia Vermelha. ECEME: Rio de Janeiro. 2021.

MOROZOV, Dmytro S. et al. **Honeypot and cyber deception as a tool for detecting cyber attacks on critical infrastructure**. 2023.

MORRIS, Loveday; BRADY, Kate. Ukraine's Zelensky visits Germany, turning a page on fragile ties. **The Washington Post**, 2023.

MUELLER, G. et al. **Cyber operations during the Russo–Ukrainian war**. Center for Strategic Int. Studies, Washington, DC, USA, 2023.

NOGUEIRA, Michel Gomes. **Estudo de caso sobre o conflito cibernético entre a Rússia e a Geórgia.** 2018.

NONATO, Marcos Paulo Cardoso; PINHO, Harley de. **A integração do Sistema Militar de Defesa Cibernética (SMDC) com a proteção cibernética das infraestruturas críticas de interesse para Defesa Nacional**. 2021.

NUNES, Cristiano Monteiro. **Análise preliminar da perspectiva cognitiva da dimensão informacional no conflito entre Russia e Ucrânia através da aplicação de técnicas de aprendizagem de máquina de supervisão fraca**. Rio de Janeiro. 2022.

NUNES, Isabel Ferreira et al. Ucrânia um ano depois. **IDN Brief**, 2023.

O TEMPO, 2022. **Fotos de voluntários brasileiros na Ucrânia facilitariam ataques.** Disponível em: <https://www.otempo.com.br/politica/fotos-de-voluntarios-brasileiros-na-ucrania-facilitariam-ataques-russos-1.2633419>. Acesso em 20 de jul. 2023.

PAGLIUSI, Paulo Sergio. **Guerra Cibernética russo-ucraniana: lições para o Brasil e para o mundo.** Revista do Clube Naval, v. 2, n. 402, p. 74-79, 2022.

PERNAMBUCO. Secretaria de Ciência, Tecnologia e Inovação. **Ministro da Defesa visita Porto Digital e defende ampliação da parceria.** 22 de ago. 2019. Disponível em: <https://www.sectec.pe.gov.br/ministro-da-defesa-visita-porto-digital-e-defende-ampliacao-da-parceria/>. Acesso em: 17 ago. 2023.

PONTES, Edison**. Políticas e normas para a segurança da informação**, Rio de Janeiro, Brasport, 2012.

PRINCE, Matthew. **Steps we've taken around Cloudfare's services in Ukraine, Belarus, and Russia**. Cloudfare, Mar. 7, 2022. Disponível em: <https://blog.cloudflare.com/steps-taken-aroundcloudflares-services-in-ukraine-belarus-and-russia/>. Acesso em: 25 de jun. 2023.

PRZETACZNIK; Jakub. TARPOVA, Simona. **EUROPEAN PARLIAMENT: Russia's war on Ukraine: Timeline of cyber-attacks**. European Union, 2022. Disponível em: <https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)73354 9_EN.pdf>. Acesso em: 04 de jun. de 2023.

RASH, Michael. **Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort**. San Francisco: No Starch Press, 2007.

RICHARDSON, R. J. **Pesquisa social: métodos e técnicas**. São Paulo: Atlas, 1999.

RODRIGUES DA SILVA, Fernando. **Anexação da Crimeia e a Crise da Ucrânia sob a perspectiva político-estratégica da Rússia**. Centro de Estudos Estratégicos do Exército: Análise Estratégica, v. 19, n. 1, p. 33-49, 2021.

SÁNCHEZ-CASTILLO, Sebastián; GALÁN-CUBILLO, Esteban; DRYLIE-CAREY, Lindsey. Unmuting leadership: the impact of Zelensky's social media strategy at the inset of the Ukrainian War. **Journal of Risk Research**, p. 1-15, 2023.

SERPANOS, Dimitrios; KOMNINOS, Theodoros. **The cyberwarfare in Ukraine.** Computer, v. 55, n. 7, p. 88-91, 2022.

SILVA, Michel Bernardo Fernandes da. **Cibersegurança: Visão Panorâmica Sobre a Segurança da Informação na Internet.** Brasil: Freitas Bastos, 2023.

SONICWALL CYBER THREAT REPORT, 2023. Disponível em: <https://www.sonicwall.com/medialibrary/en/white-paper/2023-cyber-threat-report.pdf> Acesso em: 23 de jul. 2023.

SOUZA, Julia Martins. **As contramedidas aplicadas durante o conflito Russo-Ucraniano: análise da legitimidade e eficiência do Direito Internacional Público**. 2023.

TANGALAKIS-LIPPERT, Katherine. **Amazon helped the Ukrainian government and economy using suitcase-sized hard drives brought in over the Polish border: 'You can't take out the cloud with a cruise missile**. Business Insider, Dez 18, 2022. Disponível em: <https://www.businessinsider.com/amazon-saved-the-ukrainian-government-with-suitcase-sized-hard-drives-2022-12>. Acesso em 22 de jun. 2023.

TEIXEIRA, ADRIANA; COSTA, ROGÉRIO. **Ucrânia e Rússia: guerra híbrida e destruição da verdade factual. Flagelos da desinformação**, 2023.

THREAT ANALISIS GROUP, 2022. **Fog of war_ how the Ukraine conflict transformed the cyber threat landscape.** Disponível em: <https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape>. Acesso em 22 de abr. 2023.

UNITED STATES. **Department of State.United with Ukraine: supporting ukraine's sovereignty and territorial integrity. Washington**, D.C: Department of State, 7 abr. 2022. Disponível em: <https://www.state.gov/united-with-ukraine/#supporting-ukraine>. Acesso em: 26 mar. 2023.

VERGARA, Sylvia Constant. **Projetos e relatórios de pesquisa**. São Paulo: Atlas, v. 34, p. 38, 2006.

VISACRO, ALESSANDRO. **A Guerra na Era da Informação**. Rio de Janeiro: Editora Contexto, 2018.

VISACRO, ALESSANDRO. **Guerra na Ucrânia.** Disponível em: <https://blog.editoracontexto.com.br/guerra-na-ucrania-alessandro-visacro/>. Acesso em: 28 de mar. 2023.

WILLETT, Marcus. The Cyber Dimension of the Russia–Ukraine War. **Survival**, v. 64, n. 5, p. 7-26, 2022.

ZACHARA-SZYMAŃSKA, Małgorzata. The return of the hero-leader? Volodymyr Zelensky's international image and the global response to Russia's invasion of Ukraine. **Leadership**, p. 17-24, 2023.