Defesa cibernética na guerra russo-ucraniana

Um mapeamento dos ataques cibernéticos às infraestruturas críticas da Ucrânia

Thays Felipe David de Oliveira | *Renato Victor Lira Brito* | *Priscylla Cristina de Souza Lippo*

INTRODUÇÃO

Quais ataques cibernéticos às infraestruturas críticas (IC) sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a Guerra russo-ucraniana? Sabemos que os ataques cibernéticos às IC têm como escopo gerar uma desordem ao Estado que sofreu com o dano. Uma vez que, quando isso acontece, há um comprometimento inteiro de sistemas através de *softwares* maliciosos.

No ano de 2022, a incidência de ataques cibernéticos foi menos recorrente quando comparado ao ano de 2023. Dessa forma, os dados referentes a este fenômeno apontam que a Dinamarca sofreu um total de 11 ataques, enquanto a França sete e em menor número os Países Baixos com seis[1]. Perante o exposto, esta temática é de suma importância para a área da defesa nacional, pois as IC são bens e serviços essenciais para o pleno funcionamento de um Estado. Logo, áreas como administração pública, comunicação e energia compõem esta esfera, que, quando atacadas, geram danos devastadores à sociedade, como no caso Stuxnet.

Nesse diapasão, a Ucrânia pode ser tomada como exemplo de estudo de caso único[2] para discutir questões de políticas de defesa de um Estado no espaço cibernético, uma vez que, por falta de regulação e fis-

RESUMO

Quais ataques cibernéticos às infraestruturas críticas sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana? Nos últimos meses, a Ucrânia vem sofrendo uma grande ofensiva de ataques cibernéticos às suas infraestruturas críticas. Assim, o objetivo deste trabalho é analisar quais ataques cibernéticos às infraestruturas críticas sofreu a Ucrânia dentro do recorte selecionado. Para isso, foi realizada uma pesquisa de método misto, que foi operacionalizada por meio de estatística descritiva, análise documental e revisão sistemática da literatura. Assim, a partir dos dados analisados do CyberPeace Institute, o setor mais atingido foi o de administração pública (66), enquanto a categoria de ataques mais utilizada foi de disrupção (139). Em seguida, avaliamos os tipos de ataques cibernéticos, sendo o mais utilizado o de tipo «DDoS» (135). Já na categoria de atores, a categoria «coletiva» (124), com destaque para o People's CyberArmy (48), foi a de maior ocorrência. Em suma, concluímos que os ataques às infraestruturas críticas constituem uma questão de defesa nacional, sendo necessário revisar a →

 https://doi.org/10.23906/ri2024.82a05

legislação relacionada a esse tema e garantir que os órgãos responsáveis estejam preparados para enfrentar problemas futuros.

Palavras-chave: infraestruturas críticas, defesa nacional, Ucrânia, ataques cibernéticos.

ABSTRACT

Cyber defense in the Russo-Ukrainian war: a mapping of cyber attacks on Ukrainian critical infrastructure

What cyberattacks did Ukraine's critical infrastructure experience between February 2022 and February 2023 during the Russo-Ukrainian war? In recent months, Ukraine has experienced a significant increase in cyberattacks on its critical infrastructure. Therefore, the purpose of this study is to analyze the cyberattacks suffered by Ukraine's critical infrastructure within the selected cutout. A mixed method research approach was used, operationalized through descriptive statistics, documentary analysis, and a systematic literature review. Based on the analyzed data from the CyberPeace Institute, the sector most affected was public administration (66), with the Disruption attack category being the most utilized (139). The types of cyberattacks were also evaluated, with the DDoS type being the most common (135). The collective (124), especially the People's CyberArmy (48), was the most common in the actor category. In conclusion, we can say that attacks on critical infrastructure are a matter of national defense, which requires a revision of legislation on this issue and ensuring that the responsible bodies are prepared for future challenges.

Keywords: critical infrastructure, national defense, Ukraine, cyberattacks.

calização, este domínio é visto como um campo de infinitas possibilidades de ações que podem gerar consequências no meio físico.

Este trabalho tem por objetivo geral analisar quais ataques cibernéticos às IC sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana. Para tanto, operacionalizou-se a pesquisa por meio de técnicas de métodos mistos, como de estatística descritiva, análise documental e revisão sistemática da literatura.

Nas próximas seções, apresenta-se brevemente o contexto da guerra russo-ucraniana, seguido por considerações acerca do espaço cibernético e suas IC e pela análise dos ataques direcionados à Ucrânia que têm acontecido no âmbito dessa guerra.

METODOLOGIA

A Ucrânia sofreu diversos ataques cibernéticos às suas IC desde o início da guerra russo-ucraniana. Sendo assim, para compreender este fenômeno, foi elaborado o seguinte panorama:

Quadro 1 > Desenho da pesquisa

Pergunta de pesquisa	Quais ataques cibernéticos às IC sofreu a Ucrânia entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana?
Unidade espacial de análise	Infraestruturas críticas ucranianas
Unidade temporal de análise	Fevereiro de 2022 a fevereiro de 2023
Método	Misto (quantitativo e qualitativo)
Técnica	Estatística descritiva, análise documental e revisão sistemática da literatura

Fonte: Elaborado pelos autores.

Perante o recorte metodológico realizado nesta pesquisa, foi utilizado o estudo de caso único que, segundo Yin[3], é uma das maneiras de se fazer pesquisa nas Relações Internacionais, que envolve experimentos, levantamentos, pesquisas históricas e análise de informações de documentos. Portanto, este trabalho realiza um recorte dentre os temas existentes no contexto da guerra russo-ucraniana, especialmente os ataques cibernéticos às IC da Ucrânia.

De forma complementar, essa pesquisa foi conduzida por meio de métodos mistos segundo Paranhos et al.[4], dado que foram utilizados os métodos qualitativo e quantitativo. Assim, a metodologia qualitativa responde a questões nas Relações Internacionais com um nível de complexidade difícil de ser quantificado. A partir dessa perspectiva, o presente artigo foi operacionalizado por meio de uma análise documental e de uma revisão sistemática da literatura.

Conforme exposto, o quadro 2 apresenta as fontes primárias e secundárias utilizadas neste artigo. As fontes secundárias foram utilizadas unicamente com a finalidade de exemplificar os ataques cibernéticos às IC ucranianas cometidos no espaço temporal analisado.

Quadro 2 > Categoria das fontes

Fontes primárias	CyberPeace Institute
	Documentos governamentais da Ucrânia e da Rússia
	Documentos do Conselho de Segurança das Nações Unidas
Fontes secundárias	CNN, BBC, g1, The Cyber Express

Fonte: Elaborado pelos autores.

A revisão sistemática proporcionou um levantamento do arcabouço teórico, com o intuito de auxiliar na compreensão sobre o fenômeno estudado a partir das fontes supracitadas.

O outro método utilizado foi o quantitativo, que é definido como uma «restrição ao uso de determinadas estatísticas para a identificação [...] das variáveis»[5]. Para operacionalização deste, foram considerados os dados do CyberPeace Institute, que serão exibidos nos resultados e discussões a partir de gráficos, a fim de auxiliar na compreensão das informações.

Complementarmente, foi utilizada a estatística descritiva, pois «[a] estatística descritiva auxilia os métodos quantitativos de forma a definir (frequência, média, mediana, moda etc.) a revelar formas úteis, rápidas e confiáveis a respeito de um grande número de observações»[6]. Assim, esta técnica auxiliou na elaboração de uma análise estatística sobre os ataques cibernéticos às IC sofridos pela Ucrânia no período de fevereiro de 2022 a fevereiro de 2023 da guerra em curso no leste europeu e na perfilação dos resultados quantificados. Para isso, os dados foram tabulados no Microsoft Excel.

Por fim, foram analisados os dados referenciados ao ataque cibernético das IC da Ucrânia e estão disponibilizados no GitHub[7] para oferecer uma maior replicabilidade à presente pesquisa nos termos de King[8]. Assim, uma pesquisa acadêmica de boa qualidade deve permitir gerar inferências válidas[9].

O CONTEXTO DA GUERRA RUSSO-UCRANIANA

Com o colapso da União das Repúblicas Socialistas Soviéticas, em 1991, a Ucrânia se tornou uma nação independente. A região ucraniana é dividida em dois lados: o oeste, onde fica a capital Kiev, localização que facilita o elo com o ocidente europeu, por sua posição geoestratégica, e é a região que apresenta uma maior atuação da União Europeia e da Organização do Tratado do Atlântico Norte (NATO, na sigla inglesa). Em contrapartida, existe o lado leste, predominantemente a área do Donbass, que possui uma grande quantidade de russos e de movimentos de cunho separatista.

Todavia, a partir de 2014, a Ucrânia desenvolveu uma relação de preferência, em termos de política externa, às potências ocidentais sob a liderança de Petro Poroshenko. Após esse movimento, a clara insatisfação russa com o Governo ucraniano serviu de base para que a Rússia invadisse a região da Crimeia, desrespeitando assim o Memorando de Budapeste[10].

Após este conjunto de acontecimentos, no ano de 2019, para deteriorar a situação, Volodymyr Zelensky, o atual Presidente da Ucrânia, ascendeu ao poder com um ideal de romper com a Rússia e de que apenas voltaria a ter relações com o país caso os separatistas devolvessem territórios ocupados para a Ucrânia[11]. Simultaneamente a isso, o Estado se mostrou cada vez mais próximo da NATO, deixando um sentimento ainda maior de ameaça na Federação Russa, já que uma parte de sua fronteira estava sob o domínio da NATO, devido à adesão da Polônia.

O POSSÍVEL PRIMEIRO ATAQUE DE PUTIN FOI UTILIZAR A REGIÃO DE DONBASS AO SEU FAVOR, PROMOVENDO ATAQUES CIBERNÉTICOS E DISSEMINAÇÃO DE *FAKE NEWS*, DESENCADEANDO ASSIM UMA ESPÉCIE DE GUERRA CIVIL NO PAÍS.

Em suma, a Ucrânia divide geograficamente uma grande parte da fronteira com a Rússia. Logo, a anexação desse território à organização ocidental significaria que tropas estadunidenses poderiam estar cada vez mais próximas do domínio russo. Por isso, o possível primeiro ataque de Putin foi utilizar a região de Donbass ao seu favor, promovendo ataques cibernéticos e disseminação de *fake news*, desencadeando assim uma espécie de guerra civil no país, contradizendo os princípios de ingresso à NATO de que o território não pode estar passando por conflitos internos.

O ESPAÇO CIBERNÉTICO E AS INFRAESTRUTURAS CRÍTICAS

Na atualidade, o espaço cibernético tem sido extremamente utilizado por atores estatais e não estatais em seu favor, tanto em questões referentes à defesa nacional, quanto em ofensivas diretas a outro Estado sem necessariamente existir um *front* direto. Um grande exemplo dessa ação é o caso Stuxnet, um *worm* que invadiu o sistema de supervisão e

aquisição de dados (SCADA) da empresa Siemens, que afetou gravemente as usinas nucleares iranianas e desestabilizou o funcionamento das ogivas, e que caso levasse à explosão, seria de dano inestimável ao Irã[12].

Nesse sentido, este tipo de ação é característico no espaço cibernético. Logo, podemos considerar este fenômeno como «o território não físico criado por meios computacionais, onde pessoas podem se comunicar, realizar pesquisas e trafegar dados de maneira geral, valendo-se de Tecnologias da Informação e Comunicação (TIC)»[13]. Ademais, o espaço cibernético é um fenômeno relativamente recente para os Estados, e ainda há certo receio de como estes podem atuar, tendo em vista que ainda não existe uma legislação internacional amplamente aceita que regulamente este domínio[14].

De forma complementar, a defesa do espaço cibernético é efetivada de acordo com a legislação de cada país. Assim, no Brasil, é competência de órgãos como o Ministério da Defesa e o Gabinete de Segurança Interinstitucional (GSI). Enquanto isso, nos Estados Unidos, por exemplo, o principal regulador do espaço cibernético é a National Security Agency (NSA), uma agência do Departamento de Defesa norte-americano, que trata das questões tangentes aos ataques e educação cibernética do país. A defesa cibernética dos Estados Unidos da América também é responsabilidade de 16 agências, que constituem a US Intelligence Community[15]. A Ucrânia também é um país de governança cooperativa do espaço cibernético:

> «um ambiente (espaço virtual) que oferece oportunidades de comunicação e/ou implementação de relações públicas, formado como resultado do funcionamento de sistemas de comunicação compatíveis (ligados) e de comunicações eletrônicas utilizando a Internet e/ou outras redes de dados globais»[16].

Dessa forma, a governança do espaço cibernético para o referido Estado é realizada por entidades do setor público e privado, responsáveis pela prevenção e investigação de ataques cibernéticos contra a defesa nacional. O país possui o Centro de Coordenação de Ciberdefesa e Cibersegurança, que promove assistência para formações militares atuantes na defesa de ameaças no espaço cibernético e mapeia dados de crimes virtuais com o objetivo de proteger a si e aos países com os quais coopera[17].

Sendo assim, podemos considerar os ataques cibernéticos como «qualquer tipo de manobra ofensiva para invadir um computador ou sistema»[18]. Logo, estes ataques possuem potencial de paralisar o funcionamento de serviços essenciais a um Estado, através de destruição ou interrupção do serviço, por exemplo.

No contexto atual, os Estados se tornam cada vez mais dependentes do meio cibernético, onde possuem bens e serviços essenciais para seu funcionamento. Tal dependência culmina na exposição das IC. De acordo com Martii Lehto:

> «Em geral, a infraestrutura crítica descreve os sistemas e ativos físicos e cibernéticos que são tão vitais para a nação que sua incapacidade ou destruição teria um impacto debilitante

na segurança física ou econômica ou na saúde ou segurança pública. Assim, a infraestrutura crítica da nação fornece os serviços essenciais que sustentam a sociedade»[19].

Logo, vemos que as IC possuem suma importância para a população. Portanto, são um recurso que «uma vez prejudicados por fenômenos de causas naturais, como terremotos ou inundações ou por ações intencionais de sabotagem ou terrorismo, trazem grandes reflexos negativos para toda uma nação e sua sociedade»[20].
Nesse sentido, para a Ucrânia, as IC «Devem significar e incluir os sistemas e recursos, físicos ou virtuais, que suportam funções e serviços cuja interrupção terá efeitos negativos mais graves na atividade da sociedade, no desenvolvimento socioeconômico do país e na segurança nacional»[21].
Com isso, percebemos que uma infraestrutura crítica ucraniana atacada resulta em sérios problemas para o Estado, como pode ser visto no quadro 3[22]:

Quadro 3 > Setores de IC e instituições responsáveis

Setor de IC	Principais instituições responsáveis por segurança, proteção e operação das instalações dos setores
Combustível e complexo de energia	Ministry of Energy and Coal Industry of Ukraine (MoECI), Security Service of Ukraine (SSU), Ministry of Internal Affairs of Ukraine (MIA), State Service of Special Communications and Information Protection of Ukraine (SSSCIP)
Transporte	Ministry of Infrastructure of Ukraine, SSU, MIA
Redes de suporte à vida	Ministry of Regional Development of Ukraine, Construction and Communal Services of Ukraine, State Services of Ukraine for Emergency Situations (SESU)
Telecomunicações e redes de comunicações	SSSCIP, MIA
Finanças e setor bancário	National Bank of Ukraine, Ministry of Finance of Ukraine, SSU, SSSCIP
Administração pública e aplicação da lei	SSU, MIA, State Guard Service
Complexo de defesa e segurança	Ministry of Defense of Ukraine (MoD), MIA, SSU
Indústria química	State Service of Ukraine for Labor, SSE, SSU
Serviços de emergência e proteção civil	SESU, Ministry of Health of Ukraine
Indústria de processamento alimentício e complexo agrário	Ministry of Agrarian Policy and Food of Ukraine

Fonte: Elaborado pelos autores.

Portanto, observamos que há uma gama de órgãos e instituições ucranianos responsáveis por cada setor de IC, dada a importância destes bens e serviços. Apesar de haver órgãos responsáveis, diante do cenário complexo atual, é necessário o debate acadêmico sobre os desafios e potencialidades enfrentados pelo Estado.

RESULTADOS E DISCUSSÕES

Nesta parte do artigo serão discutidos os resultados acerca da análise feita sobre os ataques cibernéticos às IC ucranianas no primeiro ano da Guerra da Ucrânia. Dessa maneira, os dados aqui apresentados foram retirados de relatórios do CyberPeace Institute no período de fevereiro de 2022 a fevereiro de 2023. Esta análise visa observar as consequências diretas para a defesa nacional da Ucrânia, visto que um ataque cibernético às suas IC tem o potencial de impactar toda uma rede de interdependência de bens e serviços.

Segundo a atual versão da Diretiva sobre a Identificação e Designação das Infraestruturas Críticas Europeias[23],o aumento da proteção das IC possibilita que o impacto gerado por ataques cibernéticos seja consideravelmente reduzido. Dessa maneira, podemos aplicar o fator da importância relativo às IC na defesa nacional dentro do contexto russo-ucraniano.

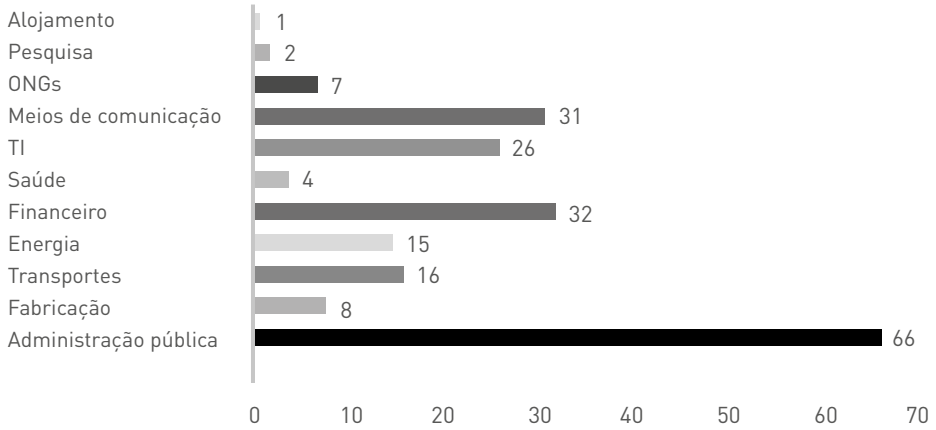
Para tal efeito, um ataque cibernético é um subconjunto de operações realizadas no espaço cibernético que fazem o uso hostil de suas capacidades, sendo realizadas por Estados ou atores não estatais com o intuito de causar danos e destruição, para alcançar objetivos militares ou políticos[24].

DURANTE A GUERRA DA UCRÂNIA HOUVE 1258 ATAQUES CIBERNÉTICOS ÀS INFRAESTRUTURAS CRÍTICAS NO MUNDO.

No entanto, durante a Guerra da Ucrânia houve 1258 ataques cibernéticos às IC no mundo, tais como em março de 2022, quando o *site* do presidente da França sofreu um ataque em meio às eleições presidenciais, enquanto apenas na Ucrânia houve 291 ataques no período estudado, e destes, 83 são desconhecidos e estão sob análise segundo o CyberPeace Institute. Mas, ao comparar com os anos anteriores, houve um aumento. Uma infraestrutura crítica, ao sofrer um ataque cibernético, gera danos às mais diversas áreas de uma sociedade. A pesquisa demonstrou que as IC da Ucrânia são compostas pelos setores presentes no gráfico 1 (p. 068), bem como seu número de ataques.

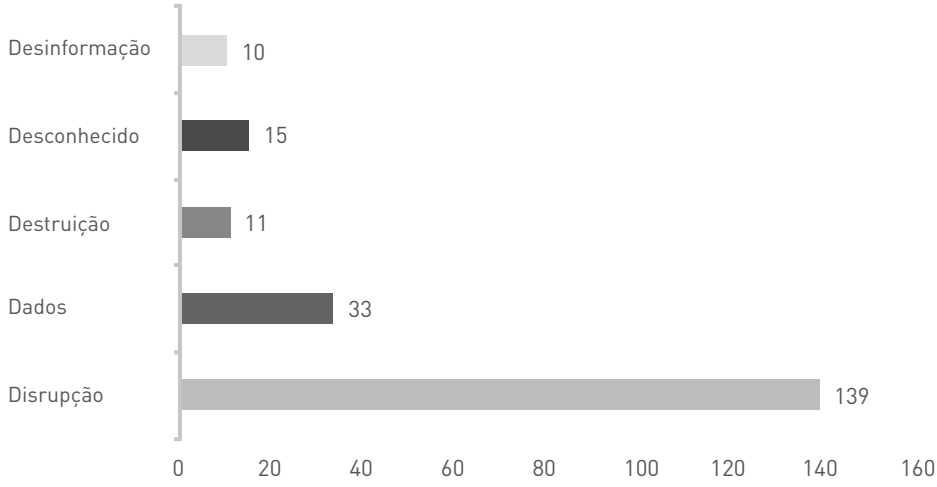
A partir dos dados apresentados, inferimos que o setor de administração pública recebeu o maior número de ataques cibernéticos (66), visto que os poderes de governar, gerenciar e regulamentar impactam diretamente o funcionamento básico de um Estado. De acordo com a CNN Brasil[25], em março de 2022 um ataque de categoria desconhecida comprometeu a rede da Ukrtelecom, uma grande operadora de telecomunicações ucraniana. Contudo, o ator responsável não foi identificado, algo comum dentro do cenário cibernético, espaço que possibilita que os atores de ataques passassem despercebidos devido à sua ausência de fiscalização.

Gráfico 1 > Ataques aos setores de infraestrutura crítica ucraniana entre fevereiro de 2022 a fevereiro de 2023



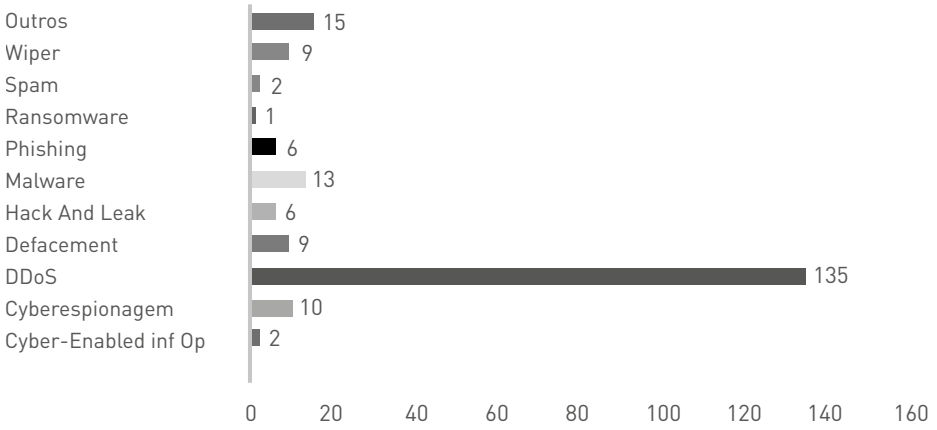
Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Gráfico 2 > Categorias dos ataques cibernéticos às IC ucranianas entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Gráfico 3 > Tipos de ataques cibernéticos às IC da Ucrânia entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

Ademais, outro setor afetado foi o da energia. Em abril de 2022, o setor da energia da Ucrânia foi afetado por um ataque cibernético de destruição, no qual *malwares* cortaram o fornecimento de energia do país, que resultou na interrupção no fornecimento de energia para aproximadamente dois milhões de ucranianos.

No gráfico 2 é possível observar que os ataques da categoria «disrupção» representam mais de metade do valor total de ataques (208) sofridos pela Ucrânia.

Assim, é indispensável salientar que a disrupção é a modalidade de ataque que ameaça a disponibilidade ou a integridade de um sistema[26], sendo estes dois dos princípios da segurança da informação de acordo com Dantas[27].

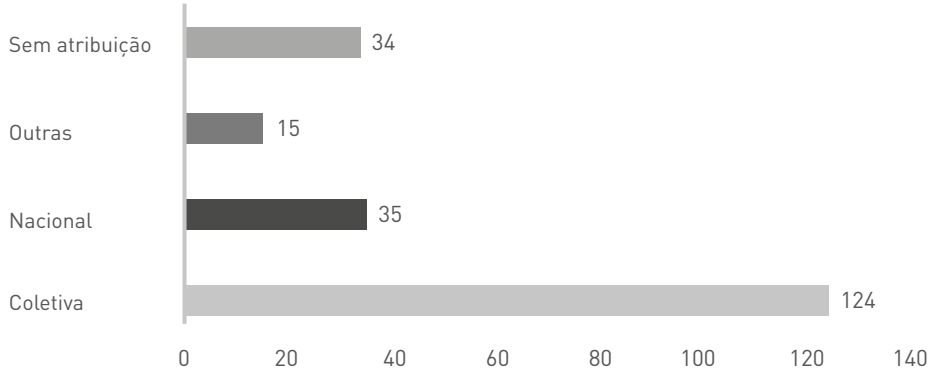
Dessa forma, a destruição, para fins comparativos, é definida por Cavelty[28] como ataques de ciberhacktivismo ou cibervandalismo – explica-se como o equivalente *online* para formas de vandalismo ou ativismo, através de panfletagem (*websites* de protesto), grafitti (*defacement*/desfiguração de algum *website*), bloqueios (ataques de negação de serviço) e ocupações (uso ilegal de algum domínio, *cybersquatting*) que visam destruir o conteúdo de um site ou sistema[29].

Além disso, ataques de desinformação baseiam-se em compartilhamento de *fake news*, modalidade esta que afeta, sobretudo, a forma como a população recebe informações. Por fim, o «desconhecido» é que ainda não se tem informação necessária para categorizar o ataque.

O gráfico 3 apresenta os tipos de ataques direcionados ao nosso objeto de estudo. O destaque vai para os 135 ataques de tipo «DDoS» (negação de serviço distribuído), que funciona por meio de envios massivos de requisições a um servidor, levando ao travamento e, consequentemente, sua interrupção[30].

Diante disso, podemos mencionar o ataque de disrupção do tipo «DDoS» ocorrido em fevereiro de 2022, noticiado pela CNN Brasil, contra o setor de finanças da Ucrânia[31]. O ator responsável pelo ataque não foi identificado, mas deixou duas importantes redes bancárias do país fora do ar.

Gráfico 4 > Categorias dos atores atribuídos aos ataques entre fevereiro de 2022 e fevereiro de 2023



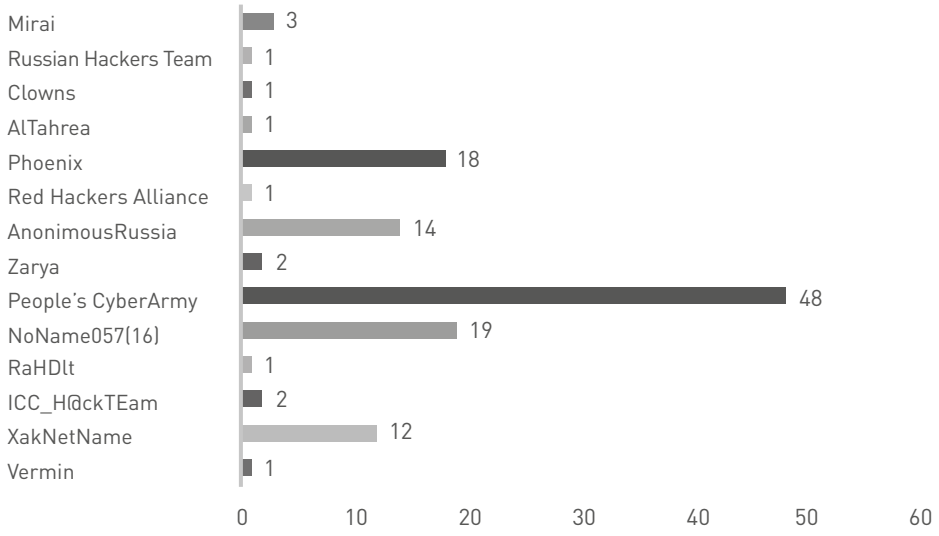
Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

O gráfico 4, da categoria dos atores, é composto por: coletiva (124), nacional (35), outras (15) e sem atribuição (34). Assim, inferimos que os atores coletivos, isto é, atores que não são vinculados a um Estado, predominam nos ataques. A exemplo de ataques atribuídos aos atores coletivos, segundo a revista *The Cyber Express*[32], em 21 de novembro de 2022, o grupo de *hackers* russos conhecido como «XakNet», foi responsável por invadir os serviços do Ministério de Finanças da Ucrânia, que possibilitou aos *hackers* obterem informações sobre mais de um milhão de documentos.

Por outro lado, em contraste com a categoria de atores coletiva, a segunda unidade com maior incidência de ataques cibernéticos é a categoria de atores nacionais, que é constituída por agentes que se intitulam como vinculados a algum governo[33].

Perante o gráfico 5 (p. 071), observamos um grande número (48) de atribuições ao grupo People's CyberArmy, grupo que se proclama afiliado à Rússia. Eles utilizam ataques «DDoS», como em janeiro de 2023 contra o *site* de uma rede de postos de gasolina da Ucrânia, em que provocaram uma disrupção na plataforma, conforme o CyberPeace Institute. Ademais, o grupo NoName057(16) possui notória participação, com o exemplo do ataque ocorrido em setembro de 2022, onde utilizou de *defacement* para violar o *site* de uma importante universidade sediada em Kiev, capital ucraniana.

Gráfico 5 > Atores atribuídos aos ataques entre fevereiro de 2022 e fevereiro de 2023



Fonte: Gráfico elaborado pelos autores a partir dos dados obtidos na pesquisa.

O *defacement* consiste em alterações não autorizadas em *sites*, afetando o princípio da integridade, o que gera um grande impacto na reputação[34]. Ao desfigurar um *site* ou sistema, é gerada desinformação para aqueles que o acessam, visto que podem considerar como informações de procedência da própria instituição.

A partir do que foi analisado, percebemos que a Ucrânia passou por diversos ataques cibernéticos às IC durante o período da guerra com a Rússia. Logo, encoraja-se que se tomem medidas cada vez mais enérgicas referentes à segurança cibernética na Ucrânia, como, por exemplo, os cinco aspectos da segurança cibernética[35] que têm o potencial de auxiliar na prevenção e mitigação dos ataques às infraestruturas críticas, sendo estes:

Eficiência operacional: em meio ao crescimento dos investimentos tecnológicos, a colaboração entre os envolvidos faz-se indispensável para que a necessidade de proteção de dados seja compreendida.

Colaboração: todas as esferas governamentais precisam estar alinhadas em uma política de combate ao crime cibernético.

Higiene cibernética: medidas como controles de segmentação de *patching* para *firmware* e métodos de autenticação multifator compõem uma boa higiene cibernética.

Educação: em um cenário onde a maior parte das violações cibernéticas é consequência de erro humano, faz-se imprescindível o enfoque à educação cibernética em todos os âmbitos de uma sociedade, tanto no eixo individual quanto no coletivo.

Tecnologia: é importante o investimento constante na tecnologia, haja vista os rápidos avanços de *software* e de *hardware*, que quando defasados e obsoletos abrem portas para exploração de vulnerabilidades.

Os resultados acima discutidos elencam a fragilidade das IC de um Estado em meio a uma guerra no que se trata de sua defesa nacional. Esta análise cobre apenas os primeiros doze meses da guerra russo-ucraniana, porém possibilita visualizar tendências de ataques a IC ao pleno funcionamento da sociedade ucraniana.

CONSIDERAÇÕES FINAIS

Conforme descrito no presente artigo, os ataques cibernéticos às IC vêm acontecendo de forma recorrente no sistema internacional. Assim, o fato de o espaço cibernético ainda ser um cenário desconhecido facilita a perpetuação desses ataques. Portanto, sabemos que o objetivo deste estudo foi analisar quais ataques cibernéticos às IC da Ucrânia sofreu entre fevereiro de 2022 e fevereiro de 2023 durante a guerra russo-ucraniana. Logo, a Ucrânia foi um país que recebeu vários ataques cibernéticos antes e durante a guerra, o que acentua ainda mais a fragilidade do Estado e suas IC. Assim, este tema é de grande valia para a defesa nacional, pois demonstra que os Estados devem ter um determinado conhecimento relacionado aos ataques cibernéticos às IC. Nesse sentido, tais ataques podem causar danos irreparáveis para a população, especialmente porque a Ucrânia está passando por um período de guerra e acaba negligenciando uma temática de extrema relevância para a agenda de defesa nacional.

A partir do exposto, podemos perceber que a Ucrânia sofreu 291 ataques no período estudado, sendo em sua maioria no setor de administração pública, como por exemplo, um ataque de disrupção, que afetou diversos bancos ucranianos, além de ministérios como o da Defesa, Relações Exteriores e outros órgãos governamentais, do tipo «DDoS». Como apresentado durante todo o artigo, fica evidente que um país com políticas de defesa cibernética robustas pode se tornar mais eficiente e resiliente aos ataques. Então, para evitar ataques às IC é necessário que o governo tenha políticas específicas para a proteção nacional baseadas na higiene cibernética, na colaboração, na educação, na tecnologia e na eficiência operacional.

Assim como um trem, que tem a sua estrutura por inteiro afetada caso um vagão descarrilhe, um país com suas IC em mau funcionamento tem as suas demais áreas vitais desestabilizadas em uma breve questão de tempo. Desse modo, é possível perceber como os Estados e outros atores utilizam-se da vulnerabilidade de países, cujas IC foram afetadas, para instaurar guerras e conflitos de interesse. Portanto, a partir de análises realizadas no presente trabalho, concluímos que não somente os Estados mencionados neste estudo, mas também nações como o Brasil, tão presente no cenário internacional, urge a criação de um Programa de Defesa Cibernética, que tenha como seu principal objetivo aprimorar o fortalecimento da defesa cibernética nacional. Pois, por ser um

fenômeno recente, é criada uma necessidade de que o país se adeque aos novos fenômenos inerentes ao cenário internacional de Estados e que interferem diretamente na soberania estatal. R:I

Data de receção: 5 de janeiro de 2024 | Data de aprovação: 5 de abril de 2024

Thays Felipe David de Oliveira Coordenadora e professora de Relações Internacionais no Centro Universitário Estácio do Recife, e professora substituta em Gestão Pública na Universidade Federal da Paraíba (UFPB). Coordenadora do Núcleo de Estudos em Processos Cibernéticos em Relações Internacionais (NEPCRI). Doutora em Ciência Política pela Universidade Federal de Pernambuco (UFPE).
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | thaysfelipe@gmail.com

Renato Victor Lira Brito Vice-coordenador do Núcleo de Estudos em Processos Cibernéticos em Relações Internacionais (NEPCRI). Doutorando, mestre e bacharel em Ciência Política pela Universidade Federal de Pernambuco (UFPE). Editor executivo da *Revista Política Hoje*. Membro da Comissão de Direitos Humanos Dom Helder Câmara da UFPE. Membro da Comissão Própria de Avaliação da UFPE.
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | renato.lirabrito@ufpe.br

Priscylla Cristina de Souza Lippo Aluna da gradução em Relações Internacionais pelo Centro Universitário Estácio do Recife. Licenciada em Letras (Língua Portuguesa) pela Universidade Federal de Pernambuco e mestre em Linguística pela mesma universidade.
> Centro Universitário Estácio do Recife, Av. Eng. Abdias de Carvalho, 1678, Madalena, Recife, Pernambuco, Brasil | priscyllaalippo@gmail.com

NOTAS

1 CYBERPEACE INSTITUTE – «Cyber threats landscape». Consultado em: 14 de março de 2023. Disponível em: https://cyberconflicts.cyberpeaceinstitute.org/threats.

2 YIN, Robert K. – «Discovering the future of the case study: method in evaluation research». In *Evaluation practice*. Vol. 15, N.º 3, 1994, pp. 283-290.

3 YIN, Robert K. – *Estudo de Caso: Planejamento e Métodos*. 5.ª edição. Porto Alegre: Editora Bookman, 2014.

4 PARANHOS, Ranulfo, et al. – «Uma introdução aos métodos mistos». In *Sociologias*. Vol. 18, N.º 42, 2016, pp. 384-411.

5 CERVI, Emerson Urizzi – «Métodos quantitativos nas ciências sociais: uma abordagem alternativa ao fetichismo dos números e ao debate com qualitativistas». In *Pesquisa Social Reflexões: Teóricas e Metodológicas*. Ponta Grossa: Todapalavra Editora, 2009, pp. 125-144.

6 PARANHOS, Ranulfo, et al. – «Uma introdução aos métodos mistos», p. 388.

7 Para visitar os dados acesse: https://github.com/nepcri/CADN-2023.

8 KING, Gary – «Replicação, replicação». In *Revista Eletrônica de Ciência Política*. Vol. 6, N.º 2, 2015, pp. 382-401.

9 KING, Gary; KEOHANE, Robert O.; VERBA, Sidney – *Designing Social Inquiry: Scientific Inference in Qualitative Research*. 1.ª edição. New Jersey: Princeton University Press, 1994.

10 KONRAD, Kaiser David Vargas; LOURENÇÃO, Humberto José – «O conflito na Ucrânia entre 2014 e 2018 e seu impacto na segurança internacional». In *Brazilian Journal of Development*. Vol. 5, N.º 8, 2019, pp. 12906-12920.

11 PEREIRA COUTINHO, Francisco – «A agressão russa à Ucrânia e o direito internacional: uma tragédia em quatro atos». In *e-publica*. Lisboa. Vol. 10, N.º 1, 2023, pp. 4-17.

12 ZETTER, Kim – «An unprecedented look at stuxnet, the world's first digital weapon». Consultado em: 13 de abril de 2023. Disponível em: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.

13 HOSANG, Alexandre – *Política Nacional de Segurança Cibernética: Uma Necessidade para o Brasil*. Consultado em: 16 de abril

de 2023. Disponível em: https://www.abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf.

14 O Manual de Tallinn é um documento estritamente normativo que visa a aplicabilidade da lei em conflitos cibernéticos e que ainda não é amplamente aceito no Sistema Internacional de Estados. Além disso, também temos a Convenção de Budapeste, que também não é aceita largamente pelos Estados.

15 CRUZ JÚNIOR, Samuel César – «A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual». Consultado em: 13 de abril de 2023. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/1590/1/TD_1850.pdf.

16 DAI GLOBAL, LLC – *Usaid Cybersecurity for Critical Infrastructure in Ukraine Review of the Regulatory Framework for Critical Infrastructure Cybersecurity in Ukraine: Legislative Assessment Report*. Consultado em: 9 de abril de 2023. Disponível em: https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf. Tradução livre a partir do original.

17 SPÎNU, Natalia – «Ukraine cybersecurity governance assessment». Consultado em: 9 de abril de 2023. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

18 TAQUARY SEGUNDO, Célio Borges – «A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos». Consultado em: 8 de abril de 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1205.

19 LEHTO, Martti – «Cyber-attacks against critical infrastructure». In *Computational Methods in Applied Sciences*. Suíça: Springer, 2022. pp. 3-42. Tradução livre dos autores a partir do original.

20 LIMA, Pedro Arthur Linhares – «Segurança cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das infraestruturas críticas nacionais, órgãos estratégicos do Governo e Forças Armadas». Consultado em: 14 de abril de 2023. Disponível em: https://www.enabed2018.abedef.org/resources/anais/8/1534802448_ARQUIVO_Artigo-PedroALinharesLima-X-ENABED-SegurancaeDefesaCibernetica.pdf.

21 KONDRATOV, Sergiy, et al. – «Developing the critical infrastructure protection system in Ukraine: monograph». Kiev: National Institute For Strategic Studies, 2017. Consultado em: 14 de abril de 2023. Disponível em: https://niss.gov.ua/sites/default/files/2017-11/niss_Engl_findruk-0e9af.pdf. Tradução livre a partir do original.

22 *Ibidem*.

23 COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council of European Union. Consultado em: 14 de abril de 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32008L0114.

24 SIGHOLM, Johan – «Non-State actors in cyberspace operations». Consultado em: 14 de abril de 2023. Disponível em: https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations.

25 «ATAQUE CIBERNÉTICO atinge provedora de telecomunicações ucraniana, dizem autoridades». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-atinge-provedora-de-telecomunicacoes-ucraniana-dizem-autoridades/.

26 COIMBRA, Sara – «Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da Força Aérea». Consultado em: 8 de abril de 2023. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSara-Coimbra_TII_VF.pdf.

27 DANTAS, Marcus Leal – *Segurança da Informação: Uma Abordagem Focada em G de Riscos*. 1.ª edição. Olinda: Livro Rápido, 2011.

28 CAVELTY, Myriam Dunn – «Cyberwar: concept, status quo, and limitations». In *ETH Zurich*. Zurique. Vol. 71, 2010, pp. 1-3.

29 AUTY, Caroline – «Political hacktivism: tool of the underdog or scourge of cyberspace?». In *Aslib Proceedings*. Vol. 56, N.º 4, 2023, pp. 212-221.

30 MELLO, Fábio P.; MENDES JÚNIOR, Ricardo da C.; ROCHA, Daniel G. – *Análise de Ataques DDoS*. Rio de Janeiro: Instituto Militar de Engenharia. 2010. Trabalho de Conclusão de Curso. Consultado em: 2 de abril de 2023. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2010-Pinhao_Mendes_Daniel.pdf.

31 «APÓS APARENTE ataque, dois bancos retomam funcionamento na Ucrânia». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em https://www.cnnbrasil.com.br/internacional/ministerio-da-defesa-e-banco-ucranianos-sao-atingidos-por-possivel-ciberataque/.

32 «RUSSIA-BASED hacker group "XakNet" infiltrates Ukraine Finance Ministry». The Cyber Express. Consultado em: 14 de abril de 2023. Disponível em: https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

33 SAILIO, Mirko; LATVALA, Outi-Marja; SZANTO, Alexander – «Cyber threat actors for the factory of the future». In *Applied Sciences*. Suíça. Vol. 10, N.º 12, 2020, p. 4334.

34 MACA, Oscar; ARCOS, Andrés Felipe; URCUQUI, Christian – «Security control for website defacement». In *Sistemas y Telemática*. Colômbia. Vol. 15, N.º 41, 2017, pp. 45-55.

35 MEYER, Eric; MONTOYA, Michael – «Como proteger a infraestrutura crítica contra ataques cibernéticos». Consultado em: 14 de abril de 2023. Disponível em: https://www.securityreport.com.br/overview/como-proteger-a-infraestrutura-critica-contra-ataques-ciberneticos/#.ZDmksXbMLrd.

BIBLIOGRAFIA

«APÓS APARENTE ataque, dois bancos retomam funcionamento na Ucrânia». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em https://www.cnnbrasil.com.br/internacional/ministerio-da-defesa-e-banco-ucranianos-sao-atingidos-por-possivel-ciberataque/.

«ATAQUE CIBERNÉTICO atinge provedora de telecomunicações ucraniana, dizem autoridades». CNN Brasil. Consultado em: 13 de abril de 2023. Disponível em: https://www.cnnbrasil.com.br/internacional/ataque-cibernetico-atinge-provedora-de-telecomunicacoes-ucraniana-dizem-autoridades/.

AUTY, Caroline – «Political hacktivism: tool of the underdog or scourge of cyberspace?». In *Aslib Proceedings*. Vol. 56, N.º 4, 2023, pp. 212-221.

CAVELTY, Myriam Dunn – «Cyberwar: concept, status quo, and limitations». In *ETH Zurich*. Zurique. Vol. 71, 2010, pp. 1-3.

CERVI, Emerson Urizzi – «Métodos quantitativos nas ciências sociais: uma abordagem alternativa ao fetichismo dos números e ao debate com qualitativistas». In *Pesquisa Social Reflexões: Teóricas e Metodológicas*. Ponta Grossa: Todapalavra Editora, 2009, pp. 125-144.

COIMBRA, Sara – «Ameaças e vulnerabilidades à segurança da informação dos sistemas de informação da Força Aérea». Consultado em: 8 de abril de 2023. Disponível em: https://comum.rcaap.pt/bitstream/10400.26/24931/1/10_CapSara-Coimbra_TII_VF.pdf.

COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Council of European Union. Consultado em: 14 de abril de 2023. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32008L0114.

CRUZ JÚNIOR, Samuel César – «A segurança e defesa cibernética no Brasil e uma revisão das estratégias dos Estados Unidos, Rússia e Índia para o espaço virtual». Consultado em: 13 de abril de 2023. Disponível em: https://repositorio.ipea.gov.br/bitstream/11058/1590/1/TD_1850.pdf.

CYBERPEACE INSTITUTE – «Cyber threats landscape». Consultado em: 14 de março de 2023. Disponível em: https://cyberconflicts.cyberpeaceinstitute.org/threats.

DAI GLOBAL, LLC – *Usaid Cybersecurity for Critical Infrastructure in Ukraine Review of the Regulatory Framework for Critical Infrastructure Cybersecurity in Ukraine: Legislative Assessment Report*. Consultado em: 9 de abril de 2023. Disponível em: https://pdf.usaid.gov/pdf_docs/PA00XX1T.pdf.

DANTAS, Marcus Leal – *Segurança da Informação: Uma Abordagem Focada em G de Riscos*. 1.ª edição. Olinda: Livro Rápido, 2011.

HOSANG, Alexandre – *Política Nacional de Segurança Cibernética: Uma Necessidade para o Brasil*. Consultado em: 16 de abril de 2023. Disponível em: https://www.abeic.org.br/Admin/Publicacoes/29/PolNacSegCib.pdf.

KING, Gary – «Replicação, replicação». In *Revista Eletrônica de Ciência Política*. Vol. 6, N.º 2, 2015, pp. 382-401.

KING, Gary; KEOHANE, Robert O.; VERBA, Sidney – *Designing Social Inquiry: Scientific Inference in Qualitative Research*. 1.ª edição. New Jersey: Princeton University Press, 1994.

KONDRATOV, Sergiy; BOBRO, Dmytro; HORBULIN, Volodymyr; SUKHODOLIA, Oleksandr; IVANIUTA, Serhii; NASVIT, Oleh; BIRIUKOV, Dmytro; RIABTSEV, Genadiy – «Developing the critical infrastructure protection system in Ukraine: monograph». Kiev: National Institute For Strategic Studies, 2017. Consultado em: 14 de abril de 2023. Disponível em: https://niss.gov.ua/sites/default/files/2017-11/niss_Engl_findruk-0e9af.pdf.

KONRAD, Kaiser David Vargas; LOURENÇÃO, Humberto José – «O conflito na Ucrânia entre 2014 e 2018 e seu impacto na segurança internacional». In *Brazilian Journal of Development*. Vol. 5, N.º 8, 2019, pp. 12906-12920.

LEHTO, Martti – «Cyber-attacks against critical infrastructure». In *Computational Methods in Applied Sciences*. Suíça: Springer, 2022, pp. 3-42.

LIMA, Pedro Arthur Linhares – «Segurança cibernética: a necessidade de se estruturar, sistematizar e integrar a proteção cibernética das infraestruturas críticas nacionais, órgãos estratégicos do Governo e Forças Armadas». Consultado em: 14 de abril de 2023. Disponível em: https://www.enabed2018.abedef.org/resources/anais/8/1534802448_ARQUIVO_Artigo-PedroALinharesLima-X-ENABED-SegurancaeDefesaCibernetica.pdf.

MACA, Oscar; ARCOS, Andrés Felipe; URCUQUI, Christian – «Security control for website defacement». In *Sistemas y Telemática*. Colômbia. Vol. 15, N.º 41, 2017, pp. 45-55.

MELLO, Fábio P.; MENDES JÚNIOR, Ricardo da C.; ROCHA, Daniel G. – *Análise de Ataques DDoS*. Rio de Janeiro: Instituto Militar de Engenharia. 2010. Trabalho de Conclusão de Curso. Consultado em: 2 de abril de 2023. Disponível em: http://www.defesacibernetica.ime.eb.br/pub/repositorio/2010-Pinhao_Mendes_Daniel.pdf.

MEYER, Eric; MONTOYA, Michael – «Como proteger a infraestrutura crítica contra ataques cibernéticos». Consultado em: 14 de abril de 2023. Disponível em: https://www.securityreport.com.br/overview/como-proteger-a-infraestrutura-critica-contra-ataques-ciberneticos/#.ZDmksXbMLrd.

PARANHOS, Ranulfo; FIGUEIREDO FILHO, Dalson Britto; ROCHA, Enivaldo Carvalho da; SILVA JÚNIOR, José Alexandre da; FREITAS, Diego – «Uma introdução aos métodos mistos». In *Sociologias*. Vol. 18, N.º 42, 2016, pp. 384-411.

PEREIRA COUTINHO, Francisco – «A agressão russa à Ucrânia e o direito internacional: uma tragédia em quatro atos». In *e-publica*. Lisboa. Vol. 10, N.º 1, 2023, pp. 4-17.

«RUSSIA-BASED hacker group "XakNet" infiltrates Ukraine Finance Ministry». The Cyber Express. Consultado em: 14 de abril de 2023. Disponível em: https://thecyberexpress.com/hacker-xaknet-infiltrates-ukraine-ministry/.

SAILIO, Mirko; LATVALA, Outi-Marja; SZANTO, Alexander – «Cyber threat actors for the factory of the future». In *Applied Sciences*. Suíça. Vol. 10, N.º 12, 2020, p. 4334.

SIGHOLM, Johan – «Non-State actors in cyberspace operations». Consultado em: 14 de abril de 2023. Disponível em: https://www.researchgate.net/publication/310827486_Non-State_Actors_in_Cyberspace_Operations.

SPÎNU, Natalia – «Ukraine cybersecurity governance assessment». Consultado em: 9 de abril de 2023. Disponível em: https://www.dcaf.ch/sites/default/files/publications/documents/UkraineCybersecurityGovernanceAssessment.pdf.

TAQUARY SEGUNDO, Célio Borges – «A defesa cibernética em ambientes de infraestrutura crítica e os riscos dos ataques cibernéticos». Consultado em: 8 de abril de 2023. Disponível em: https://repositorio.esg.br/handle/123456789/1205.

YIN, Robert K. – «Discovering the future of the case study: method in evaluation research». In *Evaluation practice*. Vol. 15, N.º 3, 1994, pp. 283-290.

YIN, Robert K. – *Estudo de Caso: Planejamento e Métodos*. 5.ª edição. Porto Alegre: Editora Bookman, 2014.

ZETTER, Kim – «An unprecedented look at stuxnet, the world's first digital weapon». Consultado em: 13 de abril de 2023. Disponível em: https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/.